

kaspersky

Kaspersky Security Center

(version: 13.0.0.11247)

User Manual

Document version: 2.00

Table of Contents

What's new.....	27
Kaspersky Security Center 13	28
About Kaspersky Security Center	30
Distribution kit	31
Hardware and software requirements	31
List of supported Kaspersky applications	41
About compatibility of Administration Server and Kaspersky Security Center 13 Web Console	42
About Kaspersky Security Center Cloud Console	43
Basic concepts.....	44
Administration Server	44
Hierarchy of Administration Servers	45
Virtual Administration Server	46
Mobile Device Server	47
Web Server.....	47
Network Agent	48
Administration groups	49
Managed device	49
Unassigned device	49
Administrator's workstation.....	50
Management plug-in	50
Management web plug-in	50
Policies	51
Policy profiles.....	52
Tasks	52
Task scope	53
How local application settings relate to policies	54
Distribution point.....	55
Connection gateway	57
Architecture.....	58
Main installation scenario	59
Ports used by Kaspersky Security Center	65
About Kaspersky Security Center certificates	86
Schemas for data traffic and port usage.....	89
Administration Server and managed devices on LAN.....	90
Primary Administration Server on LAN and two secondary Administration Servers.....	94
Administration Server on LAN, managed devices on Internet, TMG in use.....	96
Administration Server on LAN, managed devices on Internet, connection gateway in use.....	99
Administration Server in DMZ, managed devices on Internet.....	104

Interaction of Kaspersky Security Center components and security applications: more information	108
Conventions used in interaction schemas.....	108
Administration Server and DBMS.....	110
Administration Server and Administration Console.....	111
Administration Server and client device: Managing the security application	112
Upgrading software on a client device through a distribution point.....	113
Hierarchy of Administration Servers: primary Administration Server and secondary Administration Server	114
Hierarchy of Administration Servers with a secondary Administration Server in DMZ	115
Administration Server, a connection gateway in a network segment, and a client device.....	116
Administration Server and two devices in DMZ: a connection gateway and a client device	117
Administration Server and Kaspersky Security Center 13 Web Console	118
Activating and managing the security application on a mobile device	119
Deployment best practices	120
Preparation for deployment	122
Planning Kaspersky Security Center deployment	123
Preparing to mobile device management.....	141
Information about Administration Server performance.....	146
Deploying Network Agent and the security application	150
Initial deployment	151
Remote installation of applications on devices with Network Agent installed.....	160
Managing device restarts in the remote installation task	161
Suitability of databases updating in an installation package of a security application	161
Using tools for remote installation of applications in Kaspersky Security Center for running relevant executable files on managed devices	161
Monitoring the deployment	163
Configuring installers.....	163
Virtual infrastructure	175
Support of file system rollback for devices with Network Agent.....	176
Local installation of applications.....	178
Deploying mobile device management systems	188
Deploying a system for management via Exchange ActiveSync protocol	188
Deploying a system for management using iOS MDM protocol	192
Adding a KES device to the list of managed devices.....	207
Connecting KES devices to the Administration Server	208
Integration with Public Key Infrastructure.....	212
Kaspersky Security Center Web Server.....	212
Installation of Kaspersky Security Center	213
Preparing for installation.....	214
Accounts for work with the DBMS	215
Scenario: Authenticating Microsoft SQL Server	222

Recommendations on Administration Server installation	224
Creating accounts for the Administration Server services on a failover cluster	224
Defining a shared folder	224
Remote installation with Administration Server tools through Active Directory group policies	225
Remote installation through delivery of the UNC path to a stand-alone package	225
Updating from the Administration Server shared folder	225
Installing images of operating systems	225
Specifying the address of the Administration Server	226
Standard installation	226
Step 1. Reviewing the License Agreement and Privacy Policy	227
Step 2. Selecting an installation method	227
Step 3. Installing Kaspersky Security Center 13 Web Console	227
Step 4. Selecting network size	228
Step 5. Selecting a database	230
Step 6. Configuring the SQL Server	230
Step 7. Selecting an authentication mode	231
Step 8. Unpacking and installing files on the hard drive	232
Custom installation	232
Step 1. Reviewing the License Agreement and Privacy Policy	233
Step 2. Selecting an installation method	233
Step 3. Selecting the components to be installed	234
Step 4. Installing Kaspersky Security Center 13 Web Console	234
Step 5. Selecting network size	235
Step 6. Selecting a database	236
Step 7. Configuring the SQL Server	237
Step 8. Selecting an authentication mode	238
Step 9. Selecting the account to start Administration Server	238
Step 10. Selecting the account for running the Kaspersky Security Center services	240
Step 11. Selecting a shared folder	240
Step 12. Configuring the connection to Administration Server	241
Step 13. Defining the Administration Server address	241
Step 14. Administration Server address for connection of mobile devices	242
Step 15. Selecting application management plug-ins	242
Step 16. Unpacking and installing files on the hard drive	242
Installing Administration Server on a failover cluster	243
Step 1. Reviewing the License Agreement and Privacy Policy	243
Step 2. Selecting the type of installation on a cluster	244
Step 3. Specifying the name of the virtual Administration Server	244
Step 4. Specifying the network details of the virtual Administration Server	244
Step 5. Specifying a cluster group	245

Step 6. Selecting a cluster data storage	245
Step 7. Specifying an account for remote installation	245
Step 8. Selecting the components to be installed	245
Step 9. Selecting network size	246
Step 10. Selecting a database	247
Step 11. Configuring the SQL Server.....	248
Step 12. Selecting an authentication mode.....	249
Step 13. Selecting the account to start Administration Server	249
Step 14. Selecting the account for running the Kaspersky Security Center services	250
Step 15. Selecting a shared folder	251
Step 16. Configuring the connection to Administration Server	251
Step 17. Defining the Administration Server address	252
Step 18. Administration Server address for connection of mobile devices	252
Step 19. Unpacking and installing files on the hard drive	252
Installing Administration Server in non-interactive mode	253
Installing Administration Console on the administrator's workstation	258
Changes in the system after Administration Server installation on the device	259
Removing the application	261
Upgrading Kaspersky Security Center from a previous version.....	262
Initial setup of Kaspersky Security Center	264
Administration Server Quick Start Wizard	265
About Quick Start Wizard	265
Starting Administration Server Quick Start Wizard	266
Step 1. Getting acquainted with Quick Start Wizard	266
Step 2. Configuring a proxy server.....	266
Step 3. Selecting the application activation method.....	267
Step 4. Selecting the protection scopes and platforms	268
Step 5. Selecting plug-ins for managed applications	269
Step 6. Downloading distribution packages and creating installation packages.....	269
Step 7. Configuring Kaspersky Security Network usage	270
Step 8. Configuring email notifications	271
Step 9. Configuring update management	271
Step 10. Connecting mobile devices	272
Step 11. Creating an initial protection configuration.....	277
Step 12. Downloading updates	277
Step 13. Device discovery	277
Step 14. Closing the Quick Start Wizard.....	278
Configuring the connection of Administration Console to Administration Server	278
Requirements to custom certificates used in Kaspersky Security Center.....	279
Connecting out-of-office devices	282

Scenario: Connecting out-of-office devices through a connection gateway	283
About connecting out-of-office devices	285
Connecting external desktop computers to Administration Server	286
About connection profiles for out-of-office users.....	287
Creating a connection profile for out-of-office users	288
About switching Network Agent to other Administration Servers	291
Creating a Network Agent switching rule by network location	292
Encrypt communication with SSL/TLS	294
Notifications of events	297
Configuring event notification	297
Testing notifications.....	299
Event notifications displayed by running an executable file	300
Configuring the interface	300
Discovering networked devices	303
Scenario: Discovering networked devices.....	303
Unassigned devices	304
Device discovery	304
Working with Windows domains. Viewing and changing the domain settings.....	311
Configuring retention rules for unassigned devices	311
Working with IP ranges	312
Working with the Active Directory groups. Viewing and modifying group settings	313
Creating rules for moving devices to administration groups automatically	313
Using VDI dynamic mode on client devices	313
Equipment inventory	315
Adding information about new devices	316
Configuring criteria used to define enterprise devices	316
Configuring custom fields	317
Licensing.....	317
About the End User License Agreement	318
About the license	319
About the license certificate.....	319
About the license key	320
Kaspersky Security Center licensing options	320
About restrictions on the main functionality.....	322
About the activation code	323
About the key file	323
About data provision	324
About the subscription	328
Events of the licensing limit exceeded	329
Licensing features of Kaspersky Security Center and managed applications	329

Revoking consent with End User License Agreement	331
Kaspersky applications. Centralized deployment	332
Replacing third-party security applications	333
Installing applications using a remote installation task	334
Installing an application on selected devices	335
Installing an application on client devices in an administration group	335
Installing an application through Active Directory group policies	335
Installing applications on secondary Administration Servers	337
Installing applications using Remote Installation Wizard	338
Viewing a protection deployment report	342
Remote removal of applications	342
Remote removal of an application from client devices of the administration group	343
Remote removal of an application from selected devices	343
Working with installation packages	344
Creating an installation package	344
Creating stand-alone installation packages	346
Creating custom installation packages	347
Viewing and editing properties of custom installation packages	348
Distributing installation packages to secondary Administration Servers	349
Distributing installation packages through distribution points	350
Transferring application installation results to Kaspersky Security Center	350
Receiving up-to-date versions of applications	351
Preparing a device for remote installation. Utility tool riprep.exe	353
Preparing a device for remote installation in interactive mode	353
Preparing a device for remote installation in non-interactive mode	354
Preparing a Linux device for remote installation of Network Agent	355
Preparing a macOS device for remote installation of Network Agent	356
Kaspersky applications: licensing and activation	357
Licensing of managed applications	358
Viewing information about license keys in use	360
Adding a license key to the Administration Server repository	360
Deleting an Administration Server license key	361
Deploying a license key to client devices	361
Automatic distribution of a license key	361
Creating and viewing a license key usage report	362
Configuring network protection	363
Scenario: Configuring network protection	364
Policy setup and propagation: Device-centric approach	365
About device-centric and user-centric security management approaches	367
Manual setup of Kaspersky Endpoint Security policy	368

Configuring the policy in the Advanced Threat Protection section.....	369
Configuring the policy in the Essential Threat Protection section	369
Configuring the policy in the General Settings section.....	370
Configuring the policy in the Event configuration section	370
Manual setup of the group update task for Kaspersky Endpoint Security	371
Manual setup of the group task for scanning a device with Kaspersky Endpoint Security	371
Scheduling the Find vulnerabilities and required updates task	372
Manual setup of the group task for updates installation and vulnerabilities fix	372
Setting the maximum number of events in the event repository	372
Managing tasks	373
Creating a task	374
Creating an Administration Server task.....	375
Creating a task for specific devices.....	376
Creating a local task.....	376
Displaying an inherited group task in the workspace of a nested group.....	377
Automatically turning on devices before starting a task.....	377
Automatically turning off a device after a task is completed	377
Limiting task run time	378
Exporting a task.....	378
Importing a task.....	378
Converting tasks.....	379
Starting and stopping a task manually	379
Pausing and resuming a task manually	380
Monitoring task execution.....	380
Viewing task run results stored on the Administration Server.....	380
Configuring filtering of information about task run results.....	380
Modifying a task. Rolling back changes	381
Comparing tasks.....	381
Accounts to start tasks	382
Change Tasks Password Wizard	383
Creating a hierarchy of administration groups subordinate to a virtual Administration Server	384
Hierarchy of policies, using policy profiles.....	385
Hierarchy of policies	385
Policy profiles	385
Inheritance of policy settings.....	387
Managing policies.....	387
Creating a policy.....	388
Displaying inherited policy in a subgroup.....	389
Activating a policy.....	390
Activating a policy automatically at the Virus outbreak event	390

Applying an out-of-office policy	390
Modifying a policy. Rolling back changes	390
Comparing policies	391
Deleting a policy	392
Copying a policy	392
Exporting a policy	392
Importing a policy	392
Converting policies	393
Managing policy profiles	393
Device moving rules	401
Cloning device moving rules.....	402
Software categorization	403
Prerequisites for installing applications on devices of a client organization.....	403
Viewing and editing local application settings	404
Updating Kaspersky Security Center and managed applications	405
Scenario: Upgrading Kaspersky Security Center and managed applications.....	405
About updating Kaspersky databases, software modules, and applications	406
Using diff files for updating Kaspersky databases and software modules	412
Creating the task for downloading updates to the repository of the Administration Server	413
Creating the Downloading updates to the repositories of distribution points task.....	417
Configuring the Download updates to the repository of the Administration Server task.....	421
Verifying downloaded updates	422
Configuring test policies and auxiliary tasks.....	423
Viewing downloaded updates.....	424
Automatic distribution of updates	424
Distributing updates to client devices automatically.....	425
Distributing updates to secondary Administration Servers automatically	425
Installing updates for software modules of Network Agents automatically	426
Assigning distribution points automatically.....	426
Assigning a device a distribution point manually.....	427
Removing a device from the list of distribution points	430
Downloading updates by distribution points	430
Deleting software updates from the repository	431
Algorithm of patch installation for a Kaspersky application in cluster mode	431
Managing third-party applications on client devices	432
Installation of third-party software updates.....	432
Viewing information about available updates	434
Approving and declining software updates	435
Synchronizing updates from Windows Update with Administration Server	436
Automatic installation of Kaspersky Endpoint Security updates on devices	441

Offline model of update download.....	442
Enabling and disabling the offline model of update download.....	443
Installing updates on devices manually.....	444
Configuring Windows updates in a Network Agent policy.....	455
Automatic updating and patching for Kaspersky Security Center components.....	457
Enabling and disabling automatic updating and patching for Kaspersky Security Center components.....	458
Fixing third-party software vulnerabilities.....	459
Scenario: Finding and fixing vulnerabilities in third-party software.....	459
About finding and fixing software vulnerabilities.....	462
Viewing information about software vulnerabilities.....	463
Viewing statistics of vulnerabilities on managed devices.....	463
Scanning applications for vulnerabilities.....	464
Fixing vulnerabilities in applications.....	469
Ignoring software vulnerabilities.....	480
Selecting user fixes for vulnerabilities in third-party software.....	481
Rules for update installation.....	482
Groups of applications.....	485
Creating application categories for Kaspersky Endpoint Security for Windows policies.....	487
Creating an application category with content added manually.....	489
Creating an application category with content added automatically.....	491
Adding event-related executable files to the application category.....	493
Configuring application startup management on client devices.....	494
Viewing the results of static analysis of startup rules applied to executable files.....	495
Viewing the applications registry.....	496
Changing the software inventory start time.....	497
About license key management of third-party applications.....	498
Creating licensed applications groups.....	499
Managing license keys for licensed applications groups.....	499
Inventory of executable files.....	500
Viewing information about executable files.....	501
Monitoring and reporting.....	502
Traffic lights in Administration Console.....	503
Working with reports, statistics, and notifications.....	503
Working with reports.....	504
Managing statistics.....	515
Configuring event notification.....	515
Creating a certificate for an SMTP server.....	518
Event selections.....	518
Configuring event export to a SIEM system.....	521
Device selections.....	521

Monitoring of applications installation and uninstallation	535
Event types	535
Data structure of event type description.....	536
Administration Server events	536
Network Agent events	568
iOS MDM Server events.....	575
Exchange Mobile Device Server events	581
Blocking frequent events	582
About blocking frequent events	582
Managing frequent events blocking	583
Removing blocking of frequent events	583
Exporting a list of frequent events to a file	583
Controlling changes in the status of virtual machines	584
Monitoring the anti-virus protection status using information from the system registry	584
Viewing and configuring the actions when devices show inactivity.....	586
Adjustment of distribution points and connection gateways	587
Standard configuration of distribution points: Single office	588
Standard configuration of distribution points: Multiple small remote offices	588
Assigning a managed device to act as a distribution point	589
Connecting a new network segment by using Linux devices.....	590
Connecting a Linux device as a gateway in the demilitarized zone.....	590
Connecting a Linux device to the Administration Server via a connection gateway	591
Adding a connection gateway in the DMZ as a distribution point.....	592
Assigning distribution points automatically.....	593
Local installation of Network Agent on a device selected as distribution point	593
Using a distribution point as connection gateway	594
Adding IP ranges to the scanned ranges list of a distribution point	594
Other routine tasks	596
Managing Administration Servers	596
Creating a hierarchy of Administration Servers: adding a secondary Administration Server	597
Connecting to an Administration Server and switching between Administration Servers.....	600
Access rights to Administration Server and its objects	601
Conditions of connection to an Administration Server over the Internet.....	602
Encrypted connection to an Administration Server	603
Disconnecting from an Administration Server	605
Adding an Administration Server to the console tree	605
Removing an Administration Server from the console tree.....	605
Adding a virtual Administration Server to the console tree	605
Changing an Administration Server service account. Utility tool klsrvswch	606
Changing DBMS credentials	607

Resolving issues with Administration Server nodes.....	608
Viewing and modifying the settings of an Administration Server	608
Backup and restoration of Administration Server settings	615
Backup copying and restoration of Administration Server data	617
Avoiding conflicts between multiple Administration Servers	623
Two-step verification	623
Managing administration groups	630
Creating administration groups	631
Moving administration groups	632
Deleting administration groups.....	633
Automatic creation of a structure of administration groups.....	634
Automatic installation of applications on devices in an administration group	635
Managing client devices	635
Connecting client devices to the Administration Server.....	636
Manually connecting a client device to the Administration Server. Klmover utility	638
Tunneling the connection between a client device and the Administration Server.....	639
Remotely connecting to the desktop of a client device	639
Connecting to devices through Windows Desktop Sharing	641
Configuring the restart of a client device.....	641
Auditing actions on a remote client device.....	641
Checking the connection between a client device and the Administration Server.....	642
Identifying client devices on the Administration Server.....	644
Moving devices to an administration group.....	644
Changing the Administration Server for client devices	645
Clusters and server arrays	645
Turning on, turning off, and restarting client devices remotely	646
Access to local tasks and statistics, "Do not disconnect from the Administration Server" check box	646
Forced synchronization	646
About connection schedule	647
Sending messages to device users.....	647
Managing Kaspersky Security for Virtualization.....	647
Configuring the switching of device statuses	647
Tagging devices and viewing assigned tags.....	649
Remote diagnostics of client devices. Kaspersky Security Center remote diagnostics utility.....	651
UEFI protection devices	657
Settings of a managed device	658
General policy settings	663
Network Agent policy settings	665
Managing user accounts	678
Working with user accounts	678

Adding an account of an internal user.....	679
Editing an account of an internal user.....	680
Changing the number of allowed password entry attempts.....	681
Configuring the check of the name of an internal user for uniqueness.....	682
Adding a security group.....	683
Adding a user to a group.....	683
Configuring access rights to application features. Role-based access control.....	683
Assigning the user as a device owner.....	710
Delivering messages to users.....	710
Viewing the list of user mobile devices.....	711
Installing a certificate for a user.....	711
Viewing the list of certificates issued to a user.....	711
About the administrator of a virtual Administration Server.....	712
Remote installation of operating systems and applications.....	712
Creating images of operating systems.....	714
Installing images of operating systems.....	714
Adding drivers for Windows Preinstallation Environment (WinPE).....	715
Adding drivers to an installation package with an operating system image.....	716
Configuring sysprep.exe utility.....	716
Deploying operating systems on new networked devices.....	716
Deploying operating systems on client devices.....	717
Creating installation packages of applications.....	717
Issuing a certificate for installation packages of applications.....	718
Installing applications on client devices.....	719
Managing object revisions.....	719
About object revisions.....	721
Viewing the Revision history section.....	721
Comparing object revisions.....	722
Setting storage term for object revisions and for deleted object information.....	723
Viewing an object revision.....	723
Saving an object revision to a file.....	724
Rolling back changes.....	724
Adding a revision description.....	725
Deletion of objects.....	725
Deleting an object.....	726
Viewing information about deleted objects.....	726
Deleting objects permanently from the list of deleted objects.....	727
Mobile Device Management.....	727
Scenario: Mobile Device Management deployment.....	728
About group policy for managing EAS and iOS MDM devices.....	729

Enabling Mobile Device Management.....	730
Modifying the Mobile Device Management settings.....	731
Disabling Mobile Device Management.....	732
Working with commands for mobile devices.....	733
Working with certificates.....	737
Adding iOS mobile devices to the list of managed devices.....	744
Adding Android mobile devices to the list of managed devices.....	746
Managing Exchange ActiveSync mobile devices.....	749
Managing iOS MDM devices.....	755
Managing KES devices.....	766
Data encryption and protection.....	768
Viewing the list of encrypted devices.....	769
Viewing the list of encryption events.....	769
Exporting the list of encryption events to a text file.....	770
Creating and viewing encryption reports.....	770
Transmitting encryption keys between Administration Servers.....	772
Data repositories.....	774
Exporting a list of repository objects to a text file.....	774
Installation packages.....	775
Main statuses of files in the repository.....	775
Triggering of rules in Smart Training mode.....	776
Quarantine and Backup.....	780
Active threats.....	783
Kaspersky Security Network (KSN).....	785
About KSN.....	785
Setting up access to Kaspersky Security Network.....	786
Enabling and disabling KSN.....	788
Viewing the accepted KSN Statement.....	788
Viewing the KSN proxy server statistics.....	789
Accepting an updated KSN Statement.....	789
Enhanced protection with Kaspersky Security Network.....	791
Checking whether the distribution point works as KSN Proxy.....	791
Switching between Online Help and Offline Help.....	791
Exporting events to SIEM systems.....	791
Events in Kaspersky Security Center.....	792
Event export process.....	794
Configuring event export in Kaspersky Security Center.....	795
Exporting events using Syslog.....	795
Before you begin.....	796
Enabling automatic export.....	796

Selecting export events	797
Selecting events in a policy	797
Selecting events for an application.....	798
Exporting events using CEF and LEEF protocols	800
Before you begin	801
Enabling automatic export of general events	801
Exporting events directly from the database	803
Creating an SQL query using the klsql2 utility	803
Example of an SQL query in the klsql2 utility.....	804
Viewing the Kaspersky Security Center database name	805
Configuring event export in a SIEM system	806
Viewing export results	808
Using SNMP for sending statistics to third-party applications	809
SNMP agent and object identifiers	809
Getting a string counter name from an object identifier	809
Values of object identifiers for SNMP	810
Troubleshooting.....	818
Working in a cloud environment	820
About work in a cloud environment	820
Scenario: Deployment for cloud environment	821
Prerequisites for deploying Kaspersky Security Center in a cloud environment.....	825
Hardware requirements for the Administration Server in a cloud environment.....	826
Licensing options in a cloud environment	826
Database options for work in a cloud environment	827
Working in Amazon Web Services cloud environment	828
About work in Amazon Web Services cloud environment	829
Creating IAM roles and IAM user accounts for Amazon EC2 instances.....	829
Working with Amazon RDS	835
Working in Microsoft Azure cloud environment.....	842
About work in Microsoft Azure.....	843
Creating a subscription, Application ID, and password.....	843
Assigning a role to the Azure Application ID	844
Deploying Administration Server in Microsoft Azure and selecting database.....	845
Working with Azure SQL	846
Working in Google Cloud.....	849
Creating client email, project ID, and private key.....	849
Working with Google Cloud SQL for MySQL instance.....	850
Prerequisites for client devices in a cloud environment necessary for work with Kaspersky Security Center	852
Cloud Environment Configuration Wizard	853
About the Cloud Environment Configuration Wizard.....	855

Step 1. Selecting the application activation method.....	855
Step 2. Selecting the cloud environment.....	856
Step 3. Authorization in the cloud environment.....	856
Step 4. Configuring synchronization with Cloud and choosing further actions	858
Step 5. Configuring Kaspersky Security Network	860
Step 6. Configuring email notifications.....	860
Step 7. Creating an initial protection configuration.....	861
Step 8. Selecting the action when the operating system must be restarted during installation	862
Step 9. Receiving updates by the Administration Server	863
Checking configuration	864
Cloud device group.....	865
Network segment polling	865
Adding connections for cloud segment polling.....	866
Deleting connections for cloud segment polling.....	868
Configuring the polling schedule	869
Installing applications on devices in a cloud environment.....	870
Viewing the properties of cloud devices	872
Synchronization with cloud	873
Using deployment scripts for deploying security applications	876
Deployment of Kaspersky Security Center in Yandex.Cloud	877
Troubleshooting	878
Problems with remote installation of applications.....	878
Incorrect copying of a hard drive image	881
Problems with Exchange Mobile Device Server.....	882
Problems with iOS MDM Server.....	883
Portal support.kaspersky.com	883
Checking APNs service for accessibility	883
Recommended procedure for solving problems with iOS MDM web service	883
Problems with KES devices.....	885
Portal support.kaspersky.com	886
Checking the settings of Google Firebase Cloud Messaging service	886
Checking Google Firebase Cloud Messaging for accessibility	886
Problems with tasks when using Administration Server as WSUS server	886
Appendices	888
Advanced features.....	888
Kaspersky Security Center operation automation. klakaut utility	889
Custom tools.....	889
Network Agent disk cloning mode.....	889
Preparing a reference device with Network Agent installed for creating an image of operating system	890
Configuring receipt of messages from File Integrity Monitor.....	891

Administration Server maintenance	892
User notification method window.....	893
General section	894
Device selection window	894
Define the name of the new object window.....	894
Application categories section.....	894
About multi-tenant applications	895
Features of using the management interface.....	895
Console tree	896
How to return to a properties window that disappeared.....	900
How to update data in the workspace	900
How to navigate the console tree	900
How to open the object properties window in the workspace	901
How to select a group of objects in the workspace.....	901
How to change the set of columns in the workspace.....	901
Reference information	901
Context menu commands	902
List of managed devices. Description of columns	905
Statuses of devices, tasks, and policies.....	910
File status icons in Administration Console.....	913
Searching and exporting data.....	914
Finding devices.....	914
Device search settings	916
Using masks in string variables.....	927
Using regular expressions in the search field	927
Exporting lists from dialog boxes.....	928
Settings of tasks	928
General task settings.....	928
Download updates to the repository of the Administration Server task settings.....	934
Download updates to the repositories of distribution points task settings	936
Find vulnerabilities and required updates task settings	937
Install required updates and fix vulnerabilities task settings	939
Global list of subnets	941
Adding subnets to the global list of subnets.....	941
Viewing and modifying subnet properties in the global list of subnets.....	942
Usage of Network Agent for Windows, for macOS and for Linux: comparison.....	942
Frequently Asked Questions	950
Kaspersky Security Center 13 Web Console	953
About Kaspersky Security Center 13 Web Console.....	954
Hardware and software requirements for Kaspersky Security Center 13 Web Console	955

List of Kaspersky applications supported by Kaspersky Security Center 13 Web Console	957
Deployment diagram of Kaspersky Security Center Administration Server and Kaspersky Security Center 13 Web Console	959
Ports used by Kaspersky Security Center 13 Web Console	960
Scenario: Installation and initial setup of Kaspersky Security Center 13 Web Console	962
Installation.....	964
Installing a database management system	964
Configuring the MariaDB x64 server for working with Kaspersky Security Center 13	964
Installing Kaspersky Security Center (Standard installation)	966
Installing Kaspersky Security Center 13 Web Console	967
Installation of Kaspersky Security Center 13 Web Console on Linux platforms	969
Installing Kaspersky Security Center 13 Web Console on Linux platforms	969
Kaspersky Security Center 13 Web Console installation parameters.....	970
Upgrading Kaspersky Security Center Web Console	974
Specifying certificates for trusted Administration Servers	975
Replacing certificate for Kaspersky Security Center 13 Web Console	976
Converting a PFX certificate to the PEM format.....	977
Reissuing the certificate for Kaspersky Security Center Web Console.....	978
Migration to Kaspersky Security Center Cloud Console	980
Methods of migration to Kaspersky Security Center Cloud Console	980
Scenario: Migration without a hierarchy of Administration Servers.....	981
Step 1. Exporting managed devices, objects, and settings from Kaspersky Security Center Web Console	983
Step 2. Importing the export file to Kaspersky Security Center Cloud Console.....	984
Step 3. Re-installing Network Agent on devices managed through Kaspersky Security Center Cloud Console	986
Migration with a hierarchy of Administration Servers	987
Logging in to Kaspersky Security Center 13 Web Console and logging out.....	991
Configuring domain authentication by using the NTLM and Kerberos protocols	992
Quick Start Wizard (Kaspersky Security Center 13 Web Console).....	993
Getting acquainted with Quick Start Wizard	994
Step 1. Specifying the Internet connection settings	994
Step 2. Downloading required updates	995
Step 3. Selecting the protection scopes and platforms	995
Step 4. Selecting encryption in solutions.....	996
Step 5. Configuring installation of plug-ins for managed applications.....	996
Step 6. Installing the selected plug-ins	997
Step 7. Downloading distribution packages and creating installation packages.....	997
Step 8. Configuring Kaspersky Security Network.....	997
Step 9. Selecting the application activation method.....	998
Step 10. Specifying the third-party update management settings.....	999

Step 11. Creating a basic network protection configuration	1000
Step 12. Configuring email notifications	1000
Step 13. Performing a network poll	1000
Step 14. Closing the Quick Start Wizard	1001
Protection Deployment Wizard	1001
Starting Protection Deployment Wizard	1001
Step 1. Selecting the installation package.....	1002
Step 2. Selecting a method for distribution of key file or activation code	1002
Step 3. Selecting Network Agent version	1002
Step 4. Selecting devices	1002
Step 5. Specifying the remote installation task settings	1003
Step 6. Restart management.....	1004
Step 7. Removing incompatible applications before installation	1005
Step 8. Moving devices to Managed devices	1005
Step 9. Selecting accounts to access devices	1005
Step 10. Starting installation.....	1006
Configuring Administration Server	1007
Configuring the connection of Kaspersky Security Center 13 Web Console to Administration Server ..	1007
Viewing log of connections to the Administration Server	1008
Setting the maximum number of events in the event repository	1008
Modifying the Mobile Device Management settings	1009
Connection settings of UEFI protection devices.....	1010
Creating a virtual Administration Server	1010
Creating a hierarchy of Administration Servers: adding a secondary Administration Server	1011
Viewing the list of secondary Administration Servers	1013
Deleting a hierarchy of Administration Servers	1014
Configuring the interface	1014
Enabling account protection from unauthorized modification.....	1015
Two-step verification.....	1015
Scenario: configuring two-step verification for all users.....	1015
About two-step verification	1017
Enabling two-step verification for your own account	1019
Enabling two-step verification for all users	1019
Disabling two-step verification for a user account.....	1020
Disabling two-step verification for all users	1020
Excluding accounts from two-step verification	1021
Generating a new secret key.....	1021
Editing the name of a security code issuer	1022
Kaspersky applications deployment through Kaspersky Security Center 13 Web Console	1023
Scenario: Kaspersky applications deployment through Kaspersky Security Center 13 Web Console ...	1023

Getting plug-ins for Kaspersky applications	1025
Downloading and creating installation packages for Kaspersky applications	1025
Changing the limit on the size of custom installation package data	1027
Downloading distribution packages for Kaspersky applications.....	1027
Checking Kaspersky Endpoint Security for Windows for success	1028
Creating stand-alone installation packages.....	1028
Viewing the list of stand-alone installation packages	1030
Creating custom installation packages	1031
Specifying settings for remote installation on Unix devices	1034
Replacing third-party security applications	1035
Discovering networked devices	1037
Device selections.....	1037
Scenario: Discovering networked devices.....	1038
Device discovery	1039
Windows network polling	1039
Active Directory polling.....	1041
IP range polling.....	1042
Adding and modifying an IP range	1044
Configuring retention rules for unassigned devices	1045
Device tags	1046
About device tags	1046
Creating a device tag	1047
Renaming a device tag.....	1047
Deleting a device tag.....	1047
Viewing devices to which a tag is assigned	1048
Viewing tags assigned to a device	1048
Tagging a device manually.....	1048
Removing an assigned tag from a device	1049
Viewing rules for tagging devices automatically.....	1049
Editing a rule for tagging devices automatically	1049
Creating a rule for tagging devices automatically	1050
Running rules for auto-tagging devices.....	1051
Deleting a rule for tagging devices automatically.....	1051
Application tags	1052
About application tags	1052
Creating an application tag.....	1052
Renaming an application tag.....	1053
Assigning tags to an application.....	1053
Removing assigned tags from an application	1053
Deleting an application tag	1054

Kaspersky applications: licensing and activation	1054
Licensing of managed applications	1054
Adding a license key to the Administration Server repository	1056
Deploying a license key to client devices	1057
Automatic distribution of a license key	1057
Viewing information about license keys in use	1058
Deleting a license key from the repository	1058
Revoking consent with an End User License Agreement	1059
Configuring network protection	1061
Scenario: Configuring network protection	1061
About device-centric and user-centric security management approaches	1063
Policy setup and propagation: Device-centric approach	1064
Policy setup and propagation: User-centric approach	1066
Manual setup of Kaspersky Endpoint Security policy	1068
Configuring the policy in the Advanced Threat Protection section.....	1069
Configuring the policy in the Essential Threat Protection section.....	1069
Configuring the policy in the General Settings section.....	1070
Configuring the policy in the Event configuration section	1071
Manual setup of the group update task for Kaspersky Endpoint Security	1073
Granting offline access to the external device blocked by Device Control	1073
Removing applications or software updates remotely.....	1074
Rolling back an object to a previous revision	1076
Tasks	1078
About tasks.....	1078
About task scope	1079
Creating a task	1080
Starting a task manually	1080
Viewing the task list.....	1081
General task settings.....	1081
Starting the wizard for changing tasks password.....	1087
Managing client devices	1090
Settings of a managed device	1090
Creating device moving rules	1094
Copying device moving rules	1095
Adding devices to an administration group manually.....	1096
Moving devices to an administration group manually	1097
Viewing and configuring the actions when devices show inactivity	1098
About device statuses	1099
Configuring the switching of device statuses	1104
Remotely connecting to the desktop of a client device	1105

Connecting to devices through Windows Desktop Sharing	1107
Policies and policy profiles	1110
About policies and policy profiles	1110
About lock and locked settings.....	1111
Inheritance of policies and policy profiles.....	1112
Managing policies.....	1118
Managing policy profiles.....	1127
Data encryption and protection.....	1133
Viewing the list of encrypted drives	1134
Viewing the list of encryption events	1134
Creating and viewing encryption reports.....	1135
Granting access to an encrypted drive in offline mode	1136
Users and user roles	1137
About user roles	1137
Configuring access rights to application features. Role-based access control.....	1139
Adding an account of an internal user.....	1161
Creating a user group.....	1162
Editing an account of an internal user.....	1162
Editing a user group	1163
Adding user accounts to an internal group.....	1164
Assigning a user as a device owner.....	1164
Deleting a user or a security group	1164
Creating a user role.....	1165
Editing a user role	1165
Editing the scope of a user role.....	1165
Deleting a user role	1166
Associating policy profiles with roles	1167
Kaspersky Security Network (KSN).....	1168
About KSN.....	1168
Setting up access to Kaspersky Security Network.....	1169
Enabling and disabling KSN.....	1171
Viewing the accepted KSN Statement	1171
Accepting an updated KSN Statement.....	1172
Checking whether the distribution point works as KSN Proxy	1172
Scenario: Upgrading Kaspersky Security Center and managed security applications	1173
Updating Kaspersky databases and applications.....	1174
Scenario: Regular updating Kaspersky databases and applications	1174
About updating Kaspersky databases, software modules, and applications	1178
Creating the task for downloading updates to the repository of the Administration Server	1184
Creating the task for downloading updates to the repositories of distribution points	1189

Enabling and disabling automatic updating and patching for Kaspersky Security Center components	1194
Automatic installation of updates for Kaspersky Endpoint Security for Windows	1195
Approving and declining software updates	1197
Updating Administration Server	1198
Verifying downloaded updates	1198
Enabling and disabling the offline model of update download	1200
Updating Kaspersky databases and software modules on offline devices	1200
Adjustment of distribution points and connection gateways	1201
Standard configuration of distribution points: Single office	1202
Standard configuration of distribution points: Multiple small remote offices	1203
Assigning distribution points automatically	1203
Assigning distribution points manually	1204
Modifying the list of distribution points for an administration group	1207
Managing third-party applications on client devices	1207
Installation of third-party software updates	1208
Scenario: Updating third-party software	1208
About third-party software updates	1211
Installing third-party software updates	1212
Creating the Find vulnerabilities and required updates task	1216
Find vulnerabilities and required updates task settings	1219
Creating the Install required updates and fix vulnerabilities task	1221
Adding rules for update installation	1225
Creating the Install Windows Update updates task	1229
Viewing information about available third-party software updates	1231
Exporting the list of available software updates to a file	1232
Approving and declining third-party software updates	1233
Creating the Perform Windows Update synchronization task	1234
Updating third-party applications automatically	1236
Fixing third-party software vulnerabilities	1236
Scenario: Finding and fixing vulnerabilities in third-party software	1237
About finding and fixing software vulnerabilities	1240
Fixing vulnerabilities in third-party software	1241
Creating the Fix vulnerabilities task	1244
Creating the Install required updates and fix vulnerabilities task	1246
Adding rules for update installation	1250
Selecting user fixes for vulnerabilities in third-party software	1253
Viewing information about software vulnerabilities detected on all managed devices	1254
Viewing information about software vulnerabilities detected on the selected managed device	1255
Viewing statistics of vulnerabilities on managed devices	1255
Exporting the list of software vulnerabilities to a file	1256

Ignoring software vulnerabilities	1256
Managing applications run on client devices	1257
Scenario: Application Management	1258
About Application Control	1260
Obtaining and viewing a list of applications installed on client devices	1261
Obtaining and viewing a list of executable files stored on client devices	1261
Creating application category with content added manually	1262
Creating application category that includes executable files from selected devices	1265
Creating application category that includes executable files from selected folder	1267
Viewing the list of application categories	1269
Configuring Application Control in the Kaspersky Endpoint Security for Windows policy	1269
Adding event-related executable files to the application category	1270
Creating an installation package of a third-party application from the Kaspersky database	1273
Viewing and modifying the settings of an installation package of a third-party application from the Kaspersky database	1274
Settings of an installation package of a third-party application from the Kaspersky database	1274
Monitoring and reporting	1277
Scenario: Monitoring and reporting	1279
About types of monitoring and reporting	1280
Using the dashboard	1281
Adding widgets to the dashboard	1281
Hiding a widget from the dashboard	1282
Moving a widget on the dashboard	1282
Changing the widget size or appearance	1282
Changing widget settings	1283
Using reports	1283
Creating a report template	1284
Viewing and editing report template properties	1284
Exporting a report to a file	1287
Generating and viewing a report	1287
Creating a report delivery task	1288
Deleting report templates	1289
Using event selections	1289
Creating an event selection	1290
Editing an event selection	1290
Viewing a list of an event selection	1291
Viewing details of an event	1291
Exporting events to a file	1292
Viewing an object history from an event	1292
Deleting events	1292
Deleting event selections	1292

Using notifications	1293
Viewing onscreen notifications	1293
About device statuses	1296
Configuring the switching of device statuses	1301
Configuring notification delivery.....	1303
Setting the storage term for an event	1305
Event types	1306
Data structure of event type description.....	1307
Administration Server events	1307
Network Agent events	1340
iOS MDM Server events.....	1344
Exchange Mobile Device Server events	1350
Blocking frequent events	1351
About blocking frequent events	1351
Managing frequent events blocking	1352
Removing blocking of frequent events	1352
Device selections.....	1353
Creating a device selection	1353
Configuring a device selection	1354
About Kaspersky announcements.....	1365
Specifying Kaspersky announcements settings	1366
Disabling Kaspersky announcements	1367
Kaspersky Security Center 13 Web Console activity logging.....	1368
Integration between Kaspersky Security Center Web Console and other Kaspersky solutions	1369
Configuring access to KATA/KEDR Web Console.....	1369
Establishing a background connection for cross-service integration	1369
Working with Kaspersky Security Center 13 Web Console in a cloud environment	1370
Kaspersky Security Center 13 Web Console Cloud Environment Configuration Wizard.....	1371
Step 1. Reading information about the Wizard	1372
Step 2. Licensing the application.....	1372
Step 3. Selecting the cloud environment and authorization	1372
Step 4. Segment polling, configuring synchronization with Cloud and choosing further actions	1374
Step 5. Configuring Kaspersky Security Network for Kaspersky Security Center	1376
Step 6. Creating an initial configuration of protection.....	1376
Network segment polling via Kaspersky Security Center 13 Web Console	1377
Adding connections for cloud segment polling.....	1378
Deleting a connection for cloud segment polling.....	1380
Configuring the polling schedule via Kaspersky Security Center 13 Web Console	1381
Viewing the results of cloud segment polling via Kaspersky Security Center 13 Web Console	1382
Viewing the properties of cloud devices via Kaspersky Security Center 13 Web Console.....	1382

Synchronization with Cloud: configuring the moving rule.....	1383
Creating Backup of the Administration Server data task by using a cloud DBMS	1385
Remote diagnostics of client devices	1387
Opening the remote diagnostics window.....	1388
Enabling and disabling tracing for applications	1388
Downloading trace files of an application	1390
Deleting trace files	1391
Downloading application settings	1391
Downloading event logs	1392
Starting, stopping, restarting the application	1392
Running the remote diagnostics of an application and downloading the results	1393
Running an application on a client device	1393
API Reference Guide	1395
Best Practices for Service Providers	1399
Sizing Guide.....	1400
Contact Technical Support	1401
How to get technical support	1401
Get technical support by phone	1401
Technical Support via Kaspersky CompanyAccount.....	1402
Sources of information about the application	1403
Glossary	1404
Information about third-party code.....	1416
Trademark notices	1417
Limitations and warnings	1419
Index	1420

What's new

Kaspersky Security Center 13 has several new features and improvements.

Kaspersky Security Center 13 Web Console

The following features are added to Kaspersky Security Center 13 Web Console:

- Implemented two-step verification (see section "About two-step verification" on page [1017](#)). You can enable two-step verification to reduce the risk of unauthorized access to Kaspersky Security Center 13 Web Console (see section "Enabling two-step verification for all users" on page [1019](#)).
- You can now view incidents and manage workstations via Kaspersky Managed Detection and Response (see section "Establishing a background connection for cross-service integration" on page [1369](#)).
- You can now specify settings for Kaspersky Security Center 13 Web Console in the installation wizard of Administration Server.
- Notifications are displayed about new releases of updates and patches (see section "Updating Administration Server" on page [1198](#)). You can install an update immediately or later at any time. You can now install patches for Administration Server via Kaspersky Security Center 13 Web Console.
- When working with tables, you can now specify the order and the width of columns, sort data, and specify the page size.
- You can now open any report by clicking its name.
- Kaspersky Security Center 13 Web Console is now available in the Korean language.
- A new section, Kaspersky announcements (see section "About Kaspersky announcements" on page [1365](#)), is available in the **MONITORING & REPORTING** menu. This section keeps you informed by providing information related to your version of Kaspersky Security Center and the managed applications installed on the managed devices. Kaspersky Security Center periodically updates the information in this section by removing outdated announcements and adding new information. However, you can disable Kaspersky announcements if you want.
- Implemented additional authentication after changing the settings of a user account (see section "Enabling account protection from unauthorized modification" on page [1015](#)). You can enable protecting a user account from unauthorized modification. If this option is enabled, modifying user account settings requires authorization by a user with modification rights.

Kaspersky Security Center

The following features are added to Kaspersky Security Center:

- Implemented two-step verification (see section "About two-step verification" on page [625](#)). You can enable two-step verification to reduce the risk of unauthorized access to the Administration Console (see section "Enabling two-step verification for your own account" on page [627](#)).
- You can send messages to Administration Server over the HTTP protocol. A reference guide (see section "API Reference Guide" on page [1395](#)) and a Python library for working with the OpenAPI of Administration Server are now available.
- You can issue a reserve certificate (see section "Configuring a reserve iOS MDM Server certificate" on page [204](#)) for use in iOS MDM configuration profiles, to ensure seamless switching of managed iOS devices after the iOS MDM Server certificate expires.
- The multi-tenancy applications folder is no longer displayed in Administration Console.

Kaspersky Security Center 13

This section provides information about using Kaspersky Security Center 13.

Information provided in Online Help

(https://click.kaspersky.com/?hl=en&link=online_help&pid=KSC&version=13.0.0&helpid=5022) may differ from information provided in documents shipped with the application; in this case, Online Help is considered up-to-date. You can proceed to Online Help by clicking links in the application interface, or by clicking the Online Help link in documents. Online Help can be updated without prior notice. You can switch between Online Help and Offline Help (see section "Switching between Online Help and Offline Help" on page [791](#)) if necessary.

In this chapter

About Kaspersky Security Center	30
Basic concepts	44
Architecture	58
Main installation scenario	59
Ports used by Kaspersky Security Center	65
About Kaspersky Security Center certificates	86
Schemas for data traffic and port usage	89
Deployment best practices	120
Installation of Kaspersky Security Center	213
Upgrading Kaspersky Security Center from a previous version	262
Initial setup of Kaspersky Security Center	264
Discovering networked devices	303
Licensing	317
Kaspersky applications. Centralized deployment	332
Kaspersky applications: licensing and activation	357
Configuring network protection	363
Updating Kaspersky Security Center and managed applications	405
Managing third-party applications on client devices	432
Monitoring and reporting	502
Adjustment of distribution points and connection gateways	587
Other routine tasks	596
Exporting events to SIEM systems	791
Using SNMP for sending statistics to third-party applications	809
Working in a cloud environment	820
Troubleshooting	878
Appendices	888
.....	949
Frequently Asked Questions	950

About Kaspersky Security Center

The section contains information about the purpose of Kaspersky Security Center and its main features and components.

Information provided in Online Help

(https://click.kaspersky.com/?hl=en&link=online_help&pid=KSC&version=13.0.0&helpid=5022) may differ from information provided in documents shipped with the application; in this case, Online Help is considered up-to-date. You can proceed to Online Help by clicking links in the application interface, or by clicking the Online Help link in documents. Online Help can be updated without prior notice. You can switch between Online Help and Offline Help (see section "Switching between Online Help and Offline Help" on page [791](#)) if necessary.

Kaspersky Security Center is designed for centralized execution of basic administration and maintenance tasks in an organization's network. The application provides the administrator access to detailed information about the organization's network security level; it allows configuring all the components of protection built using Kaspersky applications.

Kaspersky Security Center is an application aimed at corporate network administrators and employees responsible for protection of devices in a wide range of organizations.

Using Kaspersky Security Center, you can do the following:

- Create a hierarchy of Administration Servers to manage the organization's network, as well as networks at remote offices or client organizations.
The *client organization* is an organization whose anti-virus protection is ensured by the service provider.
- Create a hierarchy of administration groups to manage a selection of client devices as a whole.
- Manage an anti-virus protection system built based on Kaspersky applications.
- Create images of operating systems and deploy them on client devices over the network, as well as perform remote installation of applications by Kaspersky and other software vendors.
- Remotely manage applications by Kaspersky and other vendors installed on client devices. Install updates, find and fix vulnerabilities.
- Perform centralized deployment of license keys for Kaspersky applications to client devices, monitor their use, and renew licenses.
- Receive statistics and reports about the operation of applications and devices.
- Receive notifications about critical events during the operation of Kaspersky applications.
- Manage mobile devices.
- Manage encryption of information stored on the hard drives of devices and removable drives and users' access to encrypted data.
- Perform inventory of hardware connected to the organization's network.
- Centrally manage files moved to Quarantine or Backup by security applications, as well as manage files for which processing by security applications has been postponed.

In this chapter

Distribution kit	31
Hardware and software requirements	31
List of supported Kaspersky applications	41
About compatibility of Administration Server and Kaspersky Security Center 13 Web Console	42
About Kaspersky Security Center Cloud Console	43

Distribution kit

You can purchase the application through online stores of Kaspersky (for example, at <https://www.kaspersky.com>) or through partner companies.

If you purchase Kaspersky Security Center in an online store, you copy the application from the store's website. Information that is required for application activation is sent to you by email after payment.

Hardware and software requirements

Administration Server

Minimum hardware requirements:

- CPU with an operating frequency of 1 GHz or higher. For a 64-bit operating system, the minimum CPU frequency is 1.4 GHz.
- RAM: 4 GB.
- Available disk space: 10 GB. When Vulnerability and Patch Management is used, at least 100 GB of free disk space must be available.

For deployment in cloud environments, the requirements for Administration Server and database server are the same as the requirements for physical Administration Server (depending on how many devices you want to manage).

Software requirements:

- Microsoft® Data Access Components (MDAC) 2.8
- Microsoft Windows® DAC 6.0
- Microsoft Windows Installer 4.5

Operating system:

- Microsoft Windows 10 20H2 32-bit/64-bit
- Microsoft Windows 10 20H1 32-bit/64-bit
- Microsoft Windows 10 Enterprise 2019 LTSC 32-bit/64-bit
- Microsoft Windows 10 Enterprise 2016 LTSC 32-bit/64-bit

- Microsoft Windows 10 Enterprise 2015 LTSB 32-bit/64-bit
- Microsoft Windows 10 Pro RS5 (October 2018 Update, 1809) 32-bit/64-bit
- Microsoft Windows 10 Pro for Workstations RS5 (October 2018 Update, 1809) 32-bit/64-bit
- Microsoft Windows 10 Enterprise RS5 (October 2018 Update, 1809) 32-bit/64-bit
- Microsoft Windows 10 Education RS5 (October 2018 Update, 1809) 32-bit/64-bit
- Microsoft Windows 10 Pro 19H1 32-bit/64-bit
- Microsoft Windows 10 Pro for Workstations 19H1 32-bit/64-bit
- Microsoft Windows 10 Enterprise 19H1 32-bit/64-bit
- Microsoft Windows 10 Education 19H1 32-bit/64-bit
- Microsoft Windows 10 Home 19H2 32-bit/64-bit
- Microsoft Windows 10 Pro 19H2 32-bit/64-bit
- Microsoft Windows 10 Pro for Workstations 19H2 32-bit/64-bit
- Microsoft Windows 10 Enterprise 19H2 32-bit/64-bit
- Microsoft Windows 10 Education 19H2 32-bit/64-bit
- Microsoft Windows 8.1 Pro 32-bit/64-bit
- Microsoft Windows 8.1 Enterprise 32-bit/64-bit
- Microsoft Windows 8 Pro 32-bit/64-bit
- Microsoft Windows 8 Enterprise 32-bit/64-bit
- Microsoft Windows 7 Professional with Service Pack 1 and higher 32-bit/64-bit
- Microsoft Windows 7 Enterprise/Ultimate with Service Pack 1 and higher 32-bit/64-bit
- Windows Server® 2019 Standard 64-bit
- Windows Server 2019 Core 64-bit
- Windows Server 2019 Datacenter 64-bit
- Windows Server 2016 Server Standard RS3 (v1709) (LTSB/CBB) 64-bit
- Windows Server 2016 Server Datacenter RS3 (v1709) (LTSB/CBB) 64-bit
- Windows Server 2016 Server Core RS3 (v1709) (Installation Option) (LTSB/CBB) 64-bit
- Windows Server 2016 Standard (LTSB) 64-bit
- Windows Server 2016 Server Core (Installation Option) (LTSB) 64-bit
- Windows Server 2016 Datacenter (LTSB) 64-bit
- Windows Server 2012 R2 Standard 64-bit
- Windows Server 2012 R2 Server Core 64-bit
- Windows Server 2012 R2 Foundation 64-bit
- Windows Server 2012 R2 Essentials 64-bit
- Windows Server 2012 R2 Datacenter 64-bit
- Windows Server 2012 Standard 64-bit

- Windows Server 2012 Server Core 64-bit
- Windows Server 2012 Foundation 64-bit
- Windows Server 2012 Essentials 64-bit
- Windows Server 2012 Datacenter 64-bit
- Windows Server 2008 R2 Standard with Service Pack 1 and higher 64-bit
- Windows Server 2008 R2 with Service Pack 1 (all editions) 64-bit
- Windows Storage Server 2016 64-bit
- Windows Storage Server 2012 R2 64-bit
- Windows Storage Server 2012 64-bit

Database server (can be installed on a different device):

- Microsoft SQL Server® 2012 Express 64-bit
- Microsoft SQL Server 2014 Express 64-bit
- Microsoft SQL Server 2016 Express 64-bit
- Microsoft SQL Server 2017 Express 64-bit
- Microsoft SQL Server 2019 Express 64-bit
- Microsoft SQL Server 2014 (all editions) 64-bit
- Microsoft SQL Server 2016 (all editions) 64-bit
- Microsoft SQL Server 2017 (all editions) on Windows 64-bit
- Microsoft SQL Server 2017 (all editions) on Linux 64-bit
- Microsoft SQL Server 2019 (all editions) on Windows 64-bit (requires additional actions (see section "Selecting a DBMS" on page [129](#)))
- Microsoft SQL Server 2019 (all editions) on Linux 64-bit (requires additional actions (see section "Selecting a DBMS" on page [129](#)))
- MySQL Standard Edition 5.7 32-bit/64-bit
- MySQL Enterprise Edition 5.7 32-bit/64-bit
- All supported SQL Server editions in Amazon™ RDS and Microsoft Azure™ cloud platforms
- MariaDB Server 10.3 32-bit/64-bit with InnoDB storage engine

It is recommended to use MariaDB 10.3.22; if you use an earlier version, the Perform Windows update task might take more than one day to work.

The following virtualization platforms are supported:

- VMware™ vSphere™ 6.7
- VMware vSphere 7.1
- VMware Workstation 15 Pro

- VMware Workstation 16 Pro
- Microsoft Hyper-V® Server 2012 64-bit
- Microsoft Hyper-V Server 2012 R2 64-bit
- Microsoft Hyper-V Server 2016 64-bit
- Microsoft Hyper-V Server 2019 64-bit
- Citrix® XenServer® 7.1 LTSR
- Citrix XenServer 8.x
- Parallels Desktop® 16
- Oracle® VM VirtualBox 6.x (Windows guest login only)

The following SIEM systems are supported:

- HP (Micro Focus) ArcSight ESM 7.0
- HP (Micro Focus) ArcSight ESM 6.8
- IBM QRadar 7.4

Kaspersky Security Center 13 Web Console

Kaspersky Security Center 13 Web Console Server

Minimum hardware requirements:

- CPU: 4 cores, operating frequency of 2.5 GHz
- RAM: 8 GB
- Available disk space: 40 GB

One of the following operating systems:

- Microsoft Windows (64-bit versions only):
 - Microsoft Windows 10 20H2
 - Microsoft Windows 10 20H1
 - Microsoft Windows 10 Enterprise 2019 LTSC
 - Microsoft Windows 10 Enterprise 2016 LTSCB
 - Microsoft Windows 10 Enterprise 2015 LTSCB
 - Microsoft Windows 10 Pro RS5 (October 2018 Update, 1809)
 - Microsoft Windows 10 Pro for Workstations RS5 (October 2018 Update, 1809)
 - Microsoft Windows 10 Enterprise RS5 (October 2018 Update, 1809)
 - Microsoft Windows 10 Education RS5 (October 2018 Update, 1809)
 - Microsoft Windows 10 Pro 19H1
 - Microsoft Windows 10 Pro for Workstations 19H1
 - Microsoft Windows 10 Enterprise 19H1
 - Microsoft Windows 10 Education 19H1

- Microsoft Windows 10 Home 19H2
- Microsoft Windows 10 Pro 19H2
- Microsoft Windows 10 Pro for Workstations 19H2
- Microsoft Windows 10 Enterprise 19H2
- Microsoft Windows 10 Education 19H2
- Microsoft Windows 8.1 Pro
- Microsoft Windows 8.1 Enterprise
- Windows Server® 2019 Standard
- Windows Server 2019 Core
- Windows Server 2019 Datacenter
- Windows Server 2016 Server Standard RS3 (v1709) (LTSB/CBB)
- Windows Server 2016 Server Datacenter RS3 (v1709) (LTSB/CBB)
- Windows Server 2016 Server Core RS3 (v1709) (Installation Option) (LTSB/CBB)
- Windows Server 2016 Standard (LTSB)
- Windows Server 2016 Server Core (Installation Option) (LTSB)
- Windows Server 2016 Datacenter (LTSB)
- Windows Server 2012 R2 Standard
- Windows Server 2012 R2 Server Core
- Windows Server 2012 R2 Foundation
- Windows Server 2012 R2 Essentials
- Windows Server 2012 R2 Datacenter
- Windows Server 2012 Standard
- Windows Server 2012 Server Core
- Windows Server 2012 Foundation
- Windows Server 2012 Essentials
- Windows Server 2012 Datacenter
- Windows Storage Server 2016
- Windows Storage Server 2012 R2
- Windows Storage Server 2012
- Linux (64-bit versions only):
 - Debian GNU/Linux® 10.x (Buster)
 - Debian GNU/Linux 9.x (Stretch)
 - Ubuntu Server 20.04 LTS (Focal Fossa)
 - Ubuntu Server 18.04 LTS (Bionic Beaver)
 - CentOS 8.x

- CentOS 7.x
- Red Hat Enterprise Linux Server 8.x
- Red Hat Enterprise Linux Server 7.x
- SUSE Linux Enterprise Server 15 (all Service Packs)
- SUSE Linux Enterprise Server 12 (all Service Packs)
- Astra Linux Special, version 1.6
- Astra Linux Special, version 1.5
- Astra Linux Common Edition, version 2.12
- ALT 9.1
- ALT 8.3
- ALT SE 8

Client devices

For a client device, use of Kaspersky Security Center 13 Web Console requires only a browser.

The hardware and software requirements for the device are identical to the requirements of the browser that is used with Kaspersky Security Center 13 Web Console.

Browser:

- Mozilla Firefox™ 78 Extended Support Release
- Mozilla Firefox 78 or later
- Google Chrome™ 88 or later
- Safari 14 on macOS

iOS™ Mobile Device Management (iOS MDM) Server

Hardware requirements:

- CPU with an operating frequency of 1 GHz or higher. For a 64-bit OS, the minimum CPU frequency is 1.4 GHz.
- RAM: 2 GB.
- Available disk space: 2 GB.

Software requirements: Microsoft Windows (the version of the supported operating system is defined by the Administration Server requirements).

Exchange Mobile Device Server

All software and hardware requirements for Exchange Mobile Device Server are included in the requirements for Microsoft Exchange Server.

Compatibility with Microsoft Exchange Server 2007, Microsoft Exchange Server 2010, and Microsoft Exchange Server 2013 is supported.

Administration Console

Hardware requirements:

- CPU with an operating frequency of 1 GHz or higher. For a 64-bit OS, the minimum CPU frequency is 1.4 GHz.
- RAM: 512 MB.
- Available disk space: 1 GB.

Software requirements:

- Microsoft Windows operating system (supported version of the operating system is determined by the requirements of Administration Server), except for the following operating systems:
 - Windows Server 2012 Server Core 64-bit
 - Windows Server 2012 R2 Server Core 64-bit
 - Windows Server 2016 Server Core (Installation Option) (LTSB) 64-bit
 - Windows Server 2016 Server Datacenter RS3 (v1709) (LTSB/CBB) 64-bit
 - Windows Server 2016 Server Standard RS3 (v1709) (LTSB/CBB) 64-bit
 - Windows Server 2016 Server Core RS3 (v1709) (Installation Option) (LTSB/CBB) 64-bit
 - Windows Server 2019 Core 64-bit
- Microsoft Management Console 2.0
- Microsoft Windows Installer 4.5
- Microsoft Internet Explorer 10.0 running on:
 - Microsoft Windows Server 2008 R2 Service Pack 1
 - Microsoft Windows Server 2012
 - Microsoft Windows Server 2012 R2
 - Microsoft Windows 7 Service Pack 1
 - Microsoft Windows 8
 - Microsoft Windows 8.1
 - Microsoft Windows 10
- Microsoft Internet Explorer 11.0 running on:
 - Microsoft Windows Server 2012 R2
 - Microsoft Windows Server 2012 R2 Service Pack 1
 - Microsoft Windows Server 2016
 - Microsoft Windows Server 2019
 - Microsoft Windows 7 Service Pack 1
 - Microsoft Windows 8.1
 - Microsoft Windows 10
- Microsoft Edge running on Microsoft Windows 10

Network Agent

Minimum hardware requirements:

- CPU with an operating frequency of 1 GHz or higher. For a 64-bit OS, the minimum CPU frequency is 1.4 GHz.
- RAM: 512 MB.
- Available disk space: 1 GB.

Software requirements:

- Microsoft Windows Embedded POSReady 2009 with latest Service Pack 32-bit
- Microsoft Windows Embedded POSReady 7 32-bit/64-bit
- Microsoft Windows Embedded Standard 7 with Service Pack 1 32-bit/64-bit
- Microsoft Windows Embedded 8 Standard 32-bit/64-bit
- Microsoft Windows Embedded 8.1 Industry Pro 32-bit/64-bit
- Microsoft Windows Embedded 8.1 Industry Enterprise 32-bit/64-bit
- Microsoft Windows Embedded 8.1 Industry Update 32-bit/64-bit
- Microsoft Windows 10 20H2 32-bit/64-bit
- Microsoft Windows 10 20H1 32-bit/64-bit
- Microsoft Windows 10 Enterprise 2015 LTSP 32-bit/64-bit
- Microsoft Windows 10 Enterprise 2016 LTSP 32-bit/64-bit
- Microsoft Windows 10 Enterprise 2019 LTSC 32-bit/64-bit
- Microsoft Windows 10 Home RS5 (Oct 2018) 32-bit/64-bit
- Microsoft Windows 10 Pro RS5 (Oct 2018) 32-bit/64-bit
- Microsoft Windows 10 Pro for Workstations RS5 (Oct 2018) 32-bit/64-bit
- Microsoft Windows 10 Enterprise RS5 (Oct 2018) 32-bit/64-bit
- Microsoft Windows 10 Education RS5 (Oct 2018) 32-bit/64-bit
- Microsoft Windows 10 Home RS4 (April 2018 Update, 17134) 32-bit/64-bit
- Microsoft Windows 10 Pro RS4 (April 2018 Update, 17134) 32-bit/64-bit
- Microsoft Windows 10 Pro for Workstations RS4 (April 2018 Update, 17134) 32-bit/64-bit
- Microsoft Windows 10 Enterprise RS4 (April 2018 Update, 17134) 32-bit/64-bit
- Microsoft Windows 10 Education RS4 (April 2018 Update, 17134) 32-bit/64-bit
- Microsoft Windows 10 Home RS3 (Fall Creators Update, v1709) 32-bit/64-bit
- Microsoft Windows 10 Pro RS3 (Fall Creators Update, v1709) 32-bit/64-bit
- Microsoft Windows 10 Pro for Workstations RS3 (Fall Creators Update, v1709) 32-bit/64-bit
- Microsoft Windows 10 Enterprise RS3 (Fall Creators Update, v1709) 32-bit/64-bit
- Microsoft Windows 10 Education RS3 (Fall Creators Update, v1709) 32-bit/64-bit
- Microsoft Windows 10 Home 19H1 32-bit/64-bit

- Microsoft Windows 10 Pro 19H1 32-bit/64-bit
- Microsoft Windows 10 Pro for Workstations 19H1 32-bit/64-bit
- Microsoft Windows 10 Enterprise 19H1 32-bit/64-bit
- Microsoft Windows 10 Education 19H1 32-bit/64-bit
- Microsoft Windows 10 Home 19H2 32-bit/64-bit
- Microsoft Windows 10 Pro 19H2 32-bit/64-bit
- Microsoft Windows 10 Pro for Workstations 19H2 32-bit/64-bit
- Microsoft Windows 10 Enterprise 19H2 32-bit/64-bit
- Microsoft Windows 10 Education 19H2 32-bit/64-bit
- Microsoft Windows 8.1 Pro 32-bit/64-bit
- Microsoft Windows 8.1 Enterprise 32-bit/64-bit
- Microsoft Windows 8 Pro 32-bit/64-bit
- Microsoft Windows 8 Enterprise 32-bit/64-bit
- Microsoft Windows 7 Professional with Service Pack 1 and higher 32-bit/64-bit
- Microsoft Windows 7 Enterprise/Ultimate with Service Pack 1 and higher 32-bit/64-bit
- Microsoft Windows 7 Home Basic/Premium with Service Pack 1 and higher 32-bit/64-bit
- Microsoft Windows XP Professional for Embedded Systems 32-bit
- Microsoft Windows XP Professional Service Pack 3 and higher 32-bit
- Windows Small Business Server 2011 Essentials 64-bit
- Windows Small Business Server 2011 Premium Add-on 64-bit
- Windows Small Business Server 2011 Standard 64-bit
- Windows MultiPoint™ Server 2011 Standard/Premium 64-bit
- Windows MultiPoint™ Server 2012 Standard/Premium 64-bit
- Windows Server 2008 R2 Standard Service Pack 1 and higher 64-bit
- Windows Server 2008 R2 Datacenter Service Pack 1 and higher 64-bit
- Windows Server 2008 R2 Enterprise Service Pack 1 and higher 64-bit
- Windows Server 2008 R2 Foundation with Service Pack 1 and higher 64-bit
- Windows Server 2008 R2 Service Pack 1 and higher Core Mode 64-bit
- Windows Server 2008 R2 Service Pack 1 (all editions) 64-bit
- Windows Server 2012 Server Core 64-bit
- Windows Server 2012 Datacenter 64-bit
- Windows Server 2012 Essentials 64-bit
- Windows Server 2012 Foundation 64-bit
- Windows Server 2012 Standard 64-bit
- Windows Server 2012 R2 Server Core 64-bit

- Windows Server 2012 R2 Datacenter 64-bit
- Windows Server 2012 R2 Essentials 64-bit
- Windows Server 2012 R2 Foundation 64-bit
- Windows Server 2012 R2 Standard 64-bit
- Windows Server 2016 Datacenter (LTSB) 64-bit
- Windows Server 2016 Standard (LTSB) 64-bit
- Windows Server 2016 Server Core (Installation Option) (LTSB) 64-bit
- Windows Server 2016 Server Datacenter RS3 (v1709) (LTSB/CBB) 64-bit
- Windows Server 2016 Server Standard RS3 (v1709) (LTSB/CBB) 64-bit
- Windows Server 2016 Server Core RS3 (v1709) (Installation Option) (LTSB/CBB) 64-bit
- Windows Server 2019 Standard 64-bit
- Windows Server 2019 Core 64-bit
- Windows Server 2019 Datacenter 64-bit
- Windows Storage Server 2016 64-bit
- Windows Storage Server 2012 64-bit
- Windows Storage Server 2012 R2 64-bit
- Debian GNU/Linux® 10.x (Buster) 32-bit/64-bit
- Debian GNU/Linux 9.x (Stretch) 32-bit/64-bit
- Ubuntu Server 20.04 LTS (Focal Fossa) 32-bit/64-bit
- Ubuntu Server 18.04 LTS (Bionic Beaver) 32-bit/64-bit
- Ubuntu Desktop 20.04 LTS (Focal Fossa) 32-bit/64-bit
- Ubuntu Desktop 18.04 LTS (Bionic Beaver) 32-bit/64-bit
- CentOS 8.x 64-bit
- CentOS 7.x 64-bit
- Red Hat Enterprise Linux® Server 8.x 64-bit
- Red Hat Enterprise Linux Server 7.x 64-bit
- SUSE Linux Enterprise Server 15 (all Service Packs) 64-bit
- SUSE Linux Enterprise Desktop 15 (all Service Packs) 64-bit
- SUSE Linux Enterprise Server 12 (all Service Packs) 64-bit
- Astra Linux Special, version 1.6
- Astra Linux Special, version 1.5
- Astra Linux Common Edition, version 2.12
- ALT 9.1
- ALT 8.3
- ALT SE 8

- OS X 10.10 (Yosemite)
- OS X 10.11 (El Capitan)
- macOS Sierra (10.12)
- macOS High Sierra (10.13)
- macOS Mojave (10.14)
- macOS Catalina (10.15)
- macOS Big Sur (11.x)

The following virtualization platforms are supported:

- VMware Workstation 16 Pro
- VMware Workstation 15 Pro
- Microsoft Hyper-V Server 2012 64-bit
- Microsoft Hyper-V Server 2012 R2 64-bit
- Microsoft Hyper-V Server 2016 64-bit
- Microsoft Hyper-V Server 2019 64-bit
- Citrix XenServer 7.1 LTSR
- Citrix XenServer 8.x
- VMware vSphere 7.1
- VMware vSphere 6.7

On the devices running Windows 10 version RS4 or RS5, Kaspersky Security Center might be unable to detect some vulnerabilities in folders where case sensitivity is enabled.
In Microsoft Windows XP, Network Agent might not perform some operations correctly (see section "Deploying Network Agent and the security application" on page 150).
Network Agent for Linux and Network Agent for macOS are provided together with Kaspersky security applications for these operating systems.

List of supported Kaspersky applications

Kaspersky Security Center supports centralized deployment and management of all Kaspersky applications that are currently supported (please refer to the Product Support Lifecycle webpage <https://support.kaspersky.com/corporate/lifecycle> for the versions of the applications):

- **For workstations:**
 - Kaspersky Endpoint Security for Windows (workstation mode)
 - Kaspersky Endpoint Security for Linux (Desktop Protection)
 - Kaspersky Endpoint Security for Linux ARM64 Edition
 - Kaspersky Endpoint Security for Mac (macOS 11.0 is not supported)
 - Kaspersky Endpoint Agent

- Kaspersky Embedded Systems Security for Windows
- **Kaspersky Industrial Cybersecurity:**
 - Kaspersky Industrial Cybersecurity for Nodes
 - Kaspersky Industrial Cybersecurity for Linux Nodes
 - Kaspersky Industrial Cybersecurity for Networks (centralized deployment is not supported)
- **For mobile devices:** Kaspersky Security for Mobile (Kaspersky Endpoint Security for Android)
- **For file servers:**
 - Kaspersky Endpoint Security for Windows (file server mode)
 - Kaspersky Security for Windows Server
 - Kaspersky Endpoint Security for Linux (Server Protection)
- **For virtual machines:**
 - Kaspersky Security for Virtualization Light Agent
 - Kaspersky Security for Virtualization Agentless
- **For mail systems and SharePoint/collaboration servers (centralized deployment is not supported):**
 - Kaspersky Security for Linux Mail Server
 - Kaspersky Secure Mail Gateway
 - Kaspersky Security for Microsoft Exchange Servers
 - Kaspersky Security for SharePoint Server
- **For detection of targeted attacks:**
 - Kaspersky Anti Targeted Attack Platform
 - Kaspersky Sandbox
 - KasperskyOS for Thin Client

About compatibility of Administration Server and Kaspersky Security Center 13 Web Console

You can install and upgrade Kaspersky Security Center Administration Server and Kaspersky Security Center Web Console independently. You must ensure that the version of the installed Kaspersky Security Center Web Console is compatible with the version of Administration Server to which you connect.

Kaspersky Security Center 13 Administration Server supports:

- Kaspersky Security Center 13 Web Console
- Kaspersky Security Center 12.2 Web Console
- Kaspersky Security Center 12.1 Web Console

We highly recommend that you use the latest version of Kaspersky Security Center Web Console; otherwise, the functionality of Kaspersky Security Center is limited.

If two-step verification (see section "About two-step verification" on page [625](#)) is set up for a user account on Kaspersky Security Center 13 Administration Server, the user will not be able to connect to the server by using Kaspersky Security Center Web Console of versions 12.1 or 12.2.

Kaspersky Security Center 13 Web Console supports:

- Kaspersky Security Center 13 Administration Server
- Kaspersky Security Center 12.2 Administration Server
- Kaspersky Security Center 12.1 Administration Server

About Kaspersky Security Center Cloud Console

You can use Kaspersky Security Center in the following ways:

- As an on-premises application
In this case you install Kaspersky Security Center, including Administration Server, on a local device and manage the network security system through the Microsoft Management Console-based Administration Console or Kaspersky Security Center Web Console.
- As a cloud service
In this case Kaspersky Security Center is installed for you in the cloud environment and Kaspersky gives you access to the Administration Server as a service. You manage the network security system through the cloud-based Administration Console named Kaspersky Security Center Cloud Console. This console has an interface similar to the interface of Kaspersky Security Center Web Console.

The interface and documentation of Kaspersky Security Center Cloud Console are available in the following languages:

- English
- French
- German
- Italian
- Portuguese (Brazil)
- Russian
- Spanish
- Spanish (LATAM)

See more information about Kaspersky Security Center Cloud Console

https://click.kaspersky.com/?hl=en&link=online_help&pid=KSC&version=1.0.0&helpid=195506 and its features https://click.kaspersky.com/?hl=en&link=online_help&pid=KSC&version=1.0.0&helpid=187522 in the Kaspersky Security Center Cloud Console documentation

https://click.kaspersky.com/?hl=en&link=online_help&pid=KSC&version=1.0.0&helpid=5022.

Basic concepts

This section explains basic concepts related to Kaspersky Security Center.

In this chapter

Administration Server	44
Hierarchy of Administration Servers	45
Virtual Administration Server	46
Mobile Device Server.....	47
Web Server	47
Network Agent	48
Administration groups	49
Managed device	49
Unassigned device	49
Administrator's workstation.....	50
Management plug-in.....	50
Management web plug-in	50
Policies.....	51
Policy profiles.....	52
Tasks	52
Task scope	53
How local application settings relate to policies	54
Distribution point	55
Connection gateway	57

Administration Server

Kaspersky Security Center components enable remote management of Kaspersky applications installed on client devices.

Devices with the Administration Server component installed will be referred to as *Administration Servers* (also referred to as *Servers*). Administration Servers must be protected, including physical protection, against any unauthorized access.

Administration Server is installed on a device as a service with the following set of attributes:

- With the name "Kaspersky Security Center Administration Server"
- Set to start automatically when the operating system starts

- With the **Local System** account or the user account selected during the installation of Administration Server

Administration Server performs the following functions:

- Storage of the administration groups' structure
- Storage of information about the configuration of client devices
- Organization of repositories for application distribution packages
- Remote installation of applications to client devices and removal of applications
- Updating application databases and software modules of Kaspersky applications
- Management of policies and tasks on client devices
- Storage of information about events that have occurred on client devices
- Generation of reports on the operation of Kaspersky applications
- Deployment of license keys to client devices and storing information about the license keys
- Forwarding notifications about the progress of tasks (such as detection of viruses on a client device)

Naming Administration Servers in the application interface

In the interface of the MMC-based Administration Console and Kaspersky Security Center 13 Web Console, Administration Servers can have the following names:

- Name of the Administration Server device, for example: "*device_name*" or "Administration Server: *device_name*".
- IP address of the Administration Server device, for example: "*IP_address*" or "Administration Server: *IP_address*".
- Secondary Administration Servers and virtual Administration Servers have custom names that you specify when you connect a virtual or a secondary Administration Server to the primary Administration Server.
- If you use Kaspersky Security Center 13 Web Console installed on a Linux device, the application displays the names of the Administration Servers that you specified as trusted in the response file (see section "Kaspersky Security Center 13 Web Console installation parameters" on page [970](#)).

You can connect to Administration Server by using Administration Console (see section "Administration Server and Administration Console" on page [111](#)) or Kaspersky Security Center 13 Web Console.

See also:

Main installation scenario	59
Scenario: Deployment for cloud environment.....	821
Installation of Kaspersky Security Center	213
Interaction of Kaspersky Security Center components and security applications: more information.....	108

Hierarchy of Administration Servers

Administration Servers can be arranged in a hierarchy. Each Administration Server can have several secondary Administration Servers (referred to as *secondary Servers*) on different nesting levels of the hierarchy. The nesting

level for secondary Servers is unrestricted. The administration groups of the primary Administration Server will then include the client devices of all secondary Administration Servers. Thus, isolated and independent sections of networks can be managed by different Administration Servers which are in turn managed by the primary Server.

Virtual Administration Servers (see section "*Virtual Administration Server*" on page [46](#)) are a particular case of secondary Administration Servers.

The hierarchy of Administration Servers can be used to do the following:

- Decrease the load on Administration Server (compared to a single installed Administration Server for an entire network).
- Decrease intranet traffic and simplify work with remote offices. You do not have to establish connections between the primary Administration Server and all networked devices, which may be located, for example, in different regions. It is sufficient to install a secondary Administration Server in each network segment, distribute devices among administration groups of secondary Servers, and establish connections between the secondary Servers and the primary Server over fast communication channels.
- Distribute responsibilities among the anti-virus security administrators. All capabilities for centralized management and monitoring of the anti-virus security status in corporate networks remain available.
- How service providers use Kaspersky Security Center. The service provider only needs to install Kaspersky Security Center and Kaspersky Security Center 13 Web Console. To manage a large number of client devices of various organizations, a service provider can add virtual Administration Servers to the hierarchy of Administration Servers.

Each device included in the hierarchy of administration groups can be connected to one Administration Server only. You must independently monitor the connection of devices to Administration Servers. Use the feature for device search in administration groups of different Servers based on network attributes.

See also:

Hierarchy of Administration Servers: primary Administration Server and secondary Administration Server [114](#)

Virtual Administration Server

Virtual Administration Server (also referred to as *virtual Server*) is a component of Kaspersky Security Center intended for managing anti-virus protection of the network of a client organization.

Virtual Administration Server is a particular case of a secondary Administration Server and has the following restrictions as compared with a physical Administration Server:

- Virtual Administration Server can be created only on a primary Administration Server.
- Virtual Administration Server uses the primary Administration Server database in its operation. Data backup and restoration tasks, as well as update scan and download tasks, are not supported on a virtual Administration Server.
- Virtual Server does not support creation of secondary Administration Servers (including virtual Servers).

In addition, virtual Administration Server has the following restrictions:

- In the virtual Administration Server properties window, the number of sections is limited.
- To install Kaspersky applications remotely on client devices managed by the virtual Administration Server, you must make sure that Network Agent is installed on one of the client devices, in order to ensure communication with the virtual Administration Server. Upon first connection to the virtual Administration Server, the device is automatically assigned as a distribution point, thus functioning as a connection gateway between the client devices and the virtual Administration Server.
- A virtual Server can poll the network only through distribution points.
- To restart a malfunctioning virtual Server, Kaspersky Security Center restarts the primary Administration Server and all virtual Administration Servers.

The administrator of a virtual Administration Server has all privileges on this particular virtual Server.

Mobile Device Server

Mobile Device Server is a component of Kaspersky Security Center that provides access to mobile devices and allows managing them through Administration Console. Mobile Device Server receives information about mobile devices and stores their profiles.

There are two types of Mobile Device Server:

- Exchange Mobile Device Server. This is installed on a device where a Microsoft Exchange server has been installed, allowing data retrieval from the Microsoft Exchange server and data transmission to Administration Server. This Mobile Device Server is used for managing mobile devices that support Exchange ActiveSync protocol.
- iOS MDM Server. This Mobile Device Server is used for managing mobile devices that support Apple® Push Notification service (APNs).

Mobile Device Servers of Kaspersky Security Center allow you to manage the following objects:

- An individual mobile device.
- Several mobile devices.
- Several mobile devices connected to a cluster of servers simultaneously. After connecting to a cluster of servers, the mobile devices server installed in this cluster is displayed in Administration Console as a single server.

Web Server

Kaspersky Security Center *Web Server* (hereinafter also referred to as *Web Server*) is a component of Kaspersky Security Center that is installed together with Administration Server. Web Server is designed for transmission, over a network, of stand-alone installation packages, iOS MDM profiles, and files from a shared folder.

When you create a stand-alone installation package, it is automatically published on Web Server. The link for downloading the stand-alone package is displayed in the list of created stand-alone installation packages. If necessary, you can cancel publication of the stand-alone package or you can publish it on Web Server again.

When you create an iOS MDM profile for a user's mobile device, it is also automatically published on Web Server. The published profile is automatically deleted from Web Server as soon as it is successfully installed on the user's mobile device (see section "Adding iOS mobile devices to the list of managed devices" on page [744](#)).

The shared folder is used for storage of information that is available to all users whose devices are managed through the Administration Server. If a user has no direct access to the shared folder, he or she can be given information from that folder by means of Web Server.

To provide users with information from a shared folder by means of Web Server, the administrator must create a subfolder named "public" in the shared folder and paste the relevant information into it.

The syntax of the information transfer link is as follows:

```
https://<Web Server name>:<HTTPS port>/public/<object>
```

where:

- <Web Server name> is the name of Kaspersky Security Center Web Server.
- <HTTPS port> is an HTTPS port of Web Server that has been defined by the Administrator. The HTTPS port can be set in the **Web Server** section of the properties window of Administration Server. The default port number is 8061.
- <object> is the subfolder or file to which the user has access.

The administrator can send the new link to the user in any convenient way, such as by email.

By using this link, the user can download the required information to a local device.

Network Agent

Interaction between Administration Server and devices is performed by the *Network Agent* component of Kaspersky Security Center. Network Agent must be installed on all devices on which Kaspersky Security Center is used to manage Kaspersky applications.

Network Agent is installed on a device as a service, with the following set of attributes:

- With the name "Kaspersky Security Center 13 Network Agent"
- Set to start automatically when the operating system starts
- Using the LocalSystem account

A device that has Network Agent installed is called a *managed device* or *device*.

You can install Network Agent on a Windows, Linux, or Mac device. You can get the component from one of the following sources:

- Installation package in Administration Server storage (you must have Administration Server installed)
- Installation package located at Kaspersky web servers (see section "Receiving up-to-date versions of applications" on page [351](#))

You do not have to install Network Agent on the device where you install Administration Server, because the server version of Network Agent is automatically installed together with Administration Server.

The name of the process that Network Agent starts is *klagent.exe*.

Network Agent synchronizes the managed device with the Administration Server. We recommend that you set the synchronization interval (also referred to as the *heartbeat*) to 15 minutes per 10 000 managed devices.

See also:

Network Agent policy settings	665
-------------------------------------	---------------------

Administration groups

An *administration group* (hereinafter also referred to as *group*) is a logical set of managed devices combined on the basis of a specific trait for the purpose of managing the grouped devices as a single unit within Kaspersky Security Center.

All managed devices within an administration group are configured to do the following:

- Use the same application settings (which you can specify in group policies).
- Use a common operating mode for all applications through the creation of group tasks with a specified collection of settings. Examples of group tasks include creating and installing a common installation package, updating the application databases and modules, scanning the device on demand, and enabling real-time protection.

A managed device can belong to only one administration group.

You can create hierarchies that have any degree of nesting for Administration Servers and groups. A single hierarchy level can include secondary and virtual Administration Servers, groups, and managed devices. You can move devices from one group to another without physically moving them. For example, if a worker's position in the enterprise changes from that of accountant to developer, you can move this worker's computer from the Accountants administration group to the Developers administration group. Thereafter, the computer will automatically receive the application settings required for developers.

Managed device

A *managed device* is a computer running Windows, Linux, or macOS on which Network Agent is installed, or a mobile device on which a Kaspersky security application is installed. You can manage such devices by creating tasks and policies for applications installed on these devices. You can also collect reports from managed devices.

You can make a non-mobile managed device function as a distribution point and as a connection gateway.

A device can be managed by only one Administration Server. One Administration Server can manage up to 100 000 devices, including mobile devices.

Unassigned device

An *unassigned device* is a device on the network that has not been included in any administration group. You can perform some actions on unassigned devices, for example, move them to administration groups or install applications on them.

When a new device is discovered on your network, this device goes to the Unassigned devices administration group. You can configure rules for devices to be moved automatically to other administration groups after the devices are discovered.

Administrator's workstation

Devices on which *Administration Console* is installed are referred to as *administrator's workstations*. Administrators can use these devices for centralized remote management of Kaspersky applications installed on client devices.

After Administration Console is installed on your device, its icon appears, allowing you to start Administration Console. Find it in the **Start** → **Programs** → **Kaspersky Security Center** menu.

There are no restrictions on the number of administrator's workstations. From any administrator's workstation you can manage administration groups of several Administration Servers on the network at once. You can connect an administrator's workstation to an Administration Server (physical or virtual) of any level of the hierarchy.

You can include an administrator's workstation in an administration group as a client device.

Within the administration groups of any Administration Server, the same device can function as an Administration Server client, an Administration Server, or an administrator's workstation.

Management plug-in

Kaspersky applications are managed through Administration Console by using a dedicated component named *management plug-in*. Each Kaspersky application that can be managed through Kaspersky Security Center includes a management plug-in.

Using the application management plug-in, you can perform the following actions in Administration Console:

- Creating and editing application policies and settings, as well as the settings of application tasks.
- Obtaining information about application tasks, application events, as well as application operation statistics received from client devices.

Management web plug-in

A special component—the *management web plug-in*—is used for remote administration of Kaspersky software by means of Kaspersky Security Center 13 Web Console. Hereinafter, a management web plug-in is also referred to as a *management plug-in*. A management plug-in is an interface between Kaspersky Security Center 13 Web Console and a specific Kaspersky application. With a management plug-in, you can configure tasks and policies for the application.

The management plug-in provides the following:

- Interface for creating and editing application tasks (on page [1078](#)) and settings
- Interface for creating and editing policies and policy profiles (on page [1110](#)) for remote and centralized configuration of Kaspersky applications and devices
- Transmission of events generated by the application
- Kaspersky Security Center 13 Web Console functions for displaying operational data and events of the application, and statistics relayed from client devices

Policies

A *policy* is a set of Kaspersky application settings that are applied to an administration group (see section "Administration groups" on page [49](#)) and its subgroups. You can install several Kaspersky applications (see section "List of Kaspersky applications supported by Kaspersky Security Center 13 Web Console" on page [957](#)) on the devices of an administration group. Kaspersky Security Center provides a single policy for each Kaspersky application in an administration group. A policy has one of the following statuses:

Table 1. The status of the policy

Status	Description
Active	The current policy that is applied to the device. Only one policy may be active for a Kaspersky application in each administration group. Devices apply the settings values of an active policy for a Kaspersky application.
Inactive	A policy that is not currently applied to a device.
Out-of-office	If this option is selected, the policy becomes active when the device leaves the corporate network.

Policies function according to the following rules:

- Multiple policies with different values can be configured for a single application.
- Only one policy can be active for the current application.
- You can activate an inactive policy when a specific event occurs. For example, you can enforce stricter anti-virus protection settings during virus outbreaks.
- A policy can have child policies.

Generally, you can use policies as preparations for emergency situations, such as a virus attack. For example, if there is an attack via flash drives, you can activate a policy that blocks access to flash drives. In this case, the current active policy automatically becomes inactive.

In order to prevent maintaining multiple policies, for example, when different occasions assume changing of several settings only, you may use policy profiles.

A *policy profile* is a named subset of policy settings values that replaces the settings values of a policy. A policy profile affects the effective settings formation on a managed device. *Effective settings* are a set of policy settings, policy profile settings, and local application settings that are currently applied for the device.

Policy profiles function according to the following rules:

- A policy profile takes an effect when a specific activation condition occurs.
- Policy profiles contain values of settings that differ from the policy settings.
- Activation of a policy profile changes the effective settings of the managed device.
- A policy can include a maximum of 100 policy profiles.

Policy profiles

Sometimes it may be necessary to create several instances of a single policy for different administration groups; you might also want to modify the settings of those policies centrally. These instances might differ by only one or two settings. For example, all the accountants in an enterprise work under the same policy—but senior accountants are allowed to use flash drives, while junior accountants are not. In this case, applying policies to devices only through the hierarchy of administration groups can be inconvenient.

To help you avoid creating several instances of a single policy, Kaspersky Security Center allows you to create *policy profiles*. Policy profiles are necessary if you want devices within a single administration group to run under different policy settings.

A policy profile is a named subset of policy settings. This subset is distributed on target devices together with the policy, supplementing it under a specific condition called the *profile activation condition*. Profiles only contain settings that differ from the "basic" policy, which is active on the managed device. Activation of a profile modifies the settings of the "basic" policy that were initially active on the device. The modified settings take values that have been specified in the profile.

Tasks

Kaspersky Security Center manages Kaspersky security applications installed on devices by creating and running *tasks*. Tasks are required for installing, launching, and stopping applications, scanning files, updating databases and software modules, and performing other actions on applications.

Tasks for a specific application can be created only if the management plug-in for that application is installed.

Tasks can be performed on the Administration Server and on devices.

The following tasks are performed on the Administration Server:

- Automatic distribution of reports
- Downloading of updates to the repository of the Administration Server
- Backup of Administration Server data
- Maintenance of the database
- Windows Update synchronization
- Creation of an installation package based on the operating system (OS) image of a reference device

The following types of tasks are performed on devices:

- *Local tasks*—Tasks that are performed on a specific device

Local tasks can be modified either by the administrator, by using Administration Console tools, or by the user of a remote device (for example, through the security application interface). If a local task has been modified simultaneously by the administrator and the user of a managed device, the changes made by the administrator will take effect because they have a higher priority.

- *Group tasks*—Tasks that are performed on all devices of a specific group

Unless otherwise specified in the task properties, a group task also affects all subgroups of the selected group. A group task also affects (optionally) devices that have been connected to secondary and virtual Administration Servers deployed in the group or any of its subgroups.

- *Global tasks*—Tasks that are performed on a set of devices, regardless of whether they are included in any group

For each application, you can create any number of group tasks, global tasks, or local tasks.

You can make changes to the settings of tasks, view the progress of tasks, and copy, export, import, and delete tasks.

A task is started on a device only if the application for which the task was created is running.

Results of tasks are saved in the Microsoft Windows event log and the Kaspersky Security Center event log (see section "Using event selections" on page [1289](#)), both centrally on the Administration Server and locally on each device.

Do not include private data in task settings. For example, avoid specifying the domain administrator password.

Task scope

The *scope of a task* (see section "About tasks" on page [1078](#)) is the set of devices on which the task is performed. The types of scope are as follows:

- For a *local task*, the scope is the device itself.
- For an *Administration Server task*, the scope is the Administration Server.
- For a *group task*, the scope is the list of devices included in the group.

When creating a *global task*, you can use the following methods to specify its scope:

- Specifying certain devices manually.

You can use an IP address (or IP range), NetBIOS name, or DNS name as the device address.

- Importing a list of devices from a .txt file with the device addresses to be added (each address must be placed on an individual line).

If you import a list of devices from a file or create a list manually, and if devices are identified by their names, the list can only contain devices for which information has already been entered into the Administration Server database. Moreover, the information must have been entered when those devices were connected or during device discovery.

- Specifying a device selection.

Over time, the scope of a task changes as the set of devices included in the selection change. A selection of devices can be made on the basis of device attributes, including software installed on a device, and on the basis of tags assigned to devices. Device selection is the most flexible way to specify the scope of a task.

Tasks for device selections are always run on a schedule by the Administration Server. These tasks cannot be run on devices that lack connection to the Administration Server. Tasks whose scope is specified by using other methods are run directly on devices and therefore do not depend on the device connection to the Administration Server.

Tasks for device selections are not run on the local time of a device; instead, they are run on the local time of the Administration Server. Tasks whose scope is specified by using other methods are run on the local time of a device.

How local application settings relate to policies

You can use policies to set identical values of the application settings for all devices in a group.

The values of the settings that a policy specifies can be redefined for individual devices in a group by using local application settings. You can set only the values of settings that the policy allows to be modified, that is, the unlocked settings.

The value of a setting that the application uses on a client device (see the figure below) is defined by the lock (🔒) position for that setting in the policy:

- If a setting modification is locked, the same value (defined in the policy) is used on all client devices.
- If a setting modification is unlocked, the application uses a local setting value on each client device instead of the value specified in the policy. The setting can then be changed in the local application settings.



Figure 1. Policy and local application settings

This means that, when a task is run on a client device, the application applies settings that have been defined in two different ways:

- By task settings and local application settings, if the setting is not locked against changes in the policy.
- By the group policy, if the setting is locked against changes.

Local application settings are changed after the policy is first applied in accordance with the policy settings.

Distribution point

Distribution point (previously known as update agent) is a device with Network Agent installed that is used for distribution of updates, remote installation of applications, and retrieval of information about networked devices. A distribution point can perform the following functions:

- Distribute updates and installation packages received from the Administration Server to client devices within the group (including by means such as multicasting using UDP). Updates can be received either from the Administration Server or from Kaspersky update servers. In the latter case, an update task must be created for the distribution point (see section "Automatic installation of Kaspersky Endpoint Security updates on devices" on page [441](#)).

The *Download updates to the repositories of distribution points* task works only on distribution point devices running Windows. Distribution point devices running Linux or macOS cannot download updates from Kaspersky update servers.

If one or more devices running Linux or macOS are within the scope of the *Download updates to the repositories of distribution points* task, the task completes with the *Failed* status, even if it has successfully completed on all Windows devices.

Distribution points accelerate update distribution and free up Administration Server resources.

- Distribute policies and group tasks through multicasting using UDP.
- Act as a gateway for connection to the Administration Server for devices in an administration group (see section "Using a distribution point as connection gateway" on page [594](#)).

If a direct connection between managed devices within the group and the Administration Server cannot be established, you can use the distribution point as connection gateway to the Administration Server for this group. In this case, managed devices connect to the connection gateway, which in turn connects to the Administration Server.

The presence of a distribution point that functions as connection gateway does not block the option of a direct connection between managed devices and the Administration Server. If the connection gateway is not available, but direct connection with the Administration Server is technically possible, managed devices are connected to the Administration Server directly.

- Poll the network to detect new devices and update information about existing ones. A distribution point can apply the same device discovery methods as the Administration Server.
- Perform remote installation of third-party software and Kaspersky applications through Microsoft Windows tools, including installation on client devices without Network Agent.

This feature allows you to remotely transfer Network Agent installation packages to client devices located on networks to which the Administration Server has no direct access.

- Act as a proxy server participating in the Kaspersky Security Network.

You can enable KSN Proxy on distribution point side (see section "Assigning a device a distribution point manually" on page [427](#)) to make the device act as KSN Proxy. In this case, KSN proxy service (ksnproxy) is run on the device (see section "Changes in the system after Administration Server installation on the device" on page [259](#)).

Files are transmitted from the Administration Server to a distribution point over HTTP or, if SSL connection is enabled, over HTTPS. Using HTTP or HTTPS results in a higher level of performance, compared to SOAP, through cutting traffic.

Devices with Network Agent installed can be assigned distribution points either manually (by the administrator) (see section "Assigning a device a distribution point manually" on page [427](#)), or automatically (by the Administration Server). The full list of distribution points for specified administration groups is displayed in the report about the list of distribution points.

The scope of a distribution point is the administration group to which it has been assigned by the administrator, as well as its subgroups of all levels of embedding. If multiple distribution points have been assigned in the hierarchy of administration groups, Network Agent on the managed device connects to the nearest distribution point in the hierarchy.

A network location can also be the scope of distribution points. The network location is used for manual creation of a set of devices to which the distribution point will distribute updates. Network location can be determined only for devices running a Windows operating system.

If distribution points are assigned automatically by the Administration Server, it assigns them by broadcast domains, not by administration groups. This occurs when all broadcast domains are known. Network Agent exchanges messages with other Network Agents in the same subnet and then sends Administration Server information about itself and other Network Agents. Administration Server can use that information to group Network Agents by broadcast domains. Broadcast domains are known to Administration Server after more than 70% Network Agents in administration groups are polled. Administration Server polls broadcast domains every two hours. After distribution points are assigned by broadcast domains, they cannot be re-assigned by administration groups.

If the administrator manually assigns distribution points, they can be assigned to administration groups or network locations.

Network Agents with the active connection profile do not participate in broadcast domain detection. Kaspersky Security Center assigns each Network Agent a unique IP multicast address that differs from every other address. This allows you to avoid network overload that might occur due to IP overlaps. The feature of unique address assignment functions in Kaspersky Security Center 10 Service Pack 3 and later versions. IP multicast addresses that were assigned in previous versions of the application will not be changed.

If two or more distribution points are assigned to a single network area or to a single administration group, one of them becomes the active distribution point, and the rest become standby distribution points. The active distribution point downloads updates and installation packages directly from the Administration Server, while standby distribution points receive updates from the active distribution point only. In this case, files are downloaded once from the Administration Server and then are distributed among distribution points. If the active distribution point becomes unavailable for any reason, one of the standby distribution points becomes active. The Administration Server automatically assigns a distribution point to act as standby.

The distribution point status (*Active/Standby*) is displayed with a check box in the `klagchk` (see section "Manually checking the connection between a client device and the Administration Server. `klagchk` utility" on page [643](#)) report.

A distribution point requires at least 4 GB of free disk space. If the free disk space of the distribution point is less than 2 GB, Kaspersky Security Center creates an incident with the *Warning* importance level. The incident will be published in the device properties, in the **Incidents** section.

Running remote installation tasks on a device assigned as a distribution point requires additional free disk space. The volume of free disk space must exceed the total size of all installation packages to be installed.

Running any updating (patching) tasks and vulnerability fix tasks on a device assigned as a distribution point requires additional free disk space. The volume of free disk space must be at least twice the total size of all patches to be installed.

Devices functioning as distribution points must be protected, including physical protection, against any unauthorized access.

Connection gateway

A connection gateway is a Network Agent acting in a special mode. A connection gateway accepts connections from other Network Agents and tunnels them to the Administration Server through its own connection with the Server. Unlike an ordinary Network Agent, a connection gateway waits for connections from the Administration Server rather than establishes connections to the Administration Server.

A connection gateway can communicate up to 10,000 devices.

You have two options for using connection gateways:

- We recommend that you install a connection gateway in a demilitarized zone (DMZ). For other Network Agents installed on out-of-office devices (see section "About connecting out-of-office devices" on page [285](#)), you need to specially configure a connection to Administration Server through the connection gateway.

A connection gateway does not in any way modify or process data that is transmitted from Network Agents to Administration Server. Moreover, it does not write this data into any buffer and therefore cannot accept data from a Network Agent and later forward it to Administration Server. If Network Agent attempts to connect to Administration Server through the connection gateway, but the connection gateway cannot connect to Administration Server, Network Agent perceives this as if Administration Server is inaccessible. All data remains on Network Agent (not on the connection gateway).

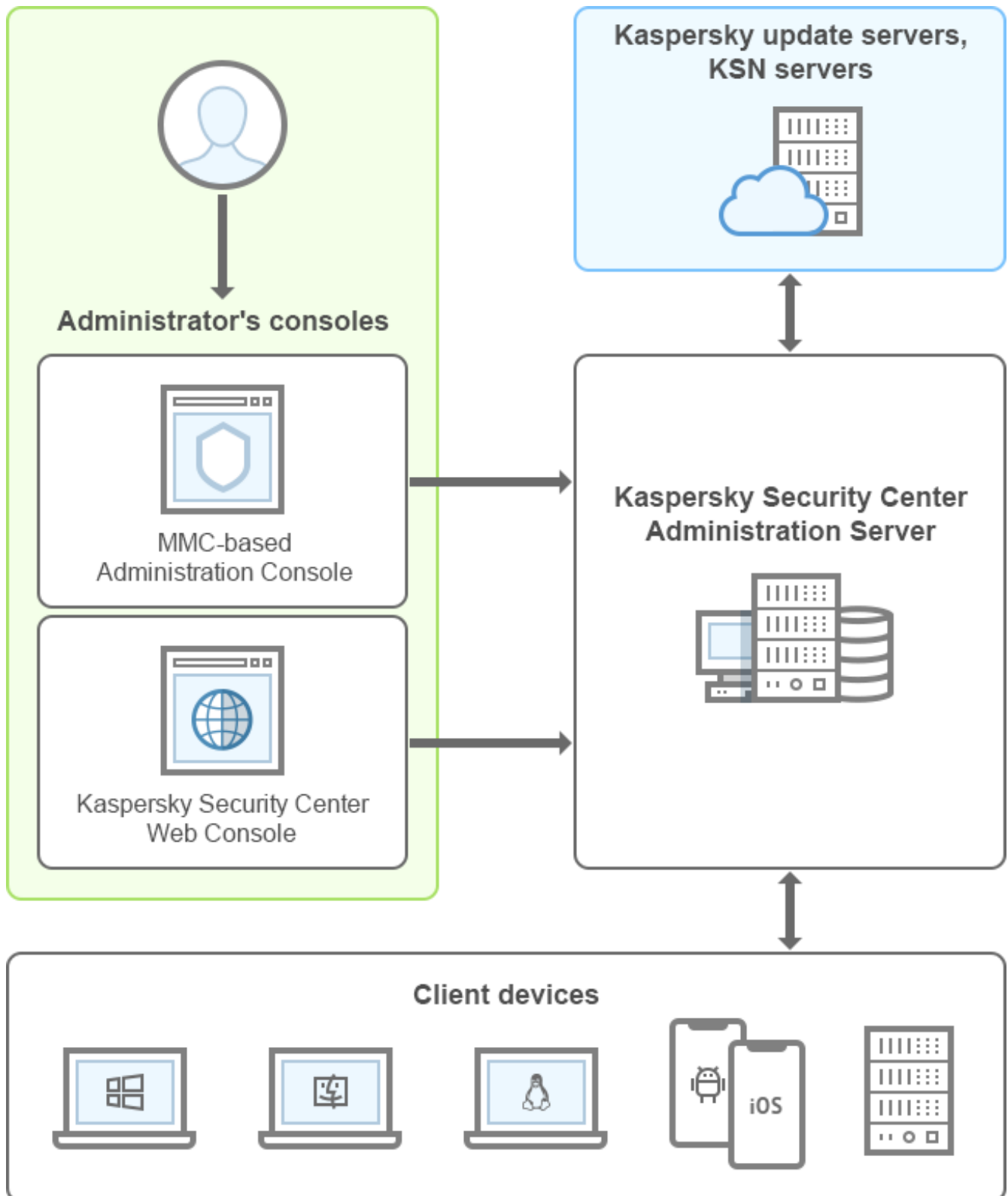
A connection gateway cannot connect to Administration Server through another connection gateway. It means that Network Agent cannot simultaneously be a connection gateway and use a connection gateway to connect to Administration Server.

A connection gateway running on a Windows device is always a distribution point. All connection gateways are included in the list of distribution points in the Administration Server properties.

- You can also use connection gateways within the network. For example, automatically assigned distribution points also become connection gateways in their own scope. However, within an internal network, connection gateways do not provide considerable benefit. They reduce the number of network connections received by Administration Server, but do not reduce the volume of incoming data. Even without connection gateways, all devices could still connect to Administration Server.

Architecture

This section provides a description of the components of Kaspersky Security Center and their interaction.



Kaspersky Security Center comprises the following main components:

- **Administration Console** (also referred to as *Console*). Provides a user interface to the administration services of Administration Server and Network Agent. Administration Console is implemented as a snap-in for Microsoft Management Console (MMC). Administration Console allows remote connection to Administration Server over the Internet.
- **Kaspersky Security Center Web Console**. Provides a web interface for creating and maintaining the protection system of a client organization's network that is managed by Kaspersky Security Center.
- **Kaspersky Security Center Administration Server** (also referred to as *Server*). Centralizes storage of information about applications installed on the organization's network and about how to manage them.
- **Kaspersky update servers**. HTTP(S) servers at Kaspersky from which Kaspersky applications download database and application module updates.
- **KSN servers**. Servers that contain a Kaspersky database with constantly updated information about the reputation of files, web resources, and software. Kaspersky Security Network ensures faster responses by Kaspersky applications to threats, improves the performance of some protection components, and reduces the likelihood of false positives.
- **Client devices**. Client company's devices protected by Kaspersky Security Center. Each device that has to be protected must have one of the Kaspersky security applications (see section "List of supported Kaspersky applications" on page [41](#)) installed.

See also:

Interaction of Kaspersky Security Center components and security applications: more information.....[108](#)

Main installation scenario

Following the main scenario, you can deploy Administration Server, as well as install Network Agent and security applications on networked devices. You can use this scenario both for a closer look at the application and for the application installation for further work.

For information about deployment of Kaspersky Security Center Cloud Console, refer to the Kaspersky Security Center Cloud Console documentation <https://help.kaspersky.com/KSC/CloudConsole/en-US/153504.htm>.

Installation and deployment of Kaspersky Security Center consists of the following steps:

1. Preparation for the deployment
2. Installation of Kaspersky Security Center and a Kaspersky security application on the Administration Server device
3. Centralized deployment of Kaspersky security applications on client devices

Deployment of Kaspersky Security Center in cloud environments (see section "Scenario: Deployment for cloud environment" on page [821](#)) and deployment of Kaspersky Security Center for service providers are described in the corresponding Help sections.

We recommend that you assign a minimum of one hour for Administration Server installation and a minimum of one working day for completion of the scenario. We also recommend that you install a security application, such as Kaspersky Security for Windows Server or Kaspersky Endpoint Security, on the computer that will act as Kaspersky Security Center Administration Server.

Upon completion of the scenario, protection will be deployed in the organization's network in the following way:

- The DBMS will be installed for the Administration Server.
- Kaspersky Security Center Administration Server will be installed.
- All required policies and tasks will be created; the default settings of policies and tasks will be specified.
- Security applications (for example, Kaspersky Endpoint Security for Windows) and Network Agent will be installed on managed devices.
- Administration groups will be created (possibly combined into a hierarchy).
- Mobile device protection will be deployed, if necessary.
- Distribution points will be assigned, if necessary.

Kaspersky Security Center deployment proceeds in stages:

Preparation for the deployment

a. Getting the necessary files

Make sure that you have a license key (activation code) for Kaspersky Security Center or license keys (activation codes) for Kaspersky security applications.

Unpack the archive that you received from your vendor. This archive contains two license keys (KEY files) and two text files. One of the license keys is needed for the activation of Kaspersky Security Center, and the other license key is needed for the activation of Kaspersky security applications. One text file provides information about the license keys and the list of Kaspersky applications that can be activated by each license key. The other text file contains an activation code (see section "About the activation code" on page [323](#)).

If you first want to try out Kaspersky Security Center, you can get a free 30-day trial at the Kaspersky website <https://usa.kaspersky.com/small-to-medium-business-security>.

For detailed information about the licensing of the Kaspersky security applications that are not included in Kaspersky Security Center, you can refer to the documentation of those applications.

b. Selecting a structure for protection of an organization

Find out more about the Kaspersky Security Center components (see section "Architecture" on page [58](#)). Select the protection structure (see section "Selecting a structure for protection of an enterprise" on page [125](#)) and the network configuration (see section "Standard configurations of Kaspersky Security Center" on page [126](#)) which suit your organization best. Based on the network configuration and throughput of communication channels, define the number of Administration Servers to use and how they must be distributed among your offices (see section "Planning Kaspersky Security Center deployment" on page [123](#)) (if you run a distributed network).

To obtain and maintain optimum performance under varying operational conditions, please take into account the number of networked devices, network topology, and set of Kaspersky Security Center features that you require (for more details, refer to the Kaspersky Security Center Sizing Guide (see section "Sizing Guide" on page [1400](#))).

Define whether a hierarchy of Administration Servers (on page [45](#)) will be used in your organization. To do this, you must evaluate whether it is possible and expedient to cover all client devices with a single Administration Server or it is necessary to build a hierarchy of Administration Servers. You may also have to build a hierarchy of Administration Servers that is identical to the organizational structure of the organization whose network you want to protect.

If you have to ensure protection of mobile devices, perform all prerequisite actions required for configuration of an Exchange Mobile Device Server (on page [141](#)) and iOS MDM Server (on page [145](#)).

Make sure that the devices that you selected as Administration Servers, as well as those for Administration Console installation, meet all the hardware and software requirements (on page [31](#)).

c. Preparation for the use of custom certificates

If your organization's Public Key Infrastructure (PKI) requires that you use custom certificates issued by a specific certification authority (CA), prepare those certificates (see section "About Kaspersky Security Center certificates" on page [86](#)) and make sure that they meet all the requirements (see section "Requirements to custom certificates used in Kaspersky Security Center" on page [279](#)).

d. Preparation for Kaspersky Security Center licensing

If you plan to use a Kaspersky Security Center version with Mobile Device Management, Integration with SIEM systems, and/or with Vulnerability and Patch Management support, make sure that you have a key file or activation code for the application licensing.

e. Preparation for licensing of managed security applications

During protection deployment, you have to provide Kaspersky with the active license keys for the applications that you intend to manage through Kaspersky Security Center (see the list of manageable security applications (see section "Kaspersky applications. Centralized deployment" on page [332](#))). For detailed information about the licensing of any security application, you can refer to the Help system of the corresponding application.

f. Selecting the hardware configuration of the Administration Server and DBMS

Plan the hardware configuration for the DBMS and the Administration Server, taking into account the number of devices on your network.

g. Selecting a DBMS

When selecting a DBMS (on page [129](#)), take into account the number of managed devices to be covered by this Administration Server. If your network includes fewer than 10 000 devices and you do not plan to increase this number, you can choose a free-of-charge DBMS, such as SQL Express, or MySQL, and install it on the same device as Administration Server. Alternatively, you can choose the MariaDB DBMS that allows you to manage up to 20 000 devices. If your network includes more than 10 000 devices (or if you plan to expand your network up to that number of devices), we recommend that you choose a paid-for SQL DBMS and install it on a dedicated device. A paid DBMS can work with multiple Administration Servers, but a DBMS that is free of charge can work with only one.

h. Installing the DBMS and creating the database

Find out more about the accounts for work with the DBMS (on page [215](#)) and install your DBMS. Write down and save the DBMS settings because you will need them during Administration Server installation. These settings include the SQL Server name, number of the port used for connecting to SQL Server, and account name and password for accessing the SQL Server.

By default, the Kaspersky Security Center Installer creates the database for storage of Administration Server information (see section "Step 7. Configuring the SQL Server" on page [237](#)), but you can opt out of creating this database and use a different database instead. In this case, make sure that the database has been created, you know its name, and the account under which the Administration Server will gain access to this database has the db_owner role for it.

If necessary, contact your DBMS administrator for more information.

i. Configuring ports

Make sure that all the necessary ports (see section "Ports used by Kaspersky Security Center" on page [65](#)) are open for interaction between components in accordance with your selected security structure.

If you have to provide Internet access to the Administration Server (see section "Providing Internet access to the Administration Server" on page [130](#)), configure the ports and specify the connection settings, depending on the network configuration.

j. Checking accounts

Make sure that you have all local administrator rights required for successful installation of Kaspersky Security Center Administration Server and further protection deployment on the devices. Local administrator rights on client devices are required for Network Agent installation on these devices. After Network Agent is installed, you can use it to install applications on devices remotely, without using the account with the device administrator rights.

By default, on the device selected for Administration Server installation, the Kaspersky Security Center Installer creates three local accounts under which Administration Server (see section "Step 9. Selecting the account to start Administration Server" on page [238](#)) and the Kaspersky Security Center services (see section "Step 10. Selecting the account for running the Kaspersky Security Center services" on page [240](#)) will be run:

- KL-AK-*: Administration Server service account
- KIScSvc: Account for other services from the Administration Server pool
- KIPxeUser: Account for deployment of operating systems

You can opt out of creating accounts for the Administration Server services and other services. You use your existing accounts instead, such as domain accounts, if you plan to install Administration Server on a failover cluster (see section "Creating accounts for the Administration Server services on a failover cluster" on page [224](#)), or plan to use domain accounts instead of local accounts for any other reason. In this case, make sure that the accounts intended for running Administration Server and the Kaspersky Security Center services have been created, are non-privileged and have all permissions required for access to the DBMS (see section "Accounts for work with the DBMS" on page [215](#)). (If you plan further deployment of operating systems (see section "Deploying operating systems on new networked devices" on page [716](#)) on devices through Kaspersky Security Center, do not opt out of creating accounts.)

Installation of Kaspersky Security Center and a Kaspersky security application on the Administration Server device

a. Installing the Administration Server, Administration Console, Kaspersky Security Center 13 Web Console, and management plug-ins for security applications

Download Kaspersky Security Center <https://www.kaspersky.com> from the Kaspersky website. You can download the full package, Web Console only, or Administration Console only.

Install Administration Server (see section "Installation of Kaspersky Security Center" on page [213](#)) on the device that you selected (or multiple devices, if you plan to use multiple Administration Servers (see section "Standard configuration: Single office" on page [126](#))). You can select standard or custom installation of Administration Server. Administration Console will be installed together with Administration Server. It is recommended to install the Administration Server on a dedicated server instead of a domain controller.

Standard installation (on page [226](#)) is recommended if you want to try out Kaspersky Security Center by, for example, testing its operation on a small area within your network. During standard installation, you only configure the database. You can also install only the default set of management plug-ins for Kaspersky applications. You can also use standard installation if you already have some experience working with Kaspersky Security Center and are able to specify all relevant settings after standard installation.

Custom installation (on page [232](#)) is recommended if you plan to modify the Kaspersky Security Center settings, such as a path to the shared folder, accounts and ports for connection to the Administration Server, and database settings. Custom installation enables you to specify which Kaspersky management plug-ins to install. If necessary, you can start custom installation in non-interactive mode (see section "Installing Administration Server in non-interactive mode" on page [253](#)).

Administration Console and the server version of Network Agent are installed together with Administration Server. You can also choose to install Kaspersky Security Center 13 Web Console (see section "Step 4. Installing Kaspersky Security Center 13 Web Console" on page [234](#)) during the installation.

If you want, install Administration Console (see section "Installing Administration Console on the administrator's workstation" on page [258](#)) and/or Kaspersky Security Center 13 Web Console on the administrator's workstation separately to manage Administration Server over the network.

b. Initial setup and licensing

When Administration Server installation is complete, at the first connection to the Administration Server the Quick Start Wizard (see section "Administration Server Quick Start Wizard" on page [265](#)) starts automatically. Perform initial configuration of Administration Server according to the existing requirements. During the initial configuration stage, the Wizard uses the default settings to create the policies (on page [51](#)) and tasks (on page [52](#)) that are required for protection deployment. However, the default settings may be less than optimal for the needs of your organization. If necessary, you can edit the settings of policies and tasks (see section "Scenario: Configuring network protection" on page [364](#)).

If you plan to use the features that are outside the basic functionality (see section "About restrictions on the main functionality" on page [322](#)), license the application. You can do this at one of the steps (see section "Step 3. Selecting the application activation method" on page [267](#)) of the Quick Start Wizard.

c. Checking Administration Server installation for success

When all the previous steps are complete, Administration Server is installed and ready for further use.

Make sure that Administration Console is running and you can connect to the Administration Server through Administration Console. Also, make sure that the Download updates to the repository of the Administration Server task is available in Administration Server (in the **Tasks** folder of the console tree (on page [896](#))), as well as the policy for Kaspersky Endpoint Security (in the **Policies** folder of the console tree).

When the check is complete, proceed to the steps below.

Centralized deployment of Kaspersky security applications on client devices

a. Discovering networked devices

This step is part of the Quick Start Wizard (see section "Step 13. Device discovery" on page [277](#)). You can also start the device discovery (on page [304](#)) manually. Kaspersky Security Center receives the addresses and names of all devices detected in the network. You can then use Kaspersky Security Center to install Kaspersky applications and software from other vendors on the detected devices. Kaspersky Security Center regularly starts device discovery, which means that if any new instances appear in the network, they will be detected automatically.

b. Installing Network Agent and security applications on networked devices

Deployment of protection (see section "Scenario: Configuring network protection" on page [364](#)) of an organization's network entails installation of Network Agent and security applications (for example, Kaspersky Endpoint Security) on devices that have been detected by Administration Server during the device discovery.

Security applications protect devices against viruses and/or other programs posing a threat. Network Agent ensures communication between the device and Administration Server. Network Agent settings are configured automatically by default.

If you want, you can install Network Agent in silent mode with a response file (see section "Installation in silent mode (with a response file)" on page [164](#)) or without a response file (see section "Installation of Network Agent in silent mode (without a response file)" on page [164](#)).

Before you start install Network Agent and the security applications on networked devices, make sure that these devices are accessible (turned on).

Security applications and Network Agent can be installed remotely or locally.

Remote installation (see section "Kaspersky applications. Centralized deployment" on page [332](#))—Using the Protection Deployment Wizard, you can remotely install the security application (for example, Kaspersky Endpoint Security for Windows) and Network Agent on devices that have been detected by Administration Server in the organization's network. Normally, the Remote installation task successfully deploys protection to most networked devices. However, it may return an error on some devices if, for example, a device is turned off or cannot be accessed for any other reason. In this case, we recommend that you connect to the device manually and use local installation.

Local installation (see section "Local installation of applications" on page [178](#))—Used on network devices on which protection could not be deployed using the remote installation task. To install protection on such devices, create a stand-alone installation package that you can run locally on those devices.

Network Agent installation on devices running Linux and macOS operating systems is described in the documentation for Kaspersky Endpoint Security for Linux and Kaspersky Endpoint Security for Mac, respectively. Although devices running Linux and macOS operating systems are considered less vulnerable than devices running Windows, we recommend that you nonetheless install security applications on such devices.

After installation, make sure that the security application is installed on managed devices. Run a Kaspersky software version report and view its results (see section "Viewing the applications registry" on page [496](#)).

c. Deploying license keys to client devices

Deploy license keys (see section "Kaspersky applications: licensing and activation" on page [357](#)) to client devices to activate managed security applications on those devices.

d. Configuring mobile device protection

This step is part of the Quick Start Wizard.

If you want to manage enterprise mobile devices, take the necessary steps for preparation (see section "Preparing to mobile device management" on page [141](#)) and deploy Mobile Device Management (see section "Deploying mobile device management systems" on page [188](#)).

e. Creating an administration group structure

In some cases, deploying protection on networked devices in the most convenient way may require you to divide the entire pool of devices into administration groups (see section "Adjustment of distribution points and connection gateways" on page [587](#)) taking into account the structure of the organization. You can create moving rules to distribute devices among groups (see section "Device moving rules" on page [401](#)) or you can distribute devices manually. You can assign group tasks for administration groups, define the scope of policies, and assign distribution points.

Make sure that all managed devices have been correctly assigned to the appropriate administration groups, and that there are no longer any unassigned devices (on page [304](#)) in the network.

f. Assigning distribution points

Distribution points (see section "About distribution points" on page [133](#)) are assigned to administration groups automatically but you can assign them manually, if necessary. We recommend that you use distribution points (see section "Adjustment of distribution points and connection gateways" on page [587](#)) on large-scale networks to reduce the load on the Administration Server, and on networks that have a distributed structure to provide the Administration Server with access to devices (or device groups) communicated through channels with low throughput rates. You can use devices running Linux as distribution points (see section "Connecting a new network segment by using Linux devices" on page [590](#)), as well as devices running Windows.

See also:

Basic concepts.....	44
Ports used by Kaspersky Security Center	65
Schemas for data traffic and port usage.....	89
Interaction of Kaspersky Security Center components and security applications: more information.....	108
Architecture.....	58
Scenario: Deployment for cloud environment.....	821
Providing Internet access to the Administration Server.....	130
Rights required for deployment of Exchange Mobile Device Server	142
How to deploy an Exchange Mobile Device Server	142
Account for Exchange ActiveSync service	143
iOS MDM Server.....	145
Connecting a new network segment by using Linux devices	590

Ports used by Kaspersky Security Center

The table below shows the default ports that must be open on Administration Servers and on client devices. If you want, you can change default port numbers.

Table 2. *Ports used by Kaspersky Security Center*

Device	Port number	Name of the process that opens the port	Protocol	TLS (except for UDP ports)	Port purpose	Scope
Administration Server	8060	klcsweb	TCP	No	Transmitting published installation packages to client devices	Publishing installation packages. You can change the default port number in the Web Server section (see section "Configuring Web Server" on page 612) of the Administration Server properties window in the MMC-based Administration Console or in Kaspersky Security Center 13 Web Console.

Device	Port number	Name of the process that opens the port	Protocol	TLS (except for UDP ports)	Port purpose	Scope
Administration Server	8061	klcsweb	TCP	Yes	Transmitting published installation packages to client devices	Publishing installation packages. You can change the default port number in the Web Server section (see section "Configuring Web Server" on page 612) of the Administration Server properties window in the MMC-based Administration Console or in Kaspersky Security Center 13 Web Console.

<p>Administration Server</p>	<p>13000</p>	<p>klserver</p>	<p>TCP</p>	<p>Yes</p>	<p>Receiving connections from Network Agents and secondary Administration Servers; also used on secondary Administration Servers for receiving connections from the primary Administration Server (for example, if the secondary Administration Server is in DMZ)</p>	<p>Managing client devices and secondary Administration Servers. You can change the number of the default port for receiving connections from Network Agents when configuring connection ports (see section "Step 12. Configuring the connection to Administration Server" on page 241); you can change the number of default port for receiving connections from secondary Administration Servers when creating a hierarchy of Administration Servers in the MMC-based Administration Console (see section "Creating a hierarchy of Administration Servers: adding a secondary Administration</p>
------------------------------	--------------	-----------------	------------	------------	---	--

Device	Port number	Name of the process that opens the port	Protocol	TLS (except for UDP ports)	Port purpose	Scope
						Administration Server" on page 1011) or in Kaspersky Security Center 13 Web Console (see section "Creating a hierarchy of Administration Servers: adding a secondary Administration Server" on page 1011).
Administration Server	13000	klserver	UDP	Null	Receiving information about devices that were turned off from Network Agents.	Managing client devices. You can change the default port number in the Network Agent policy settings in the MMC-based Administration Console (see section "Network Agent policy settings" on page 665) or in Kaspersky Security Center 13 Web Console (see section "Modifying a policy" on page 1119).

Device	Port number	Name of the process that opens the port	Protocol	TLS (except for UDP ports)	Port purpose	Scope
Administration Server	13291	klserver	TCP	Yes	Receiving connections from Administration Console to Administration Server	Managing Administration Server. You can change the default port number in the Administration Server properties window (see section "Configuring the connection of Kaspersky Security Center 13 Web Console to Administration Server" on page 1007) in the MMC-based Administration Console.

Device	Port number	Name of the process that opens the port	Protocol	TLS (except for UDP ports)	Port purpose	Scope
Administration Server	13292 (only if you manage mobile devices)	klserver	TCP	Yes	Receiving connections from mobile devices	Mobile Device Management . You can change the default port number in the Administration Server properties window in the MMC-based Administration console (see section "Modifying the Mobile Device Management settings" on page 1009) or in Kaspersky Security Center 13 Web Console (see section "Modifying the Mobile Device Management settings" on page 1009).

Device	Port number	Name of the process that opens the port	Protocol	TLS (except for UDP ports)	Port purpose	Scope
Administration Server	13294 (only if you manage mobile devices)	klserver	TCP	Yes	Receiving connections from UEFI protection devices	Managing UEFI protection client devices. You can change the default port number when connecting mobile devices (see section "Step 10. Connecting mobile devices" on page 272), or later in the Administration Server properties window (in the Additional ports subsection of the General section) in the MMC-based Administration Console or in Kaspersky Security Center 13 Web Console (see section "Connection settings of UEFI protection devices" on page 1010).

<p>Administration Server</p>	<p>13299</p>	<p>klserver</p>	<p>TCP</p>	<p>Yes</p>	<p>Receiving connections from Kaspersky Security Center 13 Web Console to the Administration Server; receiving connections to the Administration Server over OpenAPI</p>	<p>Kaspersky Security Center 13 Web Console, OpenAPI. You can change the default port number in the Administration Server properties window (in the Connection ports subsection of the General section) in the MMC-based Administration Console, or when creating a hierarchy of Administration Servers in the MMC-based Administration Console (see section "Creating a hierarchy of Administration Servers: adding a secondary Administration Server" on page 1011) or in Kaspersky Security Center 13 Web Console (see section "Creating a hierarchy of Administration</p>
------------------------------	--------------	-----------------	------------	------------	--	---

Device	Port number	Name of the process that opens the port	Protocol	TLS (except for UDP ports)	Port purpose	Scope
						on Servers: adding a secondary Administration Server" on page 1011).

Device	Port number	Name of the process that opens the port	Protocol	TLS (except for UDP ports)	Port purpose	Scope
Administration Server	14000	klserver	TCP	No	Receiving connections from Network Agents	Managing client devices. You can change the default port number when configuring connection ports (see section "Step 12. Configuring the connection to Administration Server" on page 241) during the installation of Kaspersky Security Center, or when manually connecting a client device to the Administration Server (see section "Manually connecting a client device to the Administration Server. Klmover utility" on page 638).

Device	Port number	Name of the process that opens the port	Protocol	TLS (except for UDP ports)	Port purpose	Scope
Administration Server	13111 (only if KSN proxy service is run on the device)	ksnproxy	TCP	No	Receiving requests from managed devices to KSN proxy server	KSN proxy server. You can change the default port number in the Administration Server properties window (see section "Setting up access to Kaspersky Security Network" on page 786).
Administration Server	15111 (only if KSN proxy service is run on the device)	ksnproxy	UDP	Null	Receiving requests from managed devices to KSN proxy server	KSN proxy server. You can change the default port number in the Administration Server properties window (see section "Setting up access to Kaspersky Security Network" on page 786).

Device	Port number	Name of the process that opens the port	Protocol	TLS (except for UDP ports)	Port purpose	Scope
Administration Server	17000	klactprx	TCP	Yes	Receiving connections for application activation from managed devices (except for mobile devices)	Activation proxy server for non-mobile devices. You can change the default port number in the Administration Server properties window (see section "Modifying the Mobile Device Management settings" on page 731).
Administration Server	17100 <i>(only if you manage mobile devices)</i>	klactprx	TCP	Yes	Receiving connections for application activation from mobile devices (see section "Modifying the Mobile Device Management settings" on page 731)	Activation proxy server for mobile devices. You can change the default port number in the Administration Server properties window (see section "Modifying the Mobile Device Management settings" on page 731).

Device	Port number	Name of the process that opens the port	Protocol	TLS (except for UDP ports)	Port purpose	Scope
<i>Administration Server</i>	<i>19170 (only if you manage mobile devices)</i>	<i>klserver</i>	<i>HTTPS</i>	<i>Yes</i>	<i>Tunneling connections (see section "Configuring the connection of Kaspersky Security Center 13 Web Console to Administration Server" on page 1007) to managed devices by using the <i>klstunnel</i> utility</i>	<i>Remotely connecting to managed devices by using Kaspersky Security Center 13 Web Console. You can change the default port number in the Administration Server properties window (in the Additional ports subsection of the General section) in the MMC-based Administration Console only.</i>

Device	Port number	Name of the process that opens the port	Protocol	TLS (except for UDP ports)	Port purpose	Scope
Network Agent	15000	klnagent	UDP	Null	Management signals from Administration Server to Network Agents	Managing client devices. You can change the default port number in the Network Agent policy settings in the MMC-based Administration Console (see section "Network Agent policy settings" on page 665) or in Kaspersky Security Center 13 Web Console (see section "Modifying a policy" on page 1119).
			UDP broadcast	Null	Getting data about other Network Agents within the same broadcasting domain (the data is then sent to the Administration Server)	Delivering updates and installation packages.

Device	Port number	Name of the process that opens the port	Protocol	TLS (except for UDP ports)	Port purpose	Scope
Network Agent acting as distribution point	15001	klagent	UDP	Null	Multicasting for Network Agents (see section "Assigning distribution points manually" on page 1204)	Delivering updates and installation packages. You can change the default port number in the distribution point properties window in the MMC-based Console (see section "Assigning a device a distribution point manually" on page 427) or in Kaspersky Security Center 13 Web Console (see section "Assigning distribution points manually" on page 1204).

Device	Port number	Name of the process that opens the port	Protocol	TLS (except for UDP ports)	Port purpose	Scope
Network Agent acting as distribution point	13000	klagent	TCP	Yes	Receiving connections from Network Agents (see section "Assigning distribution points manually" on page 1204)	Managing client devices, delivering updates and installation packages You can change the default port number in the distribution point properties window in the MMC-based Console (see section "Assigning a device a distribution point manually" on page 427) or in Kaspersky Security Center 13 Web Console (see section "Assigning distribution points manually" on page 1204).

Device	Port number	Name of the process that opens the port	Protocol	TLS (except for UDP ports)	Port purpose	Scope
Network Agent acting as distribution point	15111 (only if KSN proxy service is run on the device)	ksnproxy	UDP	Null	Receiving requests from managed devices to KSN proxy server	KSN Proxy server. You can change the default port number in the distribution point properties window in the MMC-based Console (see section "Assigning a device a distribution point manually" on page 427) or in Kaspersky Security Center 13 Web Console (see section "Assigning distribution points manually" on page 1204).

Device	Port number	Name of the process that opens the port	Protocol	TLS (except for UDP ports)	Port purpose	Scope
Network Agent acting as distribution point	13111 (only if KSN proxy service is run on the device)	ksnproxy	TCP	No	Receiving requests from managed devices to KSN proxy server	KSN Proxy server. You can change the default port number in the distribution point properties window in the MMC-based Console (see section "Assigning a device a distribution point manually" on page 427) or in Kaspersky Security Center 13 Web Console (see section "Assigning distribution points manually" on page 1204).
iOS MDM Server	443 (only if you manage mobile devices)	kliosmdmservicesrv	TCP	Yes	Receiving connections from iOS mobile devices (see section "Installing iOS MDM Server" on page 193)	Mobile Device Management. You can change the default port number when installing iOS MDM Server (on page 193).

Device	Port number	Name of the process that opens the port	Protocol	TLS (except for UDP ports)	Port purpose	Scope
Kaspersky Security Center 13 Web Console Server (may be the same device where the Administration Server is running, or may be a different device)	8080* (only if you work with Kaspersky Security Center 13 Web Console)	Node.js: Server-side JavaScript	TCP	Yes	Receiving connections from browser to Kaspersky Security Center 13 Web Console (see section "Installing Kaspersky Security Center 13 Web Console" on page 967)	Kaspersky Security Center 13 Web Console. You can change the default port number when installing Kaspersky Security Center 13 Web Console on a device running Windows (see section "Installing Kaspersky Security Center 13 Web Console" on page 967) or on a Linux platform (see section "Installing Kaspersky Security Center 13 Web Console on Linux platforms" on page 969).

* When you install Kaspersky Security Center 13 Web Console on Linux ALT operating system, you must specify a port number other than 8080, because port 8080 is used by the operating system. If you install the Administration Server and the database on different devices, you must make available the necessary ports on the device where the database is located (for example, port 3306 for MySQL Server and MariaDB Server, or port 1433 for Microsoft SQL Server). Please refer to the DBMS documentation for the relevant information.

See also:

Interaction of Kaspersky Security Center components and security applications: more information.....	108
Scenario: Mobile Device Management deployment	728
Ports used by Kaspersky Security Center 13 Web Console	960

About Kaspersky Security Center certificates

Kaspersky Security Center uses the following types of certificates to enable a secure interaction between the application components:

- Administration Server certificate
- Mobile certificate
- iOS MDM Server certificate
- Web Server certificate

By default, Kaspersky Security Center uses self-signed certificates (that is, issued by Kaspersky Security Center itself), but you can replace them with custom certificates to better meet the requirements of your organization's network and comply with the security standards. After Administration Server verifies whether a custom certificate meets all applicable requirements, this certificate assumes the same functional scope as a self-signed certificate. The only difference is that a custom certificate is not reissued automatically upon expiration. You replace certificates with custom ones by means of the `klsetsrvcert` utility or through the Administration Server properties section in Administration Console, depending on the certificate type. The indexes of the certificate types described below are based on the possible values of the `-t certtype` parameter in the `klsetsrvcert` utility:

- C (common certificate for ports 13000 and 13291)
- CR (common reserve certificate for ports 13000 and 13291)
- M (mobile certificate for port 13292)
- MR (mobile reserve certificate for port 13292)
- MCA (mobile certification authority for auto-generated user certificates)

Administration Server certificates

An Administration Server certificate is required for authentication of Administration Server, as well as for secure interaction between Administration Server and Network Agent on managed devices. When you connect Administration Console to Administration Server for the first time, you are prompted to confirm the use of the current Administration Server certificate. Such confirmation is also required every time the Administration Server certificate is replaced, after every reinstallation of Administration Server, and when connecting a secondary Administration Server to the primary Administration Server. This certificate is called common ("C").

Also, a common reserve ("CR") certificate exists. Kaspersky Security Center automatically generates this certificate 90 days before the expiration of the common certificate. The common reserve certificate is subsequently used for seamless replacement of the Administration Server certificate. When the common certificate is about to expire, the common reserve certificate is used to maintain the connection with Network Agent instances installed on managed devices. With this purpose, the common reserve certificate automatically becomes the new common certificate 24 hours before the old common certificate expires.

You can also back up the Administration Server certificate separately from other Administration Server settings in order to move Administration Server from one device to another without data loss.

Mobile certificates

A mobile certificate ("M") is required for authentication of the Administration Server on mobile devices. You configure the use of the mobile certificate on the dedicated step of the Quick Start Wizard.

Also, a mobile reserve ("MR") certificate exists: it is used for seamless replacement of the mobile certificate. When the mobile certificate is about to expire, the mobile reserve certificate is used to maintain the connection with Network Agent instances installed on managed mobile devices. With this purpose, the mobile reserve certificate automatically becomes the new mobile certificate 24 hours before the old mobile certificate expires.

If the connection scenario requires the use of a client certificate on mobile devices (connection involving two-way SSL authentication), you generate those certificates by means of the certificate authority for auto-generated user certificates ("MCA"). Also, the Quick Start Wizard enables you to start using custom client certificates issued by a different certification authority, while integration with the domain Public Key Infrastructure (PKI) of your organization enables you to issue client certificates by means of your domain certification authority.

iOS MDM Server certificate

An iOS MDM Server certificate is required for authentication of Administration Server on mobile devices running the iOS operating system. The interaction with these devices is performed via the Apple mobile device management (MDM) protocol that involves no Network Agent. Instead, you install a special iOS MDM profile, containing a client certificate, on each device, to ensure two-way SSL authentication.

Also, the Quick Start Wizard enables you to start using custom client certificates issued by a different certification authority, while integration with the domain Public Key Infrastructure (PKI) of your organization enables you to issue client certificates by means of your domain certification authority.

Client certificates are transmitted to iOS devices when you download those iOS MDM profiles. Each iOS MDM Server client certificate is unique. You generate all iOS MDM Server client certificates by means of the certification authority for auto-generated user certificates ("MCA").

Web Server certificate

A special type of certificate is used by Web Server, a component of Kaspersky Security Center Administration Server. This certificate is required for publishing Network Agent installation packages that you subsequently download to managed devices, as well as for publishing iOS MDM profiles, iOS apps, and Kaspersky Security for Mobile installation packages. For this purpose, Web Server can use various certificates.

If the mobile device support is disabled, Web Server uses one of the following certificates, in order of priority:

1. Custom Web Server certificate that you specified manually by means of Administration Console
2. Common Administration Server certificate ("C")

If the mobile device support is enabled, Web Server uses one of the following certificates, in order of priority:

1. Custom Web Server certificate that you specified manually by means of Administration Console
2. Custom mobile certificate
3. Self-signed mobile certificate ("M")
4. Common Administration Server certificate ("C")

See also

Requirements to custom certificates used in Kaspersky Security Center	279
Main installation scenario	59
Administration Server authentication during Administration Console connection	604
Hierarchy of Administration Servers: primary Administration Server and secondary Administration Server.....	114
Data backup and recovery in interactive mode	619
Working with certificates	737
Administration Server Quick Start Wizard	265
Adding iOS mobile devices to the list of managed devices.....	744
Issuing a certificate for an iOS MDM profile	756
Web Server	47

Schemas for data traffic and port usage

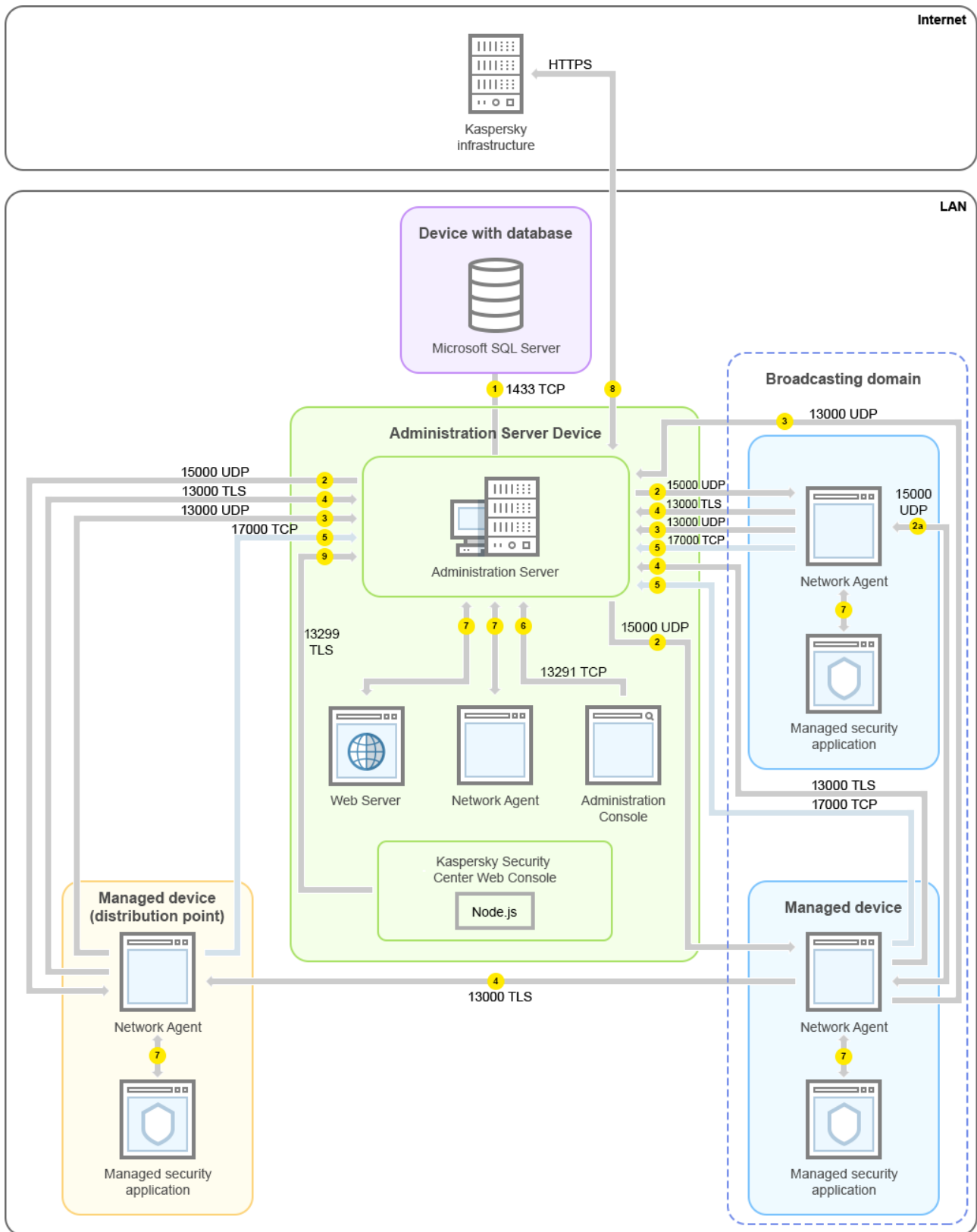
This section provides schemas for data traffic between Kaspersky Security Center components, managed security applications, and external servers under various configurations. The schemas are provided with numbers for the ports that must be available on the local devices.

In this chapter

Administration Server and managed devices on LAN.....	90
Primary Administration Server on LAN and two secondary Administration Servers.....	94
Administration Server on LAN, managed devices on Internet, TMG in use.....	96
Administration Server on LAN, managed devices on Internet, connection gateway in use.....	99
Administration Server in DMZ, managed devices on Internet.....	104
Interaction of Kaspersky Security Center components and security applications: more information.....	108

Administration Server and managed devices on LAN

The figure below shows the traffic of the data if Kaspersky Security Center is deployed on a local area network (LAN) only.



The figure shows how different managed devices connect to the Administration Server in different ways: directly or via a distribution point. Distribution points reduce the load on the Administration Server during update distribution and optimize network traffic. However, distribution points are only needed if the number of managed devices is large enough (see section "Calculating the number and configuration of distribution points" on page 134). If the

number of managed devices is small, all the managed devices can receive updates from the Administration Server directly.

The arrows indicate the initiation of traffic: each arrow points from a device that initiates the connection to the device that "answers" the call. The number of the port and the name of the protocol used for data transfer are provided. Each arrow has a number label, and details about the corresponding data traffic are as follows:

1. Administration Server sends data to the database (see section "Administration Server and DBMS" on page [110](#)). If you install the Administration Server and the database on different devices, you must make available the necessary ports on the device where the database is located (for example, port 3306 for MySQL Server and MariaDB Server, or port 1433 for Microsoft SQL Server). Please refer to the DBMS documentation for the relevant information.
2. Requests for communication from the Administration Server are transferred to all non-mobile managed devices through UDP port 15000 (see section "Administration Server and client device: Managing the security application" on page [112](#)).

Network Agents send requests to each other within one broadcasting domain. The data is then sent to the Administration Server and is used for defining the limits of the broadcasting domain and for automatic assignment of distribution points (if this option is enabled).

3. Information about shutdown of the managed devices is transferred from Network Agent to the Administration Server through UDP port 13000.
4. The Administration Server receives connection from Network Agents (see section "Administration Server and client device: Managing the security application" on page [112](#)) and from secondary Administration Servers (see section "Hierarchy of Administration Servers: primary Administration Server and secondary Administration Server" on page [114](#)) through SSL port 13000.

If you used an earlier version of Kaspersky Security Center, the Administration Server on your network can receive connection from Network Agents through non-SSL port 14000. Kaspersky Security Center also supports connection of Network Agents through port 14000, although using SSL port 13000 is recommended.

The distribution point was called "Update agent" in earlier versions of Kaspersky Security Center.

5. The managed devices (except for mobile devices) request activation through TCP port 17000. This is not necessary if the device has its own access to the Internet; in this case, the device sends the data to Kaspersky servers over the Internet directly.
6. Data from MMC-based Administration Console is transferred to the Administration Server through port 13291 (see section "Administration Server and Administration Console" on page [111](#)). (The Administration Console can be installed on the same or on a different device.)
7. Applications on a single device exchange local traffic (either on the Administration Server or on a managed device). No external ports have to be opened.
8. Data from the Administration Server to the Kaspersky servers (such as KSN data or information about licenses) and data from the Kaspersky servers to the Administration Server (such as application updates and anti-virus database updates) are transferred using the HTTPS protocol.

If you do not want your Administration Server to have access to the Internet, you must manage this data manually.

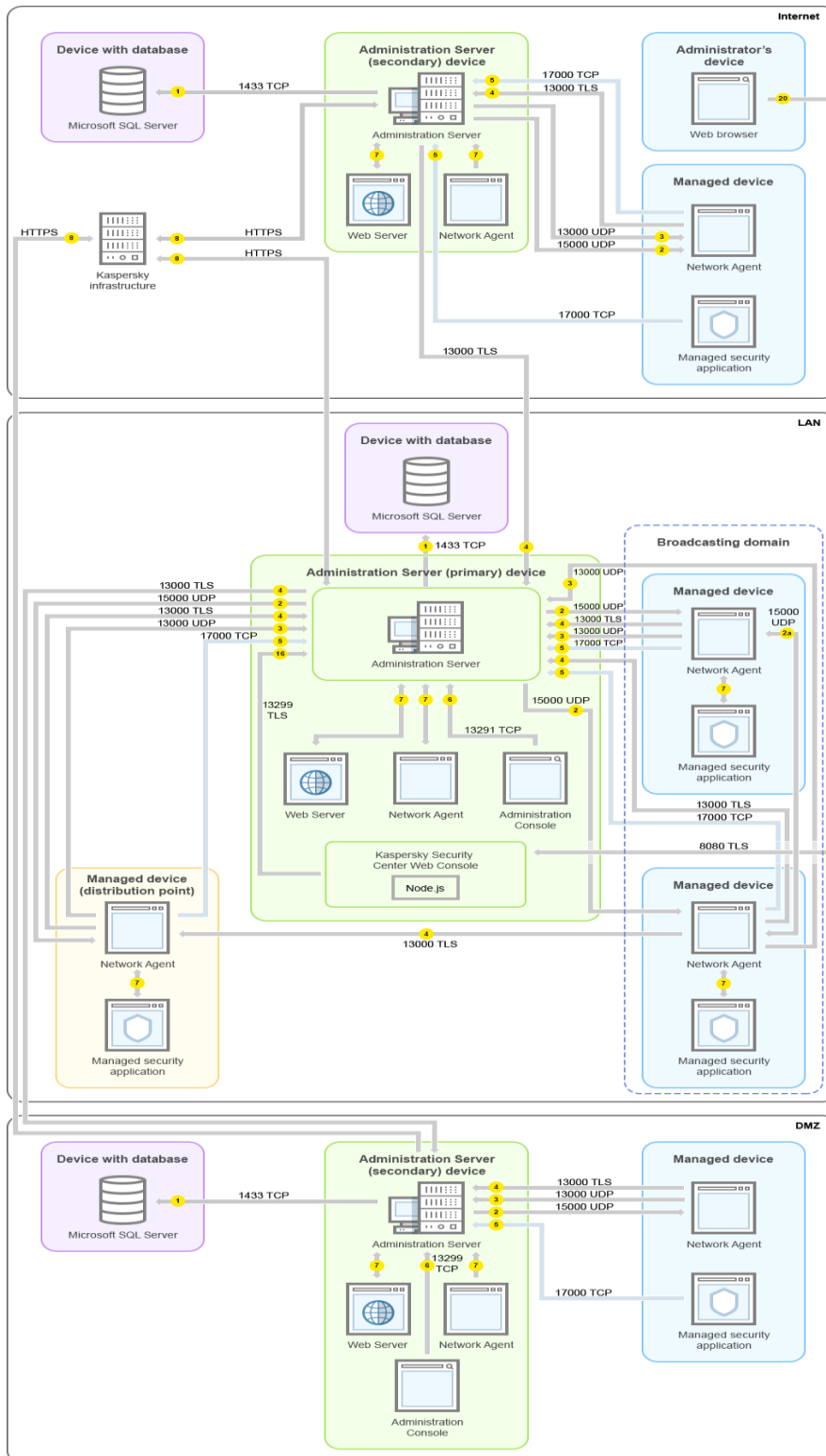
9. Kaspersky Security Center Web Console Server sends data to the Administration Server, which may be installed on the same or on a different device, through TLS port 13299 (see section "Administration Server and Kaspersky Security Center 13 Web Console" on page [118](#)).

See also:

Standard configuration: Single office.....	126
Ports used by Kaspersky Security Center	65

Primary Administration Server on LAN and two secondary Administration Servers

The figure below shows the hierarchy of Administration Servers: the primary Administration Server is on a local area network (LAN). A secondary Administration Server is in the demilitarized zone (DMZ); another secondary Administration Server is on the Internet.



The arrows indicate the initiation of traffic: each arrow points from a device that initiates the connection to the device that "answers" the call. The number of the port and the name of the protocol used for data transfer are provided. Each arrow has a number label, and details about the corresponding data traffic are as follows:

1. Administration Server sends data to the database (see section "Administration Server and DBMS" on page [110](#)). If you install the Administration Server and the database on different devices, you must make available the necessary ports on the device where the database is located (for example, port 3306 for MySQL Server and MariaDB Server, or port 1433 for Microsoft SQL Server). Please refer to the DBMS documentation for the relevant information.
2. Requests for communication from the Administration Server are transferred to all non-mobile managed devices through UDP port 15000 (see section "Administration Server and client device: Managing the security application" on page [112](#)).

Network Agents send requests to each other within one broadcasting domain. The data is then sent to the Administration Server and is used for defining the limits of the broadcasting domain and for automatic assignment of distribution points (if this option is enabled).

3. Information about shutdown of the managed devices is transferred from Network Agent to the Administration Server through UDP port 13000.
4. The Administration Server receives connection from Network Agents (see section "Administration Server and client device: Managing the security application" on page [112](#)) and from secondary Administration Servers (see section "Hierarchy of Administration Servers: primary Administration Server and secondary Administration Server" on page [114](#)) through SSL port 13000.

If you used an earlier version of Kaspersky Security Center, the Administration Server on your network can receive connection from Network Agents through non-SSL port 14000. Kaspersky Security Center also supports connection of Network Agents through port 14000, although using SSL port 13000 is recommended.

The distribution point was called "Update agent" in earlier versions of Kaspersky Security Center.

5. The managed devices (except for mobile devices) request activation through TCP port 17000. This is not necessary if the device has its own access to the Internet; in this case, the device sends the data to Kaspersky servers over the Internet directly.
6. Data from MMC-based Administration Console is transferred to the Administration Server through port 13291 (see section "Administration Server and Administration Console" on page [111](#)). (The Administration Console can be installed on the same or on a different device.)
7. Applications on a single device exchange local traffic (either on the Administration Server or on a managed device). No external ports have to be opened.
8. Data from the Administration Server to the Kaspersky servers (such as KSN data or information about licenses) and data from the Kaspersky servers to the Administration Server (such as application updates and anti-virus database updates) are transferred using the HTTPS protocol.

If you do not want your Administration Server to have access to the Internet, you must manage this data manually.

9. Kaspersky Security Center 13 Web Console Server sends data to the Administration Server, which may be installed on the same or on a different device, through TLS port 13299.
 - 9a. Data from the browser, which is installed on a separate device of the administrator, is transferred to Kaspersky Security Center 13 Web Console Server through TLS port 8080 (see section "Administration Server and Kaspersky Security Center 13 Web Console" on page [118](#)). The Kaspersky Security Center 13 Web Console Server can be installed either on the Administration Server or on another device.

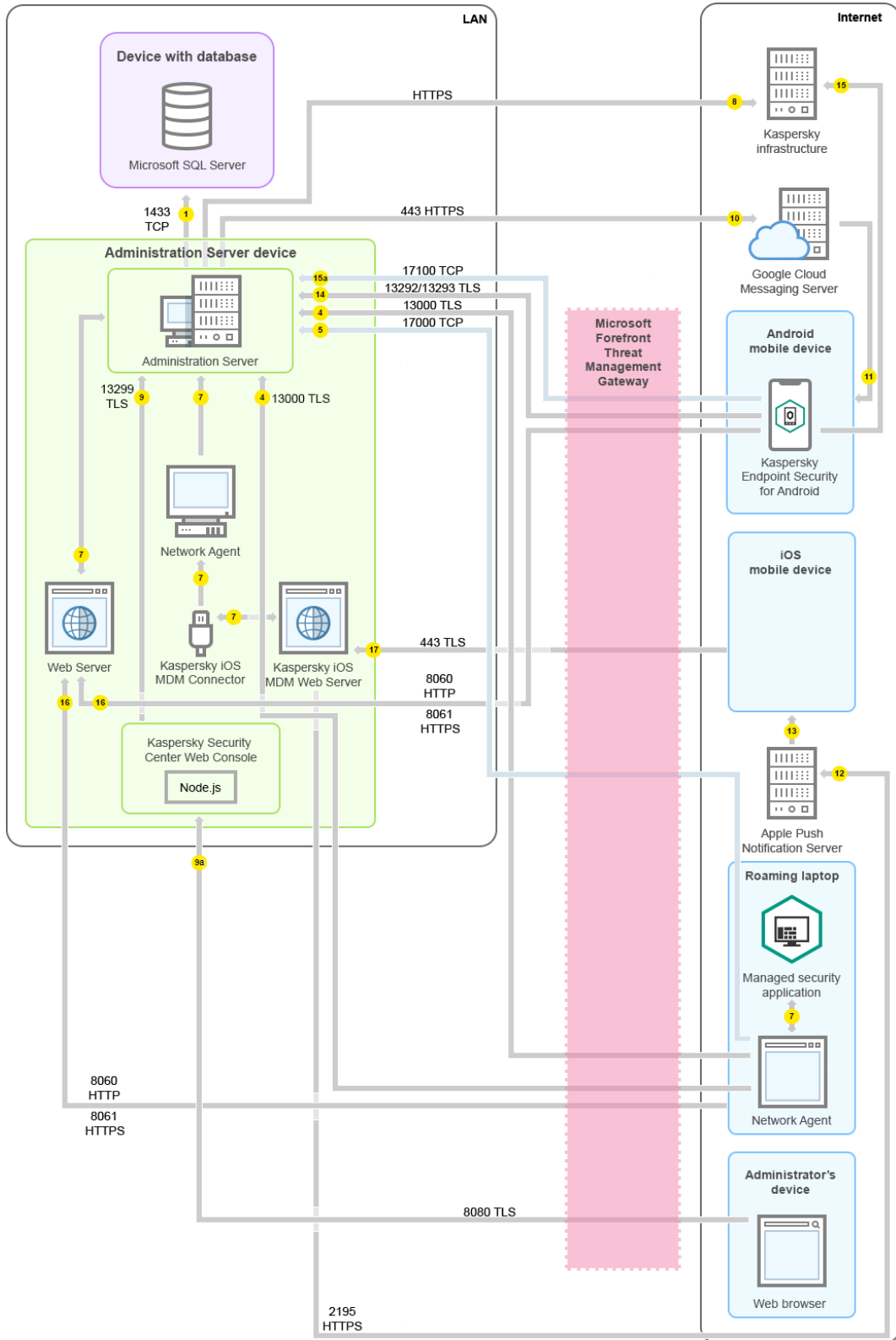
See also:

A hierarchy of Administration Servers	135
Ports used by Kaspersky Security Center	65

Administration Server on LAN, managed devices on Internet, TMG in use

The figure below shows data traffic if the Administration Server is on a local area network (LAN), and the managed devices, including mobile devices, are on the Internet. In this figure, *Microsoft Forefront Threat Management*

Gateway (TMG) is in use. However, if you want to use a corporate firewall, you can use a different application; refer to the documentation of the application of your choice for details.



This deployment scheme is recommended if you do not want the mobile devices to connect to the Administration Server directly and do not want to assign a connection gateway in the DMZ.

The arrows indicate the initiation of traffic: each arrow points from a device that initiates the connection to the device that "answers" the call. The number of the port and the name of the protocol used for data transfer are provided. Each arrow has a number label, and details about the corresponding data traffic are as follows:

1. Administration Server sends data to the database (see section "Administration Server and DBMS" on page [110](#)). If you install the Administration Server and the database on different devices, you must make available the necessary ports on the device where the database is located (for example, port 3306 for MySQL Server and MariaDB Server, or port 1433 for Microsoft SQL Server). Please refer to the DBMS documentation for the relevant information.
2. Requests for communication from the Administration Server are transferred to all non-mobile managed devices through UDP port 15000 (see section "Administration Server and client device: Managing the security application" on page [112](#)).

Network Agents send requests to each other within one broadcasting domain. The data is then sent to the Administration Server and is used for defining the limits of the broadcasting domain and for automatic assignment of distribution points (if this option is enabled).

3. Information about shutdown of the managed devices is transferred from Network Agent to the Administration Server through UDP port 13000.
4. The Administration Server receives connection from Network Agents (see section "Administration Server and client device: Managing the security application" on page [112](#)) and from secondary Administration Servers (see section "Hierarchy of Administration Servers: primary Administration Server and secondary Administration Server" on page [114](#)) through SSL port 13000.

If you used an earlier version of Kaspersky Security Center, the Administration Server on your network can receive connection from Network Agents through non-SSL port 14000. Kaspersky Security Center also supports connection of Network Agents through port 14000, although using SSL port 13000 is recommended.

The distribution point was called "Update agent" in earlier versions of Kaspersky Security Center.

5. The managed devices (except for mobile devices) request activation through TCP port 17000. This is not necessary if the device has its own access to the Internet; in this case, the device sends the data to Kaspersky servers over the Internet directly.
6. Data from MMC-based Administration Console is transferred to the Administration Server through port 13291 (see section "Administration Server and Administration Console" on page [111](#)). (The Administration Console can be installed on the same or on a different device.)
7. Applications on a single device exchange local traffic (either on the Administration Server or on a managed device). No external ports have to be opened.
8. Data from the Administration Server to the Kaspersky servers (such as KSN data or information about licenses) and data from the Kaspersky servers to the Administration Server (such as application updates and anti-virus database updates) are transferred using the HTTPS protocol.

If you do not want your Administration Server to have access to the Internet, you must manage this data manually.

9. Kaspersky Security Center 13 Web Console Server sends data to the Administration Server, which may be installed on the same or on a different device, through TLS port 13299.
 - 9a. Data from the browser, which is installed on a separate device of the administrator, is transferred to Kaspersky Security Center 13 Web Console Server through TLS port 8080 (see section "Administration Server and Kaspersky Security Center 13 Web Console" on page [118](#)). The Kaspersky Security Center 13 Web Console Server can be installed either on the Administration Server or on another device.

10. For Android mobile devices only: data from the Administration Server is transferred to Google servers. This connection is used to notify Android mobile devices that they are required to connect to the Administration Server. Then push notifications are sent to the mobile devices.
11. For Android mobile devices only: push notifications from Google servers are sent to the mobile device. This connection is used to notify mobile devices that they are required to connect to the Administration Server.
12. For iOS mobile devices only: data from the iOS MDM Server (on page [145](#)) is transferred to Apple Push Notification servers. Then push notifications are sent to the mobile devices.
13. For iOS mobile devices only: push notifications are sent from Apple servers to the mobile device. This connection is used to notify iOS mobile devices that they are required to connect to the Administration Server.
14. For mobile devices only: data from the managed application is transferred to the Administration Server (or to the connection gateway) through TLS port 13292 / 13293 (see section "Activating and managing the security application on a mobile device" on page [119](#))—directly or through a Microsoft Forefront Threat Management Gateway (TMG).
15. For mobile devices only: data from the mobile device is transferred to the Kaspersky infrastructure.
 - 15a. If a mobile device does not have Internet access, the data is transferred to Administration Server through port 17100 (see section "Activating and managing the security application on a mobile device" on page [119](#)), and the Administration Server sends it to the Kaspersky infrastructure; however, this scenario applies very rarely.
16. Requests for packages from managed devices, including mobile devices, are transferred to the Web Server (on page [47](#)), which is on the same device as the Administration Server.
17. For iOS mobile devices only: data from the mobile device is transferred through TLS port 443 to the iOS MDM Server, which is on the same device as the Administration Server or on the connection gateway.

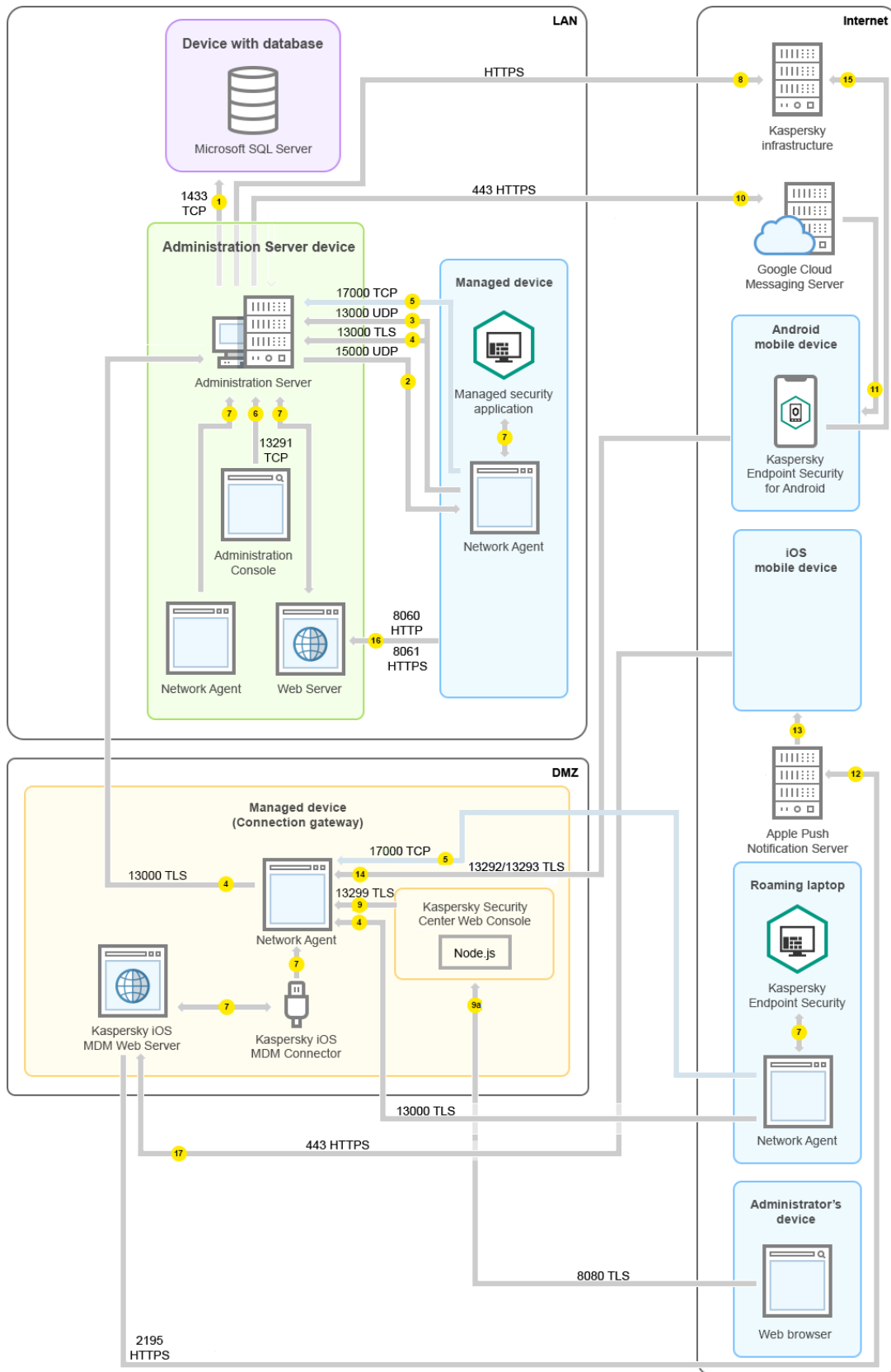
See also:

Ports used by Kaspersky Security Center[65](#)

Administration Server on LAN, managed devices on Internet, connection gateway in use

The figure below shows data traffic if the Administration Server is on a local area network (LAN) and the managed devices (including mobile devices) are on the Internet. A connection gateway is in use.

This deployment scheme is recommended if you do not want the mobile devices to connect to the Administration Server directly and do not want to use a Microsoft Forefront Threat Management Gateway (TMG) or corporate firewall.



In this figure, the managed devices are connected to the Administration Server through a connection gateway that is located in the DMZ. No TMG or corporate firewall is in use.

The arrows indicate the initiation of traffic: each arrow points from a device that initiates the connection to the device that "answers" the call. The number of the port and the name of the protocol used for data transfer are provided. Each arrow has a number label, and details about the corresponding data traffic are as follows:

1. Administration Server sends data to the database (see section "Administration Server and DBMS" on page [110](#)). If you install the Administration Server and the database on different devices, you must make available the necessary ports on the device where the database is located (for example, port 3306 for MySQL Server and MariaDB Server, or port 1433 for Microsoft SQL Server). Please refer to the DBMS documentation for the relevant information.
2. Requests for communication from the Administration Server are transferred to all non-mobile managed devices through UDP port 15000 (see section "Administration Server and client device: Managing the security application" on page [112](#)).

Network Agents send requests to each other within one broadcasting domain. The data is then sent to the Administration Server and is used for defining the limits of the broadcasting domain and for automatic assignment of distribution points (if this option is enabled).

3. Information about shutdown of the managed devices is transferred from Network Agent to the Administration Server through UDP port 13000.
4. The Administration Server receives connection from Network Agents (see section "Administration Server and client device: Managing the security application" on page [112](#)) and from secondary Administration Servers (see section "Hierarchy of Administration Servers: primary Administration Server and secondary Administration Server" on page [114](#)) through SSL port 13000.

If you used an earlier version of Kaspersky Security Center, the Administration Server on your network can receive connection from Network Agents through non-SSL port 14000. Kaspersky Security Center also supports connection of Network Agents through port 14000, although using SSL port 13000 is recommended.

The distribution point was called "Update agent" in earlier versions of Kaspersky Security Center.

5. The managed devices (except for mobile devices) request activation through TCP port 17000. This is not necessary if the device has its own access to the Internet; in this case, the device sends the data to Kaspersky servers over the Internet directly.
6. Data from MMC-based Administration Console is transferred to the Administration Server through port 13291 (see section "Administration Server and Administration Console" on page [111](#)). (The Administration Console can be installed on the same or on a different device.)
7. Applications on a single device exchange local traffic (either on the Administration Server or on a managed device). No external ports have to be opened.
8. Data from the Administration Server to the Kaspersky servers (such as KSN data or information about licenses) and data from the Kaspersky servers to the Administration Server (such as application updates and anti-virus database updates) are transferred using the HTTPS protocol.

If you do not want your Administration Server to have access to the Internet, you must manage this data manually.

9. Kaspersky Security Center 13 Web Console Server sends data to the Administration Server, which may be installed on the same or on a different device, through TLS port 13299.
 - 9a. Data from the browser, which is installed on a separate device of the administrator, is transferred to Kaspersky Security Center 13 Web Console Server through TLS port 8080 (see section "Administration Server and Kaspersky Security Center 13 Web Console" on page [118](#)). The Kaspersky Security Center 13 Web Console Server can be installed either on the Administration Server or on another device.

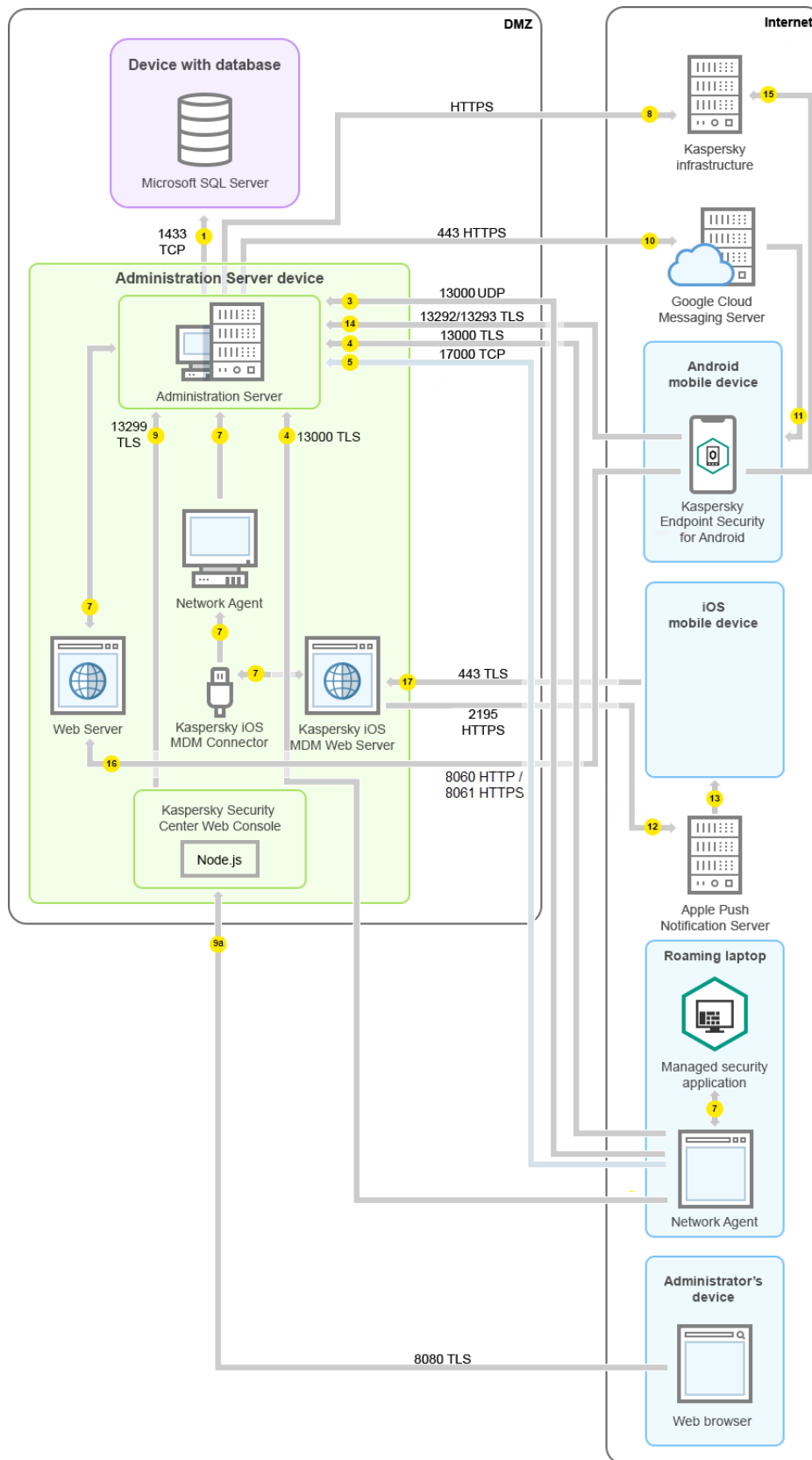
10. For Android mobile devices only: data from the Administration Server is transferred to Google servers. This connection is used to notify Android mobile devices that they are required to connect to the Administration Server. Then push notifications are sent to the mobile devices.
11. For Android mobile devices only: push notifications from Google servers are sent to the mobile device. This connection is used to notify mobile devices that they are required to connect to the Administration Server.
12. For iOS mobile devices only: data from the iOS MDM Server (on page [145](#)) is transferred to Apple Push Notification servers. Then push notifications are sent to the mobile devices.
13. For iOS mobile devices only: push notifications are sent from Apple servers to the mobile device. This connection is used to notify iOS mobile devices that they are required to connect to the Administration Server.
14. For mobile devices only: data from the managed application is transferred to the Administration Server (or to the connection gateway) through TLS port 13292 / 13293 (see section "Activating and managing the security application on a mobile device" on page [119](#))—directly or through a Microsoft Forefront Threat Management Gateway (TMG).
15. For mobile devices only: data from the mobile device is transferred to the Kaspersky infrastructure.
 - 15a. If a mobile device does not have Internet access, the data is transferred to Administration Server through port 17100 (see section "Activating and managing the security application on a mobile device" on page [119](#)), and the Administration Server sends it to the Kaspersky infrastructure; however, this scenario applies very rarely.
16. Requests for packages from managed devices, including mobile devices, are transferred to the Web Server (on page [47](#)), which is on the same device as the Administration Server.
17. For iOS mobile devices only: data from the mobile device is transferred through TLS port 443 to the iOS MDM Server, which is on the same device as the Administration Server or on the connection gateway.

See also:

Ports used by Kaspersky Security Center	65
Using a distribution point as connection gateway	594

Administration Server in DMZ, managed devices on Internet

The figure below shows data traffic if the Administration Server is in the demilitarized zone (DMZ) and the managed devices, including mobile devices, are on the Internet.



In this figure, a connection gateway is not in use: the mobile devices connect to the Administration Server directly.

The arrows indicate the initiation of traffic: each arrow points from a device that initiates the connection to the device that "answers" the call. The number of the port and the name of the protocol used for data transfer are provided. Each arrow has a number label, and details about the corresponding data traffic are as follows:

1. Administration Server sends data to the database (see section "Administration Server and DBMS" on page [110](#)). If you install the Administration Server and the database on different devices, you must make available the necessary ports on the device where the database is located (for example, port 3306 for MySQL Server and MariaDB Server, or port 1433 for Microsoft SQL Server). Please refer to the DBMS documentation for the relevant information.
2. Requests for communication from the Administration Server are transferred to all non-mobile managed devices through UDP port 15000 (see section "Administration Server and client device: Managing the security application" on page [112](#)).

Network Agents send requests to each other within one broadcasting domain. The data is then sent to the Administration Server and is used for defining the limits of the broadcasting domain and for automatic assignment of distribution points (if this option is enabled).

3. Information about shutdown of the managed devices is transferred from Network Agent to the Administration Server through UDP port 13000.
4. The Administration Server receives connection from Network Agents (see section "Administration Server and client device: Managing the security application" on page [112](#)) and from secondary Administration Servers (see section "Hierarchy of Administration Servers: primary Administration Server and secondary Administration Server" on page [114](#)) through SSL port 13000.

If you used an earlier version of Kaspersky Security Center, the Administration Server on your network can receive connection from Network Agents through non-SSL port 14000. Kaspersky Security Center also supports connection of Network Agents through port 14000, although using SSL port 13000 is recommended.

The distribution point was called "Update agent" in earlier versions of Kaspersky Security Center.

4a. A connection gateway (on page [57](#)) in DMZ also receives connection from the Administration Server through SSL port 13000 (see section "Administration Server and two devices in DMZ: a connection gateway and a client device" on page [117](#)). Because a connection gateway in DMZ cannot reach the Administration Server's ports, the Administration Server creates and maintains a permanent signal connection with a connection gateway. The signal connection is not used for data transfer; it is only used for sending an invitation to the network interaction. When the connection gateway needs to connect to the Server, it notifies the Server through this signal connection, and then the Server creates the required connection for data transfer.

Out-of-office devices connect to the connection gateway through SSL port 13000 (see section "Administration Server and two devices in DMZ: a connection gateway and a client device" on page [117](#)) as well.

5. The managed devices (except for mobile devices) request activation through TCP port 17000. This is not necessary if the device has its own access to the Internet; in this case, the device sends the data to Kaspersky servers over the Internet directly.
6. Data from MMC-based Administration Console is transferred to the Administration Server through port 13291 (see section "Administration Server and Administration Console" on page [111](#)). (The Administration Console can be installed on the same or on a different device.)
7. Applications on a single device exchange local traffic (either on the Administration Server or on a managed device). No external ports have to be opened.

8. Data from the Administration Server to the Kaspersky servers (such as KSN data or information about licenses) and data from the Kaspersky servers to the Administration Server (such as application updates and anti-virus database updates) are transferred using the HTTPS protocol.

If you do not want your Administration Server to have access to the Internet, you must manage this data manually.

9. Kaspersky Security Center 13 Web Console Server sends data to the Administration Server, which may be installed on the same or on a different device, through TLS port 13299.
 - 9a. Data from the browser, which is installed on a separate device of the administrator, is transferred to Kaspersky Security Center 13 Web Console Server through TLS port 8080 (see section "Administration Server and Kaspersky Security Center 13 Web Console" on page [118](#)). The Kaspersky Security Center 13 Web Console Server can be installed either on the Administration Server or on another device.
10. For Android mobile devices only: data from the Administration Server is transferred to Google servers. This connection is used to notify Android mobile devices that they are required to connect to the Administration Server. Then push notifications are sent to the mobile devices.
11. For Android mobile devices only: push notifications from Google servers are sent to the mobile device. This connection is used to notify mobile devices that they are required to connect to the Administration Server.
12. For iOS mobile devices only: data from the iOS MDM Server (on page [145](#)) is transferred to Apple Push Notification servers. Then push notifications are sent to the mobile devices.
13. For iOS mobile devices only: push notifications are sent from Apple servers to the mobile device. This connection is used to notify iOS mobile devices that they are required to connect to the Administration Server.
14. For mobile devices only: data from the managed application is transferred to the Administration Server (or to the connection gateway) through TLS port 13292 / 13293 (see section "Activating and managing the security application on a mobile device" on page [119](#))—directly or through a Microsoft Forefront Threat Management Gateway (TMG).
15. For mobile devices only: data from the mobile device is transferred to the Kaspersky infrastructure.
 - 15a. If a mobile device does not have Internet access, the data is transferred to Administration Server through port 17100 (see section "Activating and managing the security application on a mobile device" on page [119](#)), and the Administration Server sends it to the Kaspersky infrastructure; however, this scenario applies very rarely.
16. Requests for packages from managed devices, including mobile devices, are transferred to the Web Server (on page [47](#)), which is on the same device as the Administration Server.
17. For iOS mobile devices only: data from the mobile device is transferred through TLS port 443 to the iOS MDM Server, which is on the same device as the Administration Server or on the connection gateway.

See also:

Ports used by Kaspersky Security Center	65
Internet access: Administration Server in DMZ	131

Interaction of Kaspersky Security Center components and security applications: more information

This section provides the schemas for interaction of Kaspersky Security Center components and managed security applications. The schemas provide the numbers of the ports that must be available and the names of the processes that open those ports.










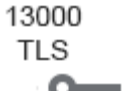



In this chapter



Conventions used in interaction schemas	108
Administration Server and DBMS	110
Administration Server and Administration Console	111
Administration Server and client device: Managing the security application.....	112
Upgrading software on a client device through a distribution point	113
Hierarchy of Administration Servers: primary Administration Server and secondary Administration Server	114
Hierarchy of Administration Servers with a secondary Administration Server in DMZ.....	115
Administration Server, a connection gateway in a network segment, and a client device	116
Administration Server and two devices in DMZ: a connection gateway and a client device.....	117
Administration Server and Kaspersky Security Center 13 Web Console.....	118
Activating and managing the security application on a mobile device	119

Conventions used in interaction schemas

The following table provides the conventions used across the schemas.

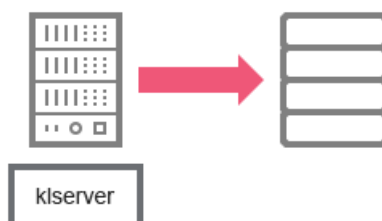
Table 3. Document conventions

Icon	Meaning
	Administration Server
	Secondary Administration Server
	DBMS
	Client device (that has Network Agent and an application from Kaspersky Endpoint Security family installed, or has a different security application installed that Kaspersky Security Center can manage)
	Connection gateway
	Distribution point
	Mobile client device with Kaspersky Security for Mobile
	Browser on the user's device
	Process running on the device and opening a port
	Port and its number
	TCP traffic (the arrow direction shows the traffic flow direction)
	UDP traffic (the arrow direction shows the traffic flow direction)
	COM invoke

	DBMS transport
	DMZ boundary

Administration Server and DBMS

Data from the Administration Server enter the SQL Server, MySQL, or MariaDB database.

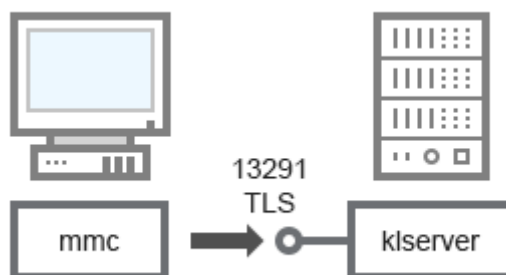


If you install the Administration Server and the database on different devices, you must make available the necessary ports on the device where the database is located (for example, port 3306 for MySQL Server and MariaDB Server, or port 1433 for Microsoft SQL Server). Please refer to the DBMS documentation for the relevant information.

See also:

Conventions used in interaction schemas	108
Interaction of Kaspersky Security Center components and security applications: more information.....	108
Ports used by Kaspersky Security Center	65
How to select a DBMS for Administration Server	128

Administration Server and Administration Console



For schema clarifications, see the table below.

Table 4. Administration Server and Administration Console (traffic)

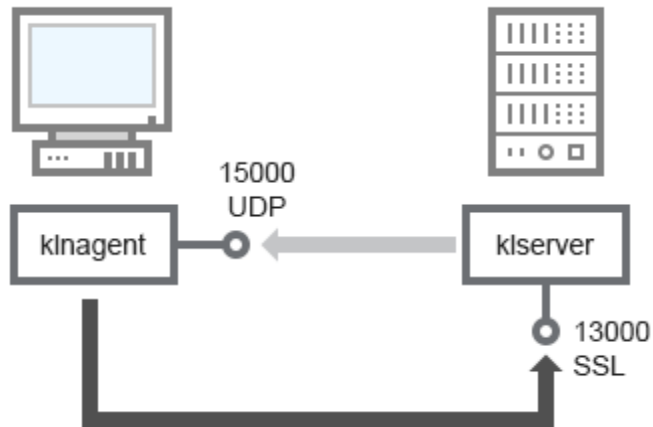
Device	Port number	Name of the process that opens the port	Protocol	TLS	Port purpose
Administration Server	13291	klserver	TCP	Yes	Receiving connections from Administration Console

See also:

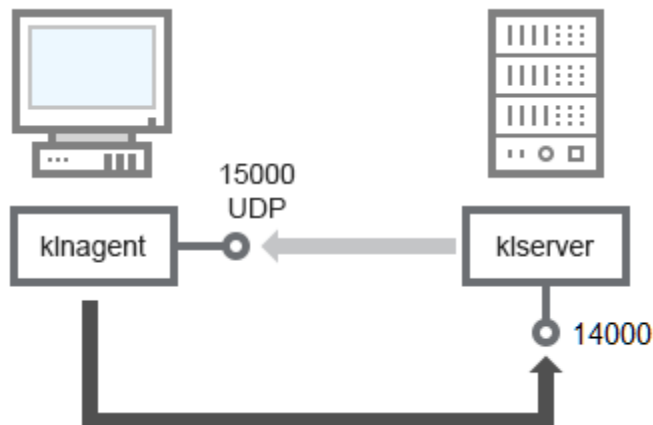
- Conventions used in interaction schemas[108](#)
- Interaction of Kaspersky Security Center components and security applications: more information.....[108](#)
- Ports used by Kaspersky Security Center[65](#)

Administration Server and client device: Managing the security application

The Administration Server receives connection from Network Agents via SSL port 13000 (see figure below).



If you used an earlier version of Kaspersky Security Center, the Administration Server on your network can receive connections from Network Agents via non-SSL port 14000 (see figure below). Kaspersky Security Center 13 also supports connection of Network Agents via port 14000, although using SSL port 13000 is recommended.



For clarifications of schemas, see the table below.

Table 5. Administration Server and client device: Managing the security application (traffic)

Device	Port number	Name of the process that opens the port	Protocol	TLS (for TCP only)	Port purpose
Network Agent	15000	klagent	UDP	Null	Multicasting for Network Agents
Administration Server	13000	klserver	TCP	Yes	Receiving connections from Network Agents
Administration Server	14000	klserver	TCP	No	Receiving connections from Network Agents

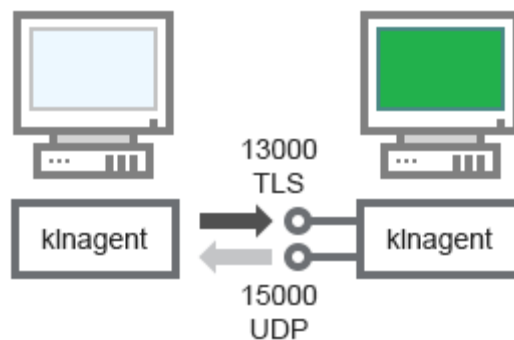
See also:

Conventions used in interaction schemas[108](#)

Interaction of Kaspersky Security Center components and security applications: more information.....[108](#)

Ports used by Kaspersky Security Center[65](#)

Upgrading software on a client device through a distribution point



For schema clarifications, see the table below.

Table 6. Upgrading software through a distribution point (traffic)

Device	Port number	Name of the process that opens the port	Protocol	TLS (for TCP only)	Port purpose
Network Agent	15000	klagent	UDP	Null	Multicasting for Network Agents
Distribution point	13000	klagent	TCP	Yes	Receiving connections from Network Agents

See also:

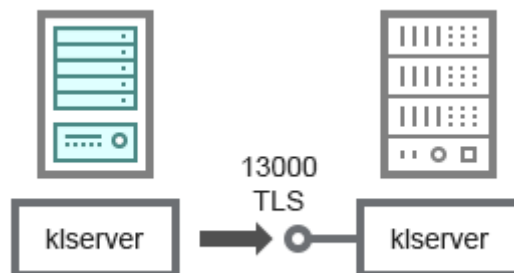
- Conventions used in interaction schemas[108](#)
- Interaction of Kaspersky Security Center components and security applications: more information.....[108](#)
- Ports used by Kaspersky Security Center[65](#)

Hierarchy of Administration Servers: primary Administration Server and secondary Administration Server

The schema (see figure below) shows how to use port 13000 to ensure interaction between Administration Servers combined into a hierarchy.

When combining two Administration Servers into a hierarchy, (see section "Creating a hierarchy of Administration Servers: adding a secondary Administration Server" on page [597](#)) make sure that port 13291 is accessible on both Administration Servers. Administration Console connects to the Administration Server (see section "Administration Server and Administration Console" on page [111](#)) through port 13291.

Subsequently, when the Administration Servers are combined into a hierarchy, you will be able to administer both of them by using Administration Console connected to the primary Administration Server. Therefore, the accessibility of port 13291 of the primary Administration Server is the only prerequisite.



For schema clarifications, see the table below.

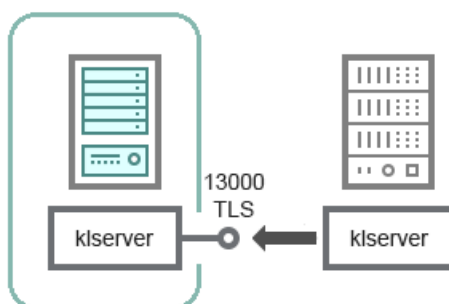
Table 7. Hierarchy of Administration Servers (traffic)

Device	Port number	Name of the process that opens the port	Protocol	TLS	Port purpose
Primary Administration Server	13000	klserver	TCP	Yes	Receiving connections from secondary Administration Servers

See also:

- Conventions used in interaction schemas[108](#)
- Interaction of Kaspersky Security Center components and security applications: more information.....[108](#)
- Ports used by Kaspersky Security Center[65](#)
- Creating a hierarchy of Administration Servers: adding a secondary Administration Server.....[597](#)

Hierarchy of Administration Servers with a secondary Administration Server in DMZ



The schema shows a hierarchy of Administration Servers in which the secondary Administration Server located in DMZ receives a connection from the primary Administration Server (see the table below for schema clarifications). When combining two Administration Servers into a hierarchy, (see section "Creating a hierarchy of Administration Servers: adding a secondary Administration Server" on page [597](#)) make sure that port 13291 is accessible on both Administration Servers. Administration Console connects to the Administration Server (see section "Administration Server and Administration Console" on page [111](#)) through port 13291.

Subsequently, when the Administration Servers are combined into a hierarchy, you will be able to administer both of them by using Administration Console connected to the primary Administration Server. Therefore, the accessibility of port 13291 of the primary Administration Server is the only prerequisite.

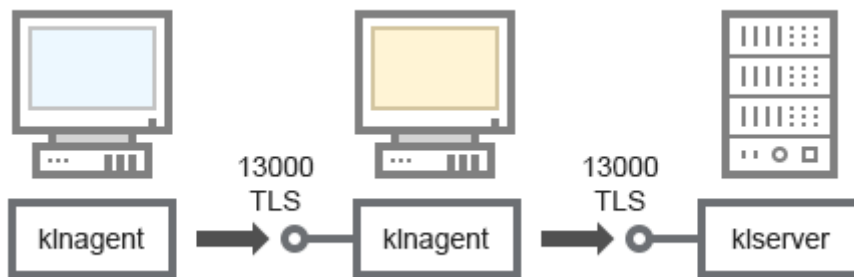
Table 8. Hierarchy of Administration Servers with a secondary Administration Server in DMZ (traffic)

Device	Port number	Name of the process that opens the port	Protocol	TLS	Port purpose
Secondary Administration Server	13000	klserver	TCP	Yes	Receiving connections from the primary Administration Server

See also:

- Conventions used in interaction schemas[108](#)
- Interaction of Kaspersky Security Center components and security applications: more information.....[108](#)
- Ports used by Kaspersky Security Center[65](#)
- Configuring the connection of Administration Console to Administration Server[278](#)
- Creating a hierarchy of Administration Servers: adding a secondary Administration Server.....[597](#)

Administration Server, a connection gateway in a network segment, and a client device



For schema clarifications, see the table below.

Table 9. Administration Server, a connection gateway in a network segment, and a client device

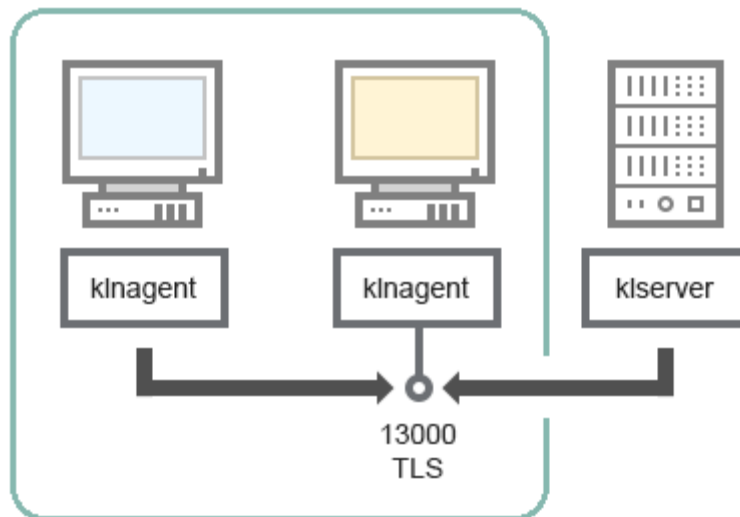
(traffic)

Device	Port number	Name of the process that opens the port	Protocol	TLS	Port purpose
Administration Server	13000	klserver	TCP	Yes	Receiving connections from Network Agents
Network Agent	13000	klagent	TCP	Yes	Receiving connections from Network Agents

See also:

- Conventions used in interaction schemas[108](#)
- Interaction of Kaspersky Security Center components and security applications: more information.....[108](#)
- Ports used by Kaspersky Security Center[65](#)

Administration Server and two devices in DMZ: a connection gateway and a client device



For schema clarifications, see the table below.

Table 10. Administration Server with a connection gateway in a network segment and a client

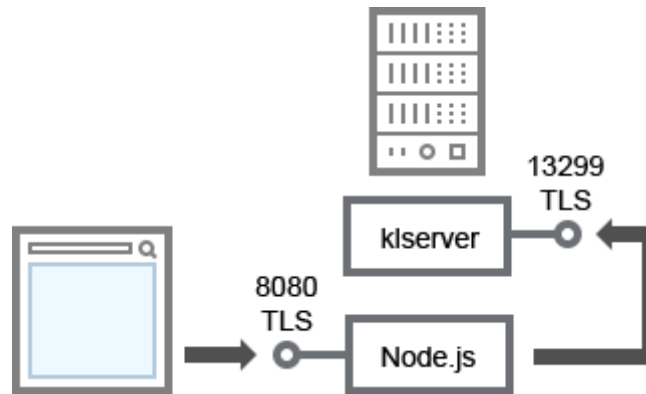
device (traffic)

Device	Port number	Name of the process that opens the port	Protocol	TLS	Port purpose
Network Agent	13000	klagent	TCP	Yes	Receiving connections from Network Agents

See also:

- Conventions used in interaction schemas[108](#)
- Interaction of Kaspersky Security Center components and security applications: more information.....[108](#)
- Ports used by Kaspersky Security Center[65](#)

Administration Server and Kaspersky Security Center 13 Web Console



For schema clarifications, see the table below.

Table 11. Administration Server and Kaspersky Security Center 13 Web Console (traffic)

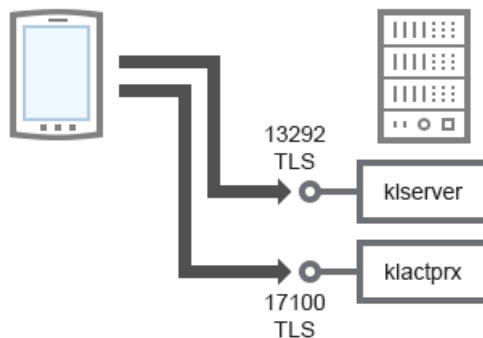
Device	Port number	Name of the process that opens the port	Protocol	TLS	Port purpose
Administration Server	13299	klserver	TCP	Yes	Receiving connections from Kaspersky Security Center 13 Web Console to the Administration Server over OpenAPI
Kaspersky Security Center 13 Web Console Server or Administration Server	8080	Node.js: Server-side JavaScript	TCP	Yes	Receiving connections from Kaspersky Security Center 13 Web Console

Kaspersky Security Center 13 Web Console can be installed on the Administration Server or on another device.

See also:

- Conventions used in interaction schemas[108](#)
- Interaction of Kaspersky Security Center components and security applications: more information.....[108](#)
- Ports used by Kaspersky Security Center[65](#)

Activating and managing the security application on a mobile device



For schema clarifications, see the table below.

Table 12. Activating and managing the security application on a mobile device (traffic)

Device	Port number	Name of the process that opens the port	Protocol	TLS	Port purpose
Administration Server	13292	klserver	TCP	Yes	Receiving connections from Administration Console to Administration Server
Administration Server	17100	klserver	TCP	Yes	Receiving connections for application activation from mobile devices

See also:

Conventions used in interaction schemas	108
Interaction of Kaspersky Security Center components and security applications: more information.....	108
Ports used by Kaspersky Security Center	65
Deploying a system for management via Exchange ActiveSync protocol	188

Deployment best practices

Kaspersky Security Center is a distributed application. Kaspersky Security Center includes the following applications:

- Administration Server—The core component, designed for managing devices of an organization and storing data in a DBMS.
- Administration Console—The basic tool for the administrator. Administration Console is shipped together with Administration Server, but it can also be installed individually on one or several devices run by the administrator.
- Network Agent—Designed for managing the security application installed on a device, as well as getting information about that device and transferring this information to the Administration Server. Network Agents are installed on devices of an organization.

Deployment of Kaspersky Security Center on an organization's network is performed as follows:

- Installation of Administration Server
- Installation of Administration Console on the administrator's device
- Installation of Network Agent and the security application on devices of the enterprise

In this section

Preparation for deployment	122
Deploying Network Agent and the security application	150
Deploying mobile device management systems	188

Preparation for deployment

This section describes steps you must take before deploying Kaspersky Security Center.

In this chapter

Planning Kaspersky Security Center deployment	123
Preparing to mobile device management	141
Information about Administration Server performance	146

Planning Kaspersky Security Center deployment

This section provides information about the most convenient options for deployment of Kaspersky Security Center components on an organization's network, depending on the following criteria:

- Total number of devices
- Units (local offices, branches) that are detached organizationally or geographically
- Separate networks connected by narrow channels
- Need for Internet access to the Administration Server

In this chapter

Typical schemes of protection system deployment.....	123
About planning Kaspersky Security Center deployment in an organization's network .	124
Selecting a structure for protection of an enterprise.....	125
Standard configurations of Kaspersky Security Center.....	126
How to select a DBMS for Administration Server.....	128
Selecting a DBMS.....	129
Managing mobile devices with Kaspersky Endpoint Security for Android.....	130
Providing Internet access to the Administration Server.....	130
About distribution points	133
Calculating the number and configuration of distribution points.....	134
A hierarchy of Administration Servers	135
Virtual Administration Servers	135
Information about limitations of Kaspersky Security Center.....	136
Network load.....	137

Typical schemes of protection system deployment

This section describes the standard deployment schemes of a protection system in an enterprise network using Kaspersky Security Center.

The system must be protected against any type of unauthorized access. We recommend that you install all available security updates for your operating system before installing the application on your device and physically protect Administration Server(s) and distribution point(s).

You can use Kaspersky Security Center to deploy a protection system on a corporate network by means of the following deployment schemes:

- Deploying a protection system through Kaspersky Security Center, in one of the following ways:
 - Through Administration Console
 - Through Kaspersky Security Center 13 Web Console

Kaspersky applications are automatically installed on client devices, which in turn are automatically connected to the Administration Server by using Kaspersky Security Center.

The basic deployment scheme is protection system deployment through Administration Console. Using Kaspersky Security Center 13 Web Console allows you to launch installation of Kaspersky applications from a browser.

- Deploying a protection system manually using stand-alone installation packages generated by Kaspersky Security Center.

Installation of Kaspersky applications on client devices and the administrator's workstation is performed manually; the settings for connecting client devices to the Administration Server are specified when Network Agent is installed.

This deployment method is recommended in cases when remote installation is not possible.

Kaspersky Security Center also allows you to deploy your protection system using Microsoft Active Directory® group policies.

About planning Kaspersky Security Center deployment in an organization's network

One Administration Server can support a maximum of 100,000 devices. If the total number of devices on an organization's network exceeds 100,000, multiple Administration Servers must be deployed on that network and combined into a hierarchy for convenient centralized management.

If an organization includes large-scale remote local offices (branches) with their own administrators, it is useful to deploy Administration Servers in those offices. Otherwise, those offices must be viewed as detached networks connected by low-throughput channels; see section "Standard configuration: A few large-scale offices run by their own administrators (on page [127](#))".

When detached networks connected with narrow channels are used, traffic can be saved by assigning one or several Network Agents to act as distribution points (see table for calculation of the number of distribution points (see section "Calculating the number and configuration of distribution points" on page [134](#))). In this case, all devices on a detached network retrieve updates from such local update centers. Actual distribution points can download updates both from the Administration Server (default scenario), and from Kaspersky servers on the Internet (see section "Standard configuration: Multiple small remote offices (on page [127](#))").

Section "Standard configurations of Kaspersky Security Center (on page [126](#))" provides detailed descriptions of the standard configurations of Kaspersky Security Center. When planning the deployment, choose the most suitable standard configuration, depending on the organization's structure.

At the stage of deployment planning, the assignment of the special certificate X.509 to the Administration Server must be considered. Assignment of the X.509 certificate to the Administration Server may be useful in the following cases (partial list):

- Inspecting secure socket layer (SSL) traffic by means of an SSL termination proxy or for using a reverse proxy
- Integration with the public keys infrastructure (PKI) of an organization

- Specifying required values in certificate fields
- Providing the required encryption strength of a certificate

Selecting a structure for protection of an enterprise

Selection of a structure for protection of an organization is defined by the following factors:

- Organization's network topology.
- Organizational structure.
- Number of employees in charge of the network protection, and allocation of their responsibilities.
- Hardware resources that can be allocated to protection management components.
- Throughput of communication channels that can be allocated to maintenance of protection components on the organizational network.
- Time limits for execution of critical administrative operations on the organization's network. Critical administrative operations include, for example, the distribution of anti-virus databases and modification of policies for client devices.

When you select a protection structure, it is recommended first to estimate the available network and hardware resources that can be used for the operation of a centralized protection system.

To analyze the network and hardware infrastructure, it is recommended that you follow the process below:

1. Define the following settings of the network on which the protection will be deployed:
 - Number of network segments.
 - Speed of communication channels between individual network segments.
 - Number of managed devices in each of the network segments.
 - Throughput of each communication channel that can be allocated to maintain the operation of the protection.
2. Determine the maximum allowed time for the execution of key administrative operations for all managed devices.
3. Analyze information from steps 1 and 2, as well as data from load testing of the administration system (see section "Network load" on page [137](#)). Based on the analysis, answer the following questions:
 - Is it possible to serve all the clients with a single Administration Server, or is a hierarchy of Administration Servers required?
 - Which hardware configuration of Administration Servers is required in order to deal with all the clients within the time limits specified in step 2?
 - Is it required to use distribution points to reduce load on communication channels?

Upon obtaining answers to the questions in step 3 above, you can compile a set of allowed structures of the organization's protection.

On the organization's network you can use one of the following standard protection structures:

- One Administration Server. All client devices are connected to a single Administration Server. Administration Server functions as distribution point.

- One Administration Server with distribution points. All client devices are connected to a single Administration Server. Some of the networked client devices function as distribution points.
- Hierarchy of Administration Servers. For each network segment an individual Administration Server is allocated and becomes part of a general hierarchy of Administration Servers. The primary Administration Server functions as distribution point.
- Hierarchy of Administration Servers with distribution points. For each network segment, an individual Administration Server is allocated and becomes part of a general hierarchy of Administration Servers. Some of the networked client devices function as distribution points.

See also:

Standard configuration of distribution points: Single office.....	588
Standard configuration: A few large-scale offices run by their own administrators.....	127
Standard configuration: Multiple small remote offices.....	127

Standard configurations of Kaspersky Security Center

This section describes the following standard configurations used for deployment of Kaspersky Security Center components on an organization's network:

- Single office
- A few large-scale offices, which are geographically detached and run by their own administrators
- Multiple small offices, which are geographically detached

In this section

Standard configuration: Single office.....	126
Standard configuration: A few large-scale offices run by their own administrators.....	127
Standard configuration: Multiple small remote offices.....	127

Standard configuration: Single office

One or several Administration Servers can be deployed on the organization's network. The number of Administration Servers can be selected either based on available hardware, or on the total number of managed devices.

One Administration Server can support up to 100 000 devices. You must consider the possibility of increasing the number of managed devices in the near future: it may be useful to connect a slightly smaller number of devices to a single Administration Server.

Administration Servers can be deployed either on the internal network, or in the DMZ, depending on whether Internet access to the Administration Servers is required.

If multiple Servers are used, it is recommended that you combine them into a hierarchy. Using an Administration Server hierarchy allows you to avoid duplicated policies and tasks, and handle the whole set of managed devices as if they are managed by a single Administration Server (that is, search for devices, build selections of devices, and create reports).

See also:

About distribution points	133
Ports used by Kaspersky Security Center	65

Standard configuration: A few large-scale offices run by their own administrators

If an organization has a few large-scale, geographically separate offices, you must consider the option of deploying Administration Servers at each of the offices. One or several Administration Servers can be deployed per office, depending on the number of client devices and hardware available. In this case, each of the offices can be viewed as a "Standard configuration: Single office (on page [126](#))". For ease of administration, it is recommended to combine all of the Administration Servers into a hierarchy (possibly multi-level).

If some employees move between offices with their devices (laptops), a rule for Network Agent switching between Administration Servers must be created in the Network Agent policy.

See also:

About connection profiles for out-of-office users	287
Standard configuration: Single office	126
Ports used by Kaspersky Security Center	65

Standard configuration: Multiple small remote offices

This standard configuration provides for a headquarters office and many remote small offices that may communicate with the HQ office over the Internet. Each of the remote offices may be located behind a Network Address Translation (NAT), that is, no connection can be established between two remote offices because they are isolated.

An Administration Server must be deployed at the headquarters office, and one or multiple distribution points must be assigned to all other offices. If the offices are linked through the Internet, it may be useful to create a *Download updates to the repositories of distribution points* task for the distribution points (see section "Creating the Downloading updates to the repositories of distribution points task" on page [417](#)), so that they will download updates directly from Kaspersky servers, not from the Administration Server.

If some devices at a remote office have no direct access to the Administration Server (for example, access to the Administration Server is provided over the Internet but some devices have no Internet access), distribution points must be switched into connection gateway mode. In this case, Network Agents on devices at the remote office will be connected, for further synchronization, to the Administration Server—but through the gateway, not directly.

As the Administration Server, most probably, will not be able to poll the remote office network, it may be useful to turn this function over to a distribution point.

The Administration Server will not be able to send notifications to port 15000 UDP to managed devices located behind the NAT at the remote office. To resolve this issue, it may be useful to enable the mode of continuous connection to the Administration Server in the properties of devices acting as distribution points (**Do not disconnect from the Administration Server** check box). This mode is available if the total number of distribution points does not exceed 300.

See also:

About distribution points	133
Providing Internet access to the Administration Server.....	130
Ports used by Kaspersky Security Center	65

How to select a DBMS for Administration Server

When selecting the database management system (DBMS) to be used by an Administration Server, you must take into account the number of devices covered by the Administration Server.

SQL Server Express Edition has limitations on the memory volume used, number of CPU cores used, and maximum size of the database. Therefore, you cannot use SQL Server Express Edition if your Administration Server covers more than 10 000 devices, or if Application Control is used on managed devices.

If your Administration Server covers more than 10 000 devices, we recommend that you use SQL Server versions with fewer limitations, such as: SQL Server Workgroup Edition, SQL Server® Web Edition, SQL Server Standard Edition, or SQL Server Enterprise Edition.

If the Administration Server covers 20 000 devices (or fewer) and if Application Control is not used on managed devices, you can use MariaDB Server 10.3 as the DBMS.

If the Administration Server covers 10 000 devices (or less), and if Application Control is not used on managed devices, you can also use MySQL 5.5, 5.6, or 5.7 as the DBMS. MySQL versions 5.5.1, 5.5.2, 5.5.3, 5.5.4, and 5.5.5 are no longer supported.

If you are using SQL Server 2019 as a DBMS, you have to perform the following after installing Kaspersky Security Center:

1. Connect to SQL Server using SQL Management Studio.
2. Run the following commands (if you chose a different name (see section "Step 7. Configuring the SQL Server" on page [237](#)) for the database, use that name instead of KAV):

```
USE KAV  
  
GO  
  
ALTER DATABASE SCOPED CONFIGURATION SET  
TSQL_SCALAR_UDF_INLINING = OFF  
  
GO
```

3. Restart the SQL Server 2019 service.

Otherwise, using SQL Server 2019 may result in errors, such as "There is insufficient system memory in resource pool 'internal' to run this query".

See also:

Selecting a DBMS..... [129](#)

Selecting a DBMS

When installing Administration Server, you can select the DBMS that Administration Server will use. When selecting the database management system (DBMS) to be used by an Administration Server, you must take into account the number of devices covered by the Administration Server.

The following table lists the valid DBMS options, as well as the restrictions on their use.

Table 13. Restrictions on DBMS

DBMS	Restrictions
SQL Server Express Edition 2012 or later	Not recommended if you intend to run a single Administration Server for more than 10 000 devices or to use Application Control.
Local SQL Server edition, other than Express, 2012 or later	No limitations.
Remote SQL Server edition, other than Express, 2012 or later	Only valid if both devices are in the same Windows® domain; if the domains differ, a two-way trust relationship must be established between them.
Local or remote MySQL 5.5, 5.6, or 5.7 (MySQL versions 5.5.1, 5.5.2, 5.5.3, 5.5.4, and 5.5.5 are no longer supported)	Not recommended if you intend to run a single Administration Server for more than 10 000 devices or to use Application Control.
Local or remote MariaDB Server 10.3	Not recommended if you intend to run a single Administration Server for more than 20 000 devices or to use Application Control.

If you are using SQL Server 2019 as a DBMS, you have to perform the following after installing Kaspersky Security Center:

1. Connect to SQL Server using SQL Management Studio.
2. Run the following commands (if you chose a different name (see section "Step 7. Configuring the SQL Server" on page [237](#)) for the database, use that name instead of KAV):

```
USE KAV
GO

ALTER DATABASE SCOPED CONFIGURATION SET
    TSQL_SCALAR_UDF_INLINING = OFF
GO
```

3. Restart the SQL Server 2019 service.

Otherwise, using SQL Server 2019 may result in errors, such as "There is insufficient system memory in resource pool 'internal' to run this query".

Concurrent use of the SQL Server Express Edition DBMS by Administration Server and another application is strictly forbidden.

See also:

How to select a DBMS for Administration Server	128
Accounts for work with the DBMS	215

Managing mobile devices with Kaspersky Endpoint Security for Android

Mobile devices with installed Kaspersky Endpoint Security for Android™ (hereinafter referred to as KES devices) are managed by means of the Administration Server. Kaspersky Security Center 10 Service Pack 1, as well as later versions, supports the following features for managing KES devices:

- Handling mobile devices as client devices:
 - Membership in administration groups
 - Monitoring, such as viewing statuses, events, and reports
 - Modifying local settings and assigning policies for Kaspersky Endpoint Security for Android
- Sending commands in centralized mode
- Installing mobile apps packages remotely

Administration Server manages KES devices through TLS, TCP port 13292.

See also:

Providing Internet access to the Administration Server.....	130
---	---------------------

Providing Internet access to the Administration Server

The following cases require Internet access to the Administration Server:

- Regular updating of Kaspersky databases, software modules, and applications
- Updating third-party software

By default, Internet connection is not required for Administration Server to install Microsoft software updates on the managed devices. For example, the managed devices can download the Microsoft software updates directly from Microsoft Update servers or from Windows Server with Microsoft Windows Server Update Services (WSUS) deployed in your organization's network. Administration Server must be connected to the Internet in the following cases:

- When you use Administration Server as WSUS server

- To install updates of third-party software other than Microsoft software
- Fixing vulnerabilities in third-party software

Internet connection is required for Administration Server to perform the following tasks:

- To make a list of recommended fixes for vulnerabilities in Microsoft software. The list is created and regularly updated by Kaspersky specialists.
- To fix vulnerabilities in third-part software other than Microsoft software.
- Managing devices (laptops) of out-of-office users
- Managing devices in remote offices
- Interacting with primary or secondary Administration Servers located in remote offices
- Managing mobile devices

This section describes typical ways of providing access to the Administration Server over the Internet. Each of the cases focusing on providing Internet access to the Administration Server may require a dedicated certificate for the Administration Server.

See also:

Main installation scenario	59
Internet access: Administration Server on a local network.....	131
Internet access: Administration Server in DMZ	131
Internet access: Network Agent as connection gateway in DMZ	132

Internet access: Administration Server on a local network

If the Administration Server is located on the internal network of an organization, you might want to make TCP port 13000 of the Administration Server accessible from outside by means of port forwarding. If mobile device management is required, you might want to make accessible port 13292 TCP.

Internet access: Administration Server in DMZ

If the Administration Server is located in the DMZ of the organization's network, it has no access to the organization's internal network. Therefore, the following limitations apply:

- The Administration Server cannot detect new devices.
- The Administration Server cannot perform initial deployment of Network Agent through forced installation on devices on the internal network of the organization.

This only applies to the initial installation of Network Agent. Any further upgrades of Network Agent or the security application installation can, however, be performed by the Administration Server. At the same time, the initial deployment of Network Agents can be performed by other means, for example, through group policies of Microsoft® Active Directory®.

- The Administration Server cannot send notifications to managed devices through port 15000 UDP, which is not critical for the Kaspersky Security Center functioning.

- The Administration Server cannot poll Active Directory. However, results of Active Directory polling are not required in most scenarios.

If the above limitations are viewed as critical, they can be removed by using distribution points located on the organization's network:

- To perform initial deployment on devices without Network Agent, you first install Network Agent on one of the devices and then assign it the distribution point status. As a result, initial installation of Network Agent on other devices will be performed by the Administration Server through this distribution point.
- To detect new devices on the internal network of the organization and poll Active Directory, you must enable the relevant device discovery methods on one of the distribution points.
- To ensure a successful sending of notifications to port 15000 UDP on managed devices located on the internal network of the organization, you must cover the entire network with distribution points. In the properties of the distribution points that were assigned, select the **Do not disconnect from the Administration Server** check box. As a result, the Administration Server will establish a continuous connection to the distribution points while they will be able to send notifications to port 15000 UDP on devices that are on the organization's internal network (see section "About distribution points" on page [133](#)).

See also:

Administration Server in DMZ, managed devices on Internet[104](#)

Internet access: Network Agent as connection gateway in DMZ

Administration Server can be located on the internal network of the organization, and in that network's DMZ there can be a device with Network Agent running as a connection gateway (on page [57](#)) with reverse connectivity (Administration Server establishes a connection to Network Agent). In this case, the following conditions must be met to ensure Internet access:

- Network Agent must be installed on the device (see section "Local installation of Network Agent" on page [178](#)) that is in the DMZ. When you install Network Agent, in the **Connection gateway** window of the Setup Wizard, select **Use Network Agent as a connection gateway in DMZ**.
- The device with the installed connection gateway must be added as a distribution point (see section "Adding a connection gateway in the DMZ as a distribution point" on page [592](#)). When you add the connection gateway, in the **Add distribution point** window, select the **Select** → **Add connection gateway in DMZ by address** option.
- To use an Internet connection to connect external desktop computers to the Administration Server, the installation package for Network Agent must be corrected. In the properties of the created installation package (see section "Connecting external desktop computers to Administration Server" on page [286](#)), select the **Advanced** → **Connect to Administration Server by using connection gateway** option, and then specify the newly created connection gateway.

For the connection gateway in the DMZ, Administration Server creates a certificate signed with the Administration Server certificate. If the administrator decides to assign a custom certificate to Administration Server, it must be done before a connection gateway is created in the DMZ.

If some employees use laptops that can connect to Administration Server either from the local network or over the Internet, it may be useful to create a switching rule for Network Agent in the Network Agent's policy.

About distribution points

A device with Network Agent installed can be used as a distribution point. In this mode, Network Agent can perform the following functions:

- Distribute updates (these can be retrieved either from the Administration Server or from Kaspersky servers). In the latter case, the *Download updates to the repositories of distribution points* task (see section "Creating the Downloading updates to the repositories of distribution points task" on page [417](#)) must be created for the device that serves as the distribution point:
 - Install software (including initial deployment of Network Agents) on other devices.
 - Poll the network to detect new devices and update information about existing ones. A distribution point can apply the same device discovery methods as the Administration Server.

Deployment of distribution points on an organization's network has the following objectives:

- Reducing the load on the Administration Server.
- Optimizing traffic.
- Providing the Administration Server with access to devices in hard-to-reach spots of the organization's network. The availability of a distribution point on the network behind a NAT (in relation to the Administration Server) allows the Administration Server to perform the following actions:
 - Send notifications to devices over UDP.
 - Poll the network.
 - Perform initial deployment.

A distribution point is assigned for an administration group. In this case, the scope of the distribution point includes all devices within the administration group and all of its subgroups. However, the device that acts as the distribution point may not be included in the administration group to which it has been assigned.

You can make a distribution point function as a connection gateway. In this case, devices in the scope of the distribution point will be connected to the Administration Server through the gateway, not directly. This mode can be useful in scenarios that do not allow the establishment of a direct connection between the Administration Server and managed devices.

See also:

Adjustment of distribution points and connection gateways[587](#)

Calculating the number and configuration of distribution points

The more client devices a network contains, the more distribution points it requires. We recommend that you not disable automatic assignment of distribution points. When automatic assignment of distribution points is enabled, Administration Server assigns distribution points if the number of client devices is quite large and defines their configuration.

Using exclusively assigned distribution points

If you plan to use certain specific devices as distribution points (that is, exclusively assigned servers), you can opt out of using automatic assignment of distribution points. In this case, make sure that the devices that you intend to make distribution points have sufficient volume of free disk space, are not shut down regularly, and have Sleep mode disabled.

Table 14. Number of exclusively assigned distribution points on a network that contains a single network segment, based on the number of networked devices

Number of client devices in the network segment	Number of distribution points
Less than 300	0 (Do not assign distribution points)
More than 300	Acceptable: $(N/10,000 + 1)$, recommended: $(N/5,000 + 2)$, where N is the number of networked devices

Table 15. Number of exclusively assigned distribution points on a network that contains multiple network segments, based on the number of networked devices

Number of client devices per network segment	Number of distribution points
Less than 10	0 (Do not assign distribution points)
10... 100	1
More than 100	Acceptable: $(N/10,000 + 1)$, recommended: $(N/5,000 + 2)$, where N is the number of networked devices

Using standard client devices (workstations) as distribution points

If you plan to use standard client devices (that is, workstations) as distribution points, we recommend that you assign distribution points as shown in the tables below in order to avoid excessive load on the communication channels and on Administration Server:

Table 16. Number of workstations functioning as distribution points on a network that contains a single network segment, based on the number of networked devices

Number of client devices in the network segment	Number of distribution points
Less than 300	0 (Do not assign distribution points)
More than 300	$(N/300 + 1)$, where N is the number of networked devices; there must be at least 3 distribution points

Table 17. Number of workstations functioning as distribution points on a network that contains

multiple network segments, based on the number of networked devices

Number of client devices per network segment	Number of distribution points
Less than 10	0 (Do not assign distribution points)
10... 30	1
31... 300	2
More than 300	$(N/300 + 1)$, where N is the number of networked devices; there must be at least 3 distribution points

If a distribution point is shut down (or not available for some other reason), the managed devices in its scope can access the Administration Server for updates.

See also:

- Scenario: Regular updating Kaspersky databases and applications[1174](#)
- Standard configuration: Multiple small remote offices.....[127](#)

A hierarchy of Administration Servers

An MSP may run multiple Administration Servers. It can be inconvenient to administer several separate Administration Servers, so a hierarchy can be applied. A primary/secondary configuration for two Administration Servers provides the following options:

- A secondary Administration Server inherits policies and tasks from the primary Administration Server, thus preventing duplication of settings.
- Selections of devices on the primary Administration Server can include devices from secondary Administration Servers.
- Reports on the primary Administration Server can contain data (including detailed information) from secondary Administration Servers.

Virtual Administration Servers

On the basis of a physical Administration Server, multiple virtual Administration Servers can be created, which will be similar to secondary Administration Servers. Compared to the discretionary access model, which is based on access control lists (ACLs), the virtual Administration Server model is more functional and provides a larger degree of isolation. In addition to a dedicated structure of administration groups for assigned devices with policies and tasks, each virtual Administration Server features its own group of unassigned devices, own sets of reports, selected devices and events, installation packages, moving rules, etc. The functional scope of virtual Administration Servers can be used both by service providers (xSP) to maximize the isolation of customers, and by large-scale organizations with sophisticated workflows and numerous administrators.

Virtual Administration Servers are very similar to secondary Administration Servers, but with the following distinctions:

- A virtual Administration Server lacks most global settings and its own TCP ports.
- A virtual Administration Server has no secondary Administration Servers.

- A virtual Administration Server has no other virtual Administration Servers.
- A physical Administration Server views devices, groups, events, and objects on managed devices (items in Quarantine, applications registry, etc.) of all its virtual Administration Servers.
- A virtual Administration Server can only scan the network with distribution points connected.

Information about limitations of Kaspersky Security Center

The following table displays the limitations of the current version of Kaspersky Security Center.

Table 18. Limitations of Kaspersky Security Center

Type of limitation	Value
Maximum number of managed devices per Administration Server	100 000
Maximum number of devices with the Do not disconnect from the Administration Server check box selected	300
Maximum number of administration groups	10 000
Maximum number of events to store	45 000 000
Maximum number of policies	2000
Maximum number of tasks	2000
Maximum total number of Active Directory objects (organizational units (OUs) and accounts of users, devices, and security groups)	1 000 000
Maximum number of profiles in a policy	100
Maximum number of secondary Administration Servers on a single primary Administration Server	500
Maximum number of virtual Administration Servers	500
Maximum number of devices that a single distribution point can cover (distribution points can cover non-mobile devices only)	10 000
Maximum number of devices that may use a single connection gateway	10 000, including mobile devices
Maximum number of mobile devices per Administration Server	100 000 minus the number of stationary managed devices

Network load

This section contains information about the volume of network traffic that the client devices and Administration Server exchange during key administrative scenarios.

The main load on the network is caused by the following administrative scenarios in progress:

- Initial deployment of anti-virus protection
- Initial update of anti-virus databases
- Synchronization of a client device with Administration Server
- Regular updates of anti-virus databases
- Processing of events on client devices by Administration Server

In this chapter

Initial deployment of anti-virus protection	137
Initial update of anti-virus databases	138
Synchronizing a client with the Administration Server.....	139
Additional update of anti-virus databases	140
Processing of events from clients by Administration Server	140
Traffic per 24 hours.....	141

Initial deployment of anti-virus protection

This section provides information about traffic volume values after Network Agent 13 and Kaspersky Endpoint Security for Windows are installed on the client device (see the table below).

The Network Agent is installed using forced installation, when the files required for setup are copied by Administration Server to a shared folder on the client device. After installation, the Network Agent retrieves the distribution package of Kaspersky Endpoint Security for Windows, using the connection to the Administration Server.

Table 19. Traffic

Scenario	Network Agent installation for a single client device	Installing Kaspersky Endpoint Security for Windows on one client device (with databases updated)	Concurrent installation of Network Agent and Kaspersky Endpoint Security for Windows
Traffic from a client device to Administration Server, KB	1638.4	7843.84	9707.52
Traffic from Administration Server to a client device, KB	69 990.4	259 317.76	329 318.4
Total traffic (for a single client device), KB	71 628.8	267 161.6	339 025.92

After Network Agents are installed on the client devices, one of the devices in the administration group can be assigned to act as distribution point. It is used for distribution of installation packages. In this case, traffic volume transferred during initial deployment of anti-virus protection varies significantly depending on whether you are using IP multicasting.

If IP multicasting is used, installation packages are sent once to all running devices in the administration group. Thus, total traffic becomes N times smaller, where N stands for the total number of running devices in the administration group. If you are not using IP multicasting, the total traffic is identical to the traffic calculated as if the distribution packages are downloaded from the Administration Server. However, the package source is the distribution point, not the Administration Server.

Initial update of anti-virus databases

This section provides information about traffic volume values when starting the database update task for the first time on a client device (see the table below). The data in the table may vary slightly depending upon the current version of the anti-virus database.

Table 20. Traffic rates during initial update of anti-virus databases

Traffic flow	Value
Traffic from a client device to Administration Server, KB	1 064.96
Traffic from Administration Server to a client device, KB	29 306.88
Total traffic (for a single client device), KB	30 371.84

Synchronizing a client with the Administration Server

This scenario describes the state of the administration system when intensive data synchronization occurs between a client device and the Administration Server. Client devices connect to the Administration Server with the interval defined by the administrator. The Administration Server compares the status of data on a client device with that on the Server, records information in the database about the last client device connection, and synchronizes data.

This section contains information about traffic values for basic administration scenarios when connecting a client to the Administration Server (see table below). The data in the table may vary slightly depending upon the current version of the anti-virus database.

Table 21. Traffic

Scenario	Traffic from client devices to Administration Server, KB	Traffic from Administration Server to client devices, KB	Total traffic (for a single client device), KB
Initial synchronization prior to updating databases on a client device	699.44	568.42	1 267.86
Initial synchronization after updating databases on a client device	735.8	4 474.88	5 210.68
Synchronization with no changes on a client device and the Administration Server	11.99	6.73	18.72
Synchronization after changing the value of a setting in a group policy	9.79	11.39	21.18
Synchronization after changing the value of a setting in a group task	11.27	11.72	22.99
Forced synchronization with no changes on a client device	77.59	99.45	177.04

Overall traffic volume varies considerably depending on whether IP multicasting is used within administration groups. If IP multicasting is used, the total traffic volume decreases approximately by N times for the group, where N stands for the total number of devices included in the administration group.

The volume of traffic at initial synchronization before and after an update of the databases is specified for the

following cases:

- Installing Network Agent and a security application on a client device
- Moving a client device to an administration group
- Applying a policy and tasks that have been created for the group by default, to a client device

The table specifies traffic rates in case of changes to one of the protection settings that are included in the Kaspersky Endpoint Security policy settings. Data for other policy settings may differ from data displayed in the table.

Additional update of anti-virus databases

This section contains information about traffic rates in case of an incremental update of anti-virus databases 20 hours after the previous update (see table below). The data in the table may vary slightly depending upon the current version of the anti-virus database.

Table 22. Traffic rates during incremental update of anti-virus databases

Traffic flow	Value
Traffic from a client device to Administration Server, KB	2 611.2
Traffic from Administration Server to a client device, KB	53 237.76
Total traffic (for a single client device), KB	55 848.96

Traffic volume varies significantly depending on whether IP multicasting is used within administration groups. If IP multicasting is used, the total traffic volume decreases approximately by N times for the group, where N stands for the total number of devices included in the administration group.

Processing of events from clients by Administration Server

This section provides information about traffic volume values when a client device encounters a "Virus detected" event, which is then sent to the Administration Server and registered in the database (see table below).

Table 23. Traffic

Scenario	Data transfer to Administration Server when a "Virus detected" event occurs	Data transfer to Administration Server when nine "Virus detected" events occur
Traffic from a client device to Administration Server, KB	49.66	64.05
Traffic from Administration Server to a client device, KB	28.64	31.97
Total traffic (for a single client device), KB	78.3	96.02

Data in the table may vary slightly depending upon the current version of the anti-virus application and the events that are defined in its policy for registration in the Administration Server database.

Traffic per 24 hours

This section contains information about traffic rates for 24 hours of the administration system's activity in a "quiet" condition, when no data changes are made either by client devices or by the Administration Server (see table below).

Data presented in the table describe the network's condition after standard installation of Kaspersky Security Center and completion of the Quick Start Wizard. The frequency of synchronization of the client device with Administration Server was 20 minutes; updates were downloaded to the Administration Server repository once per hour.

Table 24. Traffic rates per 24 hours in idle state

Traffic flow	Value
Traffic from a client device to Administration Server, KB	3 235.84
Traffic from Administration Server to a client device, KB	64 378.88
Total traffic (for a single client device), KB	67 614.72

Preparing to mobile device management

This section provides the following information:

- About Exchange Mobile Device Server intended for management of mobile devices over the Exchange ActiveSync protocol
- About iOS MDM Server intended for management of iOS devices by installing dedicated iOS MDM profiles on them
- About management of mobile devices that have Kaspersky Endpoint Security for Android installed

In this section

Exchange Mobile Device Server	141
iOS MDM Server.....	145
Managing mobile devices with Kaspersky Endpoint Security for Android.....	146

Exchange Mobile Device Server

An Exchange Mobile Device Server allows you to manage mobile devices that are connected to an Administration Server using the Exchange ActiveSync protocol (EAS devices).

In this section

How to deploy an Exchange Mobile Device Server	142
Rights required for deployment of Exchange Mobile Device Server	142
Account for Exchange ActiveSync service	143

How to deploy an Exchange Mobile Device Server

If multiple Microsoft Exchange servers within a Client Access Server array have been deployed in the organization, an Exchange Mobile Device Server must be installed on each of the servers in that array. The **Cluster mode** option must be enabled in the Exchange Mobile Device Server Installation Wizard. In this case, the set of instances of the Exchange Mobile Device Server installed on servers in the array is called the cluster of Exchange Mobile Device Servers.

If no Client Access server array of Microsoft Exchange Servers has been deployed in the organization, an Exchange Mobile Device Server must be installed on a Microsoft Exchange Server that has Client Access. In this case, the **Standard mode** option must be enabled in the Setup Wizard of the Exchange Mobile Device Server.

Together with the Exchange Mobile Device Server, Network Agent must be installed on the device; it helps integrate the Exchange Mobile Device Server with Kaspersky Security Center.

The default scan scope of the Exchange Mobile Device Server is the current Active Directory domain in which it was installed. Deploying an Exchange Mobile Device Server on a server with Microsoft Exchange Server (versions 2010, 2013) installed allows you to expand the scan scope to include the entire domain forest in the Exchange Mobile Device Server (see section "Configuring the scan scope (on page [752](#))"). Information requested during a scan includes accounts of Microsoft Exchange server users, Exchange ActiveSync policies, and users' mobile devices connected to the Microsoft Exchange Server over Exchange ActiveSync protocol.

Multiple instances of Exchange Mobile Device Server cannot be installed within a single domain if they run in **Standard mode** being managed by a single Administration Server.
Within a single Active Directory domain forest, multiple instances of Exchange Mobile Device Server (or multiple clusters of Exchange Mobile Device Servers) cannot be installed either—if they run in **Standard mode** with an expanded scan scope that includes the entire domain forest and if they are connected to a single Administration Server.

See also:

Main installation scenario	59
Configuring the scan scope	752

Rights required for deployment of Exchange Mobile Device Server

Deployment of Exchange Mobile Device Server on Microsoft Exchange Server (2010, 2013) requires domain administrator rights and the Organization Management role. Deployment of Exchange Mobile Device Server on Microsoft Exchange Server (2007) requires domain administrator rights and membership in the Exchange Organization Administrators security group.

See also:

Main installation scenario	59
Account for Exchange ActiveSync service	143

Account for Exchange ActiveSync service

When an Exchange Mobile Device Server is installed, an account is automatically created in Active Directory:

- On Microsoft Exchange Server (2010, 2013): KLMDM4ExchAdmin***** account with the KLMDM Role Group role.
- On Microsoft Exchange Server (2007): KLMDM4ExchAdmin***** account, a member of the KLMDM Secure Group security group.

The Exchange Mobile Device Server service runs under this account.

If you want to cancel the automatic generation of an account, you need to create a custom one with the following rights:

- When using Microsoft Exchange Server (2010, 2013), the account must be assigned a role that has been allowed to execute the following cmdlets:
 - Get-CASMailbox
 - Set-CASMailbox
 - Remove-ActiveSyncDevice
 - Clear-ActiveSyncDevice
 - Get-ActiveSyncDeviceStatistics
 - Get-AcceptedDomain
 - Set-AdServerSettings
 - Get-ActiveSyncMailboxPolicy
 - New-ActiveSyncMailboxPolicy
 - Set-ActiveSyncMailboxPolicy
 - Remove-ActiveSyncMailboxPolicy
- When using a Microsoft Exchange Server (2007), the account must be granted the access rights to Active Directory objects (see the table below).

Table 25. Access rights to Active Directory objects

Access	Object	Cmdlet
Full	Thread "CN=Mobile Mailbox Policies,CN=<Organization name>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<Domain name>"	Add-ADPermission -User <User or group name> - Identity "CN=Mobile Mailbox Policies,CN=<Organization name>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<Domain name>" - InheritanceType All - AccessRight GenericAll
Read	Thread "CN=<Organization name>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<Domain name>"	Add-ADPermission -User <User or group name> - Identity "CN=<Organization name>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<Domain name>" - InheritanceType All - AccessRight GenericRead
Read/write	Properties msExchMobileMailboxPolicyLink and msExchOmaAdminWirelessEnable for objects in Active Directory	Add-ADPermission -User <User or group name> - Identity "DC=<Domain name>" - InheritanceType All - AccessRight ReadProperty,WriteProperty -Properties msExchMobileMailboxPolicyLink, msExchOmaAdminWirelessEnable
Extended right ms-Exch-Store-Active	Mailbox repositories of Exchange server, thread "CN=Databases,CN=Exchange Administrative Group (FYDIBOHF23SPDLT),CN=Administrative Groups,CN=<Organization name>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<Domain name>"	Get-MailboxDatabase Add-ADPermission -User <User or group name> - ExtendedRights ms-Exch-Store-Admin

See also:

Main installation scenario	59
Rights required for deployment of Exchange Mobile Device Server	142

iOS MDM Server

iOS MDM Server allows you to manage iOS devices by installing dedicated iOS MDM profiles on them. The following features are supported:

- Device lock
- Password reset
- Data wipe
- Installation or removal of apps
- Use of an iOS MDM profile with advanced settings (such as VPN settings, email settings, Wi-Fi settings, camera settings, certificates, etc.)

iOS MDM Server is a web service that receives inbound connections from mobile devices through its TLS port (by default, port 443), which is managed by Kaspersky Security Center using Network Agent. Network Agent is installed locally on a device with an iOS MDM Server deployed.

When deploying an iOS MDM Server, the administrator must perform the following actions:

- Provide Network Agent with access to the Administration Server
- Provide mobile devices with access to the TCP port of the iOS MDM Server

This section addresses two standard configurations of an iOS MDM Server.

See also:

Main installation scenario	59
Standard configuration: Kaspersky Device Management for iOS in DMZ	145
Standard configuration: iOS MDM Server on the local network of an organization	146

Standard configuration: Kaspersky Device Management for iOS in DMZ

An iOS MDM Server is located in the DMZ of an organization's local network with Internet access. A special feature of this approach is the absence of any problems when the iOS MDM web service is accessed from devices over the Internet.

Because management of an iOS MDM Server requires Network Agent to be installed locally, you must ensure the interaction of Network Agent with the Administration Server. You can ensure this by using one of the following methods:

- By moving the Administration Server to the DMZ.

- By using a connection gateway (see section "Internet access: Network Agent as connection gateway in DMZ" on page [132](#)):
 - a. On the device with iOS MDM Server deployed, connect Network Agent to the Administration Server through a connection gateway.
 - b. On the device with iOS MDM Server deployed, assign Network Agent to act as connection gateway.

See also:

Simplified deployment scheme	199
------------------------------------	---------------------

Standard configuration: iOS MDM Server on the local network of an organization

An iOS MDM Server is located on the internal network of an organization. Port 443 (default port) must be enabled for external access, for example, by publishing the iOS MDM web service on Microsoft Forefront® Threat Management Gateway (hereinafter referred to as TMG) (see section "Scheme for connecting KES devices to the Server involving Kerberos constrained delegation (KCD)" on page [209](#)).

Any standard configuration requires access to Apple web services for the iOS MDM Server (range 17.0.0.0/8) through TCP port 2195. This port is used for notifying devices of new commands by means of a dedicated service named APNs (see section "Configuring access to Apple Push Notification service" on page [206](#)).

Managing mobile devices with Kaspersky Endpoint Security for Android

Mobile devices with installed Kaspersky Endpoint Security for Android™ (hereinafter referred to as KES devices) are managed by means of the Administration Server. Kaspersky Security Center 10 Service Pack 1, as well as later versions, supports the following features for managing KES devices:

- Handling mobile devices as client devices:
 - Membership in administration groups
 - Monitoring, such as viewing statuses, events, and reports
 - Modifying local settings and assigning policies for Kaspersky Endpoint Security for Android
- Sending commands in centralized mode
- Installing mobile apps packages remotely

Administration Server manages KES devices through TLS, TCP port 13292.

See also:

Providing Internet access to the Administration Server.....	130
---	---------------------

Information about Administration Server performance

This section presents the results of performance testing of the Administration Server for different hardware configurations, as well as the limitations on connecting managed devices to the Administration Server.

In this section

Limitations on connection to an Administration Server	147
Results of Administration Server performance testing	148
Results of KSN Proxy server performance testing	150

Limitations on connection to an Administration Server

An Administration Server supports management of up to 100,000 devices without a loss in performance.

Limitations on connections to an Administration Server without a loss in performance:

- One Administration Server can support up to 500 virtual Administration Servers.
- The primary Administration Server supports no more than 1000 sessions simultaneously.
- Virtual Administration Servers support no more than 1000 sessions simultaneously.

See also:

Results of Administration Server performance testing	148
--	---------------------

Results of Administration Server performance testing

Results of Administration Server performance testing have allowed us to determine the maximum numbers of client devices with which Administration Server can be synchronized for specified time intervals. This information can be used to select the optimal scheme for deploying anti-virus protection on computer networks.

Devices with the following hardware configurations (see the tables below) were used for testing:

Table 26. Administration Server hardware configuration

Parameter	Value
CPU	Intel Xeon CPU E5506, clock speed of 2.13 GHz, 1 socket, 8 cores
RAM	4 GB
Hard drive	IBM ServeRAID M5015 SCSI Disk Device, 928 GB
Operating system	Microsoft Windows Server 2008 R2 Standard, Service Pack 1, 6.1.7601
Network	Broadcom BCM5709C NetXtreme II GigE (NDIS VBD Client)

Table 27. Hardware configuration of the SQL Server device

Parameter	Value
CPU	Intel Xeon CPU E5630, clock speed of 2.53 GHz, 1 socket, 8 cores, 16 logical processors
RAM	26 GB
Hard drive	IBM ServeRAID M5014 SCSI Disk Device, 929 GB
Operating system	Microsoft Windows Server 2012 R2 Standard, 6.3.9600
Network	Broadcom BCM5709C NetXtreme II GigE (NDIS VBD Client)

Administration Server supported creation of 500 virtual Administration Servers.

The synchronization interval was 15 minutes for every 10 000 managed devices (see the table below).

Table 28. Summarized results of Administration Server load testing

Synchronization interval (min)	Number of managed devices
15	10 000
30	20 000
45	30 000
60	40 000
75	50 000
90	60 000
105	70 000
120	80 000
135	90 000
150	100 000

If you connect Administration Server to a MySQL or SQL Express database server, it is not recommended to use the application to manage more than 10 000 devices. For the MariaDB database management system, the maximum recommended number of managed devices is 20 000.

Results of KSN Proxy server performance testing

If your enterprise network includes a large amount of client devices and they use the Administration Server as KSN Proxy server, the Administration Server hardware must meet specific requirements to be able to process the requests from the client devices. You can use the testing results below to evaluate the Administration Server load on your network and plan the hardware resources to provide for normal functioning of the KSN Proxy service.

The table below shows the Administration Server hardware configuration that was used for testing.

Table 29. Administration Server hardware configuration

Parameter	Value
CPU	Intel(R) Xeon(R) CPU E5540, clock speed of 2.53 GHz, 2 sockets, 8 cores, hyper-threading is off
RAM	18 GB
Operating system	Microsoft Windows Server 2012 R2 Standard

The table below shows the results of the test.

Table 30. Summarized results of KSN Proxy server performance testing

Parameter	Value
Maximum number of requests processed per second	about 15 000
Maximum CPU utilization	60%

Deploying Network Agent and the security application

To manage devices in an organization, you have to install Network Agent on each of them. Deployment of distributed Kaspersky Security Center on corporate devices normally begins with installation of Network Agent on them.

In Microsoft Windows XP, Network Agent might not perform the following operations correctly: downloading updates directly from Kaspersky servers (as a distribution point); functioning as KSN Proxy (as a distribution point); and detecting third-party vulnerabilities (if Vulnerability and Patch Management is used).

In this section

Initial deployment.....	151
Remote installation of applications on devices with Network Agent installed	160
Managing device restarts in the remote installation task.....	161
Suitability of databases updating in an installation package of a security application	161
Using tools for remote installation of applications in Kaspersky Security Center for running relevant executable files on managed devices.....	
Monitoring the deployment	163
Configuring installers	163
Virtual infrastructure.....	175
Support of file system rollback for devices with Network Agent	176
Local installation of applications	178

Initial deployment

If a Network Agent has already been installed on a device, remote installation of applications on that device is performed through this Network Agent. The distribution package of an application to be installed is transferred over communication channels between Network Agents and Administration Server, along with the installation settings defined by the administrator. To transfer the distribution package, you can use relay distribution nodes, that is, distribution points, multicast delivery, etc. For more details on how to install applications on managed devices with Network Agent already installed, see below in this section.

You can perform initial installation of Network Agent on devices running Windows, using one of the following methods:

- With third-party tools for remote installation of applications.
- By cloning an image of the administrator's hard drive with the operating system and Network Agent: using tools provided by Kaspersky Security Center for handling disk images, or using third-party tools.
- With Windows group policies: using standard Windows management tools for group policies, or in automatic mode, through the corresponding, dedicated option in the remote installation task of Kaspersky Security Center.
- In forced mode, using special options in the remote installation task of Kaspersky Security Center.
- By sending device users links to stand-alone packages generated by Kaspersky Security Center. Stand-alone packages are executable modules that contain the distribution packages of selected applications with their settings defined.
- Manually, by running application installers on devices.

On platforms other than Microsoft Windows, initial installation of Network Agent on managed devices must be performed through available third-party tools. You can upgrade Network Agent to a new version or install other Kaspersky applications on non-Windows platforms, using Network Agents (already installed on devices) to perform remote installation tasks. In this case, installation is identical to that on devices running Microsoft Windows.

When selecting a method and a strategy for deployment of applications on a managed network, you must consider

a number of factors (partial list):

- Organization's network (see section "Standard configurations of Kaspersky Security Center" on page [126](#)) configuration.
- Total number of devices.
- Presence of devices on the organization's network, which are not members of any Active Directory domain, and presence of uniform accounts with administrator rights on those devices.
- Capacity of the channel between the Administration Server and devices.
- Type of communication between Administration Server and remote subnets and capacity of network channels in those subnets.
- Security settings applied on remote devices at the start of deployment (such as use of UAC and Simple File Sharing mode).

In this section

Configuring installers	152
Installation packages	152
MSI properties and transform files.....	153
Deployment with third-party tools for remote installation of applications	153
About remote installation tasks in Kaspersky Security Center	154
Deployment by capturing and copying the hard drive image of a device.....	154
Deployment using group policies of Microsoft Windows	156
Forced deployment through the remote installation task of Kaspersky Security Center.....	158
Running stand-alone packages created by Kaspersky Security Center	159
Options for manual installation of applications	159

Configuring installers

Before starting deployment of Kaspersky applications on a network, you must specify the installation settings, that is, those defined during the application installation. When installing Network Agent, you should specify, at a minimum, an address for connection to Administration Server; some advanced settings may also be required. Depending on the installation method that you have selected, you can define settings in different ways. In the simplest case (manual interactive installation on a selected device), all relevant settings can be defined through the user interface of the installer.

This method of defining the settings is inappropriate for non-interactive ("silent") installation of applications on groups of devices. In general, the administrator must specify values for settings in centralized mode; those values can subsequently be used for non-interactive installation on selected networked devices.

Installation packages

The first and main method of defining the installation settings of applications is all-purpose and thus suitable for all installation methods, both with Kaspersky Security Center tools, and with most third-party tools. This method consists of creating installation packages of applications in Kaspersky Security Center.

Installation packages are generated using the following methods:

- Automatically, from specified distribution packages, on the basis of included *descriptors* (files with the *kud* extension that contain rules for installation and results analysis, and other information)
- From the executable files of installers or from installers in Microsoft Windows Installer (MSI) format, for standard or supported applications

Generated installation packages are organized hierarchically as folders with nested subfolders and files. In addition to the original distribution package, an installation package contains editable settings (including the installer's settings and rules for processing such cases as necessity of restarting the operating system in order to complete installation), as well as minor auxiliary modules.

Values of installation settings that would be specific for an individual supported application can be defined in the user interface of Administration Console when the installation package is created. When performing remote installation of applications through Kaspersky Security Center tools, installation packages are delivered to devices so that running the installer of an application makes all administrator-defined settings available for that application. When using third-party tools for installation of Kaspersky applications, you only have to ensure the availability of the entire installation package on the device, that is, the availability of the distribution package and its settings. Installation packages are created and stored by Kaspersky Security Center in a dedicated subfolder of the shared folder (see section "Defining a shared folder" on page [224](#)).

Do not specify any details of privileged accounts in the parameters of installation packages.

For the instruction about using this configuration method for Kaspersky applications before deployment through third-party tools, see section "Deployment using group policies of Microsoft Windows (on page [156](#))".

Immediately after Kaspersky Security Center installation, a few installation packages are automatically generated; they are ready for installation and include Network Agent packages and security application packages for Microsoft Windows.

Although the license key for an application can be set in the properties of an installation package, it is advisable to avoid this method of license distribution because there it is easy to obtain read access to installation packages. You should use automatically distributed license keys or installation tasks for license keys.

MSI properties and transform files

Another way of configuring installation on Windows platform is to define MSI properties and transform files. This method can be applied in the following cases:

- When installing through Windows group policies, by using regular Microsoft tools or other third-party tools for handling Windows group policies.
- When installing applications by using third-party tools intended for handling installers in Microsoft Installer format (see section "Configuring installers" on page [163](#)).

Deployment with third-party tools for remote installation of applications

When any tools for remote installation of applications (such as Microsoft System Center) are available in an organization, it is convenient to perform initial deployment by using those tools.

The following actions must be performed:

- Select the method for configuring installation that best suits the deployment tool to be used.
- Define the mechanism for synchronization between the modification of the settings of installation packages (through the Administration Console interface) and the operation of selected third-party tools used for deployment of applications from installation package data.
- When performing installation from a shared folder, you must make sure that this file resource has sufficient capacity.

See also:

Defining a shared folder	224
Configuring installers	163

About remote installation tasks in Kaspersky Security Center

Kaspersky Security Center provides various mechanisms for remote installation of applications, which are implemented as remote installation tasks (forced installation, installation by copying a hard drive image, installation through group policies of Microsoft Windows). You can create a remote installation task both for a specified administration group and for specific devices or a selection of devices (such tasks are displayed in Administration Console, in the **Tasks** folder). When creating a task, you can select installation packages (those of Network Agent and / or another application) to be installed within this task, as well as specify certain settings that define the method of remote installation. In addition, you can use the Remote Installation Wizard, which is based on creation of a remote installation task and results monitoring.

Tasks for administration groups affect both devices included in a specified group and all devices in all subgroups within that administration group. A task covers devices of secondary Administration Servers included in a group or any of its subgroups if the corresponding setting is enabled in the task.

Tasks for specific devices refresh the list of client devices at each run in accordance with the selection contents at the moment the task starts. If a selection includes devices that have been connected to secondary Administration Servers, the task will run on those devices, too. For details on those settings and installation methods see below in this section.

To ensure a successful operation of a remote installation task on devices connected to secondary Administration Servers, you must use the relaying task to relay installation packages used by your task to corresponding secondary Administration Servers in advance.

Deployment by capturing and copying the hard drive image of a device

If you need to install Network Agent on devices on which an operating system and other software also must be installed (or reinstalled), you can use the mechanism of capturing and copying the hard drive of that device.

To perform deployment by capturing and copying a hard drive:

1. Create a reference device with an operating system and the relevant software installed, including Network Agent and a security application.
2. Capture the reference image on the device and distribute that image on new devices through the dedicated task of Kaspersky Security Center.

To capture and install disk images, you can use either third-party tools available in the organization, or the feature provided (under the Vulnerability and Patch Management license) by Kaspersky Security Center (see section "Installing images of operating systems" on page [714](#)).

If you use any third-party tools to process disk images, you must delete the information that Kaspersky Security Center uses to identify the managed device, when performing deployment on a device from a reference image. Otherwise, Administration Server will not be able to properly distinguish devices that have been created by copying the same image (see section "Preparing a reference device with Network Agent installed for creating an image of operating system" on page [890](#)).
When capturing a disk image with Kaspersky Security Center tools, this issue is solved automatically.

Copying a disk image with third-party tools

When applying third-party tools for capturing the image of a device with Network Agent installed, use one of the following methods:

- Recommended method. When installing Network Agent on a reference device (see section "Preparing a reference device with Network Agent installed for creating an image of operating system" on page [890](#)), capture the device image before the first run of Network Agent service (because unique information identifying the device is created at the first connection of Network Agent to the Administration Server). After that, it is recommended that you avoid running Network Agent service until the completion of the image capturing operation.
- On the reference device, stop the Network Agent service and run the `klmover` utility with the `-dupfix` key. The utility `klmover` is included in the installation package of Network Agent. Avoid any subsequent runs of Network Agent service until the image capturing operation completes.
- Make sure that `klmover` will be run with the `-dupfix` key before (mandatory requirement) the first run of the Network Agent service on target devices, at the first launch of the operating system after the image deployment. The utility `klmover` is included in the installation package of Network Agent.

If the hard drive image has been copied incorrectly, you can resolve this problem (see section "Incorrect copying of a hard drive image" on page [881](#)).

You can apply an alternate scenario for Network Agent deployment on new devices through operating system images:

- The captured image contains no Network Agent installed.
- A stand-alone installation package of Network Agent located in the shared folder of Kaspersky Security Center has been added to the list of executable files that are run upon completion of the image deployment on target devices.

This deployment scenario adds flexibility: you can use a single operating system image together with various installation options for Network Agent and / or the security application, including device moving rules related to the

standalone package. This slightly complicates the deployment process: you have to provide access to the network folder with stand-alone installation packages from a device (see section "Installing images of operating systems" on page [714](#)).

See also:

Network Agent disk cloning mode[889](#)

Deployment using group policies of Microsoft Windows

It is recommended that you perform the initial deployment of Network Agents through Microsoft Windows group policies if the following conditions are met:

- This device is member of an Active Directory domain.
- The deployment scheme allows you to wait for the next routine restart of target devices before starting deployment of Network Agents on them (or you can force a Windows group policy to be applied to those devices).

This deployment scheme consists of the following:

- The application distribution package in Microsoft Installer format (MSI package) is located in a shared folder (a folder where the LocalSystem accounts of target devices have read permissions).
- In the Active Directory group policy, an installation object is created for the distribution package.
- The installation scope is set by specifying the organizational unit (OU) and / or the security group, which includes the target devices.
- The next time a target device logs in to the domain (before device users log in to the system), all installed applications are checked for the presence of the required application. If the application is not found, the distribution package is downloaded from the resource specified in the policy and is then installed.

An advantage of this deployment scheme is that assigned applications are installed on target devices while the operating system is loading, that is, even before the user logs in to the system. Even if a user with sufficient rights removes the application, it will be reinstalled at the next launch of the operating system. This deployment scheme's shortcoming is that changes made by the administrator to the group policy will not take effect until the devices are restarted (if no additional tools are involved).

You can use group policies to install both Network Agent and other applications if their respective installers are in Windows Installer format.

When this deployment scheme is selected, you must also assess the load on the file resource from which files will be copied to devices after applying the Windows group policy.

Handling Microsoft Windows policies through the remote installation task of Kaspersky Security Center

The simplest way to install applications through group policies of Microsoft Windows is to select the **Assign package installation in Active Directory group policies** check box in the properties of the remote installation task of Kaspersky Security Center. In this case, Administration Server automatically performs the following actions when you run the task:

- Creates required objects in the group policy of Microsoft Windows.
- Creates dedicated security groups, includes the target devices in those groups, and assigns installation of selected applications for them. The set of security groups will be updated at every task run, in accordance with the pool of devices at the moment of the run.

To make this feature operable, in the task properties, specify an account that has write permissions in Active Directory group policies.

If you intend to install both Network Agent and another application through the same task, selecting the **Assign package installation in Active Directory group policies** check box causes the application to create an installation object in the Active Directory policy for Network Agent only. The second application selected in the task will be installed through the tools of Network Agent as soon as the latter is installed on the device. If you want to install an application other than Network Agent through Windows group policies, you must create an installation task for this installation package only (without the Network Agent package). Not every application can be installed using Microsoft Windows group policies. To find out about this capability, you can refer to information about the possible methods for installing the application.

If required objects are created in the group policy by using Kaspersky Security Center tools, the shared folder of Kaspersky Security Center will be used as the source of the installation package. When planning the deployment, you must correlate the reading speed for this folder with the number of devices and the size of the distribution package to be installed. It may be useful to locate the shared folder of Kaspersky Security Center in a high-performance dedicated file repository (see section "Defining a shared folder" on page [224](#)).

In addition to its ease of use, automatic creation of Windows group policies through Kaspersky Security Center has this advantage: when planning Network Agent installation, you can easily specify the Kaspersky Security Center administration group into which devices will be automatically moved after installation completes. You can specify this group in the New Task Wizard or in the settings window of the remote installation task.

When handling Windows group policies through Kaspersky Security Center, you can specify devices for a group policy object by creating a security group. Kaspersky Security Center synchronizes the contents of the security group with the current set of devices in the task. When using other tools for handling group policies, you can associate objects of group policies with selected OUs of Active Directory directly.

Unassisted installation of applications through policies of Microsoft Windows

The administrator can create objects required for installation in a Windows group policy on his or her own behalf. In this case, he or she can provide links to packages stored in the shared folder of Kaspersky Security Center, or upload those packages to a dedicated file server and then provide links to them.

The following installation scenarios are possible:

- The administrator creates an installation package and sets up its properties in Administration Console. The group policy object provides a link to the msi file of this package stored in the shared folder of Kaspersky Security Center.
- The administrator creates an installation package and sets up its properties in Administration Console. Then the administrator copies the entire EXEC subfolder of this package from the shared folder of Kaspersky Security Center to a folder on a dedicated file resource of the organization. The group policy object provides a link to the msi file of this package stored in a subfolder on the dedicated file resource of the organization.
- The administrator downloads the application distribution package (including that of Network Agent) from the Internet and uploads it to the dedicated file resource of the organization. The group policy object provides a link to the msi file of this package stored in a subfolder on the dedicated file resource of the organization. The installation settings are defined by configuring the MSI properties or by configuring MST transform files (see section "Configuring installers" on page [163](#)).

See also:

| Installing an application through Active Directory group policies[335](#)

Forced deployment through the remote installation task of Kaspersky Security Center

If you need to start deploying Network Agents or other applications immediately, without waiting for the next time target devices log in to the domain, or if any target devices that are not members of the Active Directory domain are available, you can force installation of selected installation packages through the remote installation task of Kaspersky Security Center.

In this case, you can specify target devices either explicitly (with a list), or by selecting the Kaspersky Security Center administration group to which they belong, or by creating a selection of devices based upon a specific criterion. The installation start time is defined by the task schedule. If the **Run missed tasks** setting is enabled in the task properties, the task can be run either immediately after target devices are turned on, or when they are moved to the target administration group.

This type of installation consists in copying files to the administrative resource (admin\$) on each device and performing remote registration of supporting services on them. The following conditions must be met in this case:

- Devices must be available for connection either from the Administration Server side, or from the distribution point side.
- Name resolution for target devices must function properly in the network.
- The administrative shares (admin\$) must remain enabled on target devices.
- The Server system service must be running on target devices (by default, it is running).
- The following ports must be open on target devices to allow remote access through Windows tools: TCP 139, TCP 445, UDP 137, and UDP 138.
- Simple File Sharing mode must be disabled on target devices.
- On target devices, the access sharing and security model must be set as *Classic – local users authenticate as themselves*, it can be in no way *Guest only – local users authenticate as Guest*.
- Target devices must be members of the domain, or uniform accounts with administrator rights must be created on target devices in advance.

Devices in workgroups can be adjusted in accordance with the above requirements by using the riprep.exe utility, which is described on Kaspersky Technical Support website.

During installation on new devices that have not yet been allocated to any of the Kaspersky Security Center administration groups, you can open the remote installation task properties and specify the administration group to which devices will be moved after Network Agent installation.

When creating a group task, keep in mind that each group task affects all devices in all nested groups within a selected group. Therefore, you must avoid duplicating installation tasks in subgroups.

Automatic installation is a simplified way to create tasks for forced installation of applications. To do this, open the administration group properties, open the list of installation packages and select the ones that must be installed on devices in this group. As a result, the selected installation packages will be automatically installed on all devices in

this group and all of its subgroups. The time interval over which the packages will be installed depends on the network throughput and the total number of networked devices.

Forced installation can also be applied if devices cannot be directly accessed by the Administration Server: for example, devices are on isolated networks, or they are on a local network while the Administration Server item is in DMZ. To make forced installation possible, you must provide distribution points to each of the isolated networks.

Using distribution points as local installation centers may also be useful when performing installation on devices in subnets communicated with Administration Server via a low-capacity channel while a broader channel is available between devices in the same subnet. However, note that this installation method places a significant load on devices acting as distribution points. Therefore, it is recommended that you select powerful devices with high-performance storage units as distribution points. Moreover, the free disk space in the partition with the `%ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit` folder must exceed, by many times, the total size of the distribution packages of installed applications.

Running stand-alone packages created by Kaspersky Security Center

The above-described methods of initial deployment of Network Agent and other applications cannot always be implemented because it is not possible to meet all of the applicable conditions. In such cases, you can create a common executable file called a *stand-alone installation package* through Kaspersky Security Center, using installation packages with the relevant installation settings that have been prepared by the administrator. The stand-alone installation package is stored in the shared folder of Kaspersky Security Center.

You can use Kaspersky Security Center to send selected users an email message containing a link to this file in the shared folder, prompting them to run the file (either in interactive mode, or with the key "-s" for silent installation). You can attach the stand-alone installation package to an email message and then send it to the users of devices that have no access to the shared folder of Kaspersky Security Center. The administrator can also copy the stand-alone package to a removable drive, deliver it to a relevant device, and then run it later.

You can create a stand-alone package from a Network Agent package, a package of another application (for example, the security application), or both. If the stand-alone package has been created from Network Agent and another application, installation starts with Network Agent.

When creating a stand-alone package with Network Agent, you can specify the administration group to which new devices (those that have not been allocated to any of the administration groups) will be automatically moved when Network Agent installation completes on them.

Stand-alone packages can run in interactive mode (by default), displaying the result for installation of applications they contain, or they can run in silent mode (when run with the key "-s"). Silent mode can be used for installation from scripts, for example, from scripts configured to run after an operating system image is deployed. The result of installation in silent mode is determined by the return code of the process.

Options for manual installation of applications

Administrators or experienced users can install applications manually in interactive mode. They can use either original distribution packages or installation packages generated from them and stored in the shared folder of Kaspersky Security Center. By default, installers run in interactive mode and prompt users for all required values. However, when running the process `setup.exe` from the root of an installation package with the key "-s", the installer will be running in silent mode and with the settings that have been defined when configuring the installation package.

When running setup.exe from the root of an installation package stored in the shared folder of Kaspersky Security Center, the package will first be copied to a temporary local folder, and then the application installer will be run from the local folder.

Remote installation of applications on devices with Network Agent installed

If an operable Network Agent connected to the primary Administration Server (or to any of its secondary Servers) is installed on a device, you can upgrade Network Agent on this device, as well as install, upgrade, or remove any supported applications through Network Agent.

You can enable this option by selecting the **Using Network Agent** check box in the properties of the remote installation task (see section "About remote installation tasks in Kaspersky Security Center" on page [154](#)).

If this option is selected, installation packages with installation settings defined by the administrator will be transferred to target devices over communication channels between Network Agent and the Administration Server.

To optimize the load on the Administration Server and minimize traffic between the Administration Server and the devices, it is useful to assign distribution points on every remote network or in every broadcasting domain (see sections "About distribution points (on page [133](#))" and "Building a structure of administration groups and assigning distribution points (see section "Adjustment of distribution points and connection gateways" on page [587](#))"). In this case, installation packages and the installer settings are distributed from the Administration Server to target devices through distribution points.

Moreover, you can use distribution points for broadcasting (multicast) delivery of installation packages, which allows reducing network traffic significantly when deploying applications.

When transferring installation packages to target devices over communication channels between Network Agents and the Administration Server, all installation packages that have been prepared for transfer will also be cached in the %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\working\FTServer folder. When using multiple large installation packages of various types and involving a large number of distribution points, the size of this folder may increase dramatically.

Files cannot be deleted from the FTServer folder manually. When original installation packages are deleted, the corresponding data will be automatically deleted from the FTServer folder.

The data received by distribution points is saved in the folder %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1103\FTCITmp.

Files cannot be deleted from the \$FTCITmp folder manually. As tasks using data from this folder complete, the contents of this folder will be deleted automatically.

Because installation packages are distributed over communication channels between Administration Server and Network Agents from an intermediate repository in a format optimized for network transfers, no changes are allowed in installation packages stored in the original folder of each installation package. Those changes will not be automatically registered by Administration Server. If you need to modify the files of installation packages manually (although you are recommended to avoid this scenario), you must edit any of the settings of an installation package in Administration Console. Editing the settings of an installation package in Administration Console causes

Administration Server to update the package image in the cache that has been prepared for transfer to target devices.

Managing device restarts in the remote installation task

Devices often need a restart to complete the remote installation of applications (particularly on Windows).

If you use the remote installation task of Kaspersky Security Center, in the New Task Wizard or in the properties window of the task that has been created (**Operating system restart** section), you can select the action to perform when a restart is required:

- **Do not restart the device.** In this case, no automatic restart will be performed. To complete the installation, you must restart the device (for example, manually or through the device management task). Information about the required restart will be saved in the task results and in the device status. This option is suitable for installation tasks on servers and other devices where continuous operation is critical.
- **Restart the device.** In this case, the device is always restarted automatically if a restart is required for completion of the installation. This option is useful for installation tasks on devices that provide for regular pauses in their operation (shutdown or restart).
- **Prompt user for action.** In this case, the restart reminder is displayed on the screen of the client device, prompting the user to restart it manually. Some advanced settings can be defined for this option: text of the message for the user, message display frequency, and time interval after which the restart will be forced (without the user's confirmation). The **Prompt user for action** is the most suitable for workstations where users need a possibility of selecting the most convenient time for a restart.

Suitability of databases updating in an installation package of a security application

Before starting the protection deployment, you must keep in mind the possibility of updating anti-virus databases (including modules of automatic patches) shipped together with the distribution package of the security application. It is useful to update the databases in the installation package of the application before starting the deployment (for example, by using the corresponding command in the context menu of a selected installation package). This will reduce the number of restarts required for completion of protection deployment on target devices.

Using tools for remote installation of applications in Kaspersky Security Center for running relevant executable files on managed devices

Using the New Package Wizard, you can select any executable file and define the settings of the command line for it. For this you can add to the installation package either the selected file itself or the entire folder in which this file is stored. Then you must create the remote installation task and select the installation package that has been created.

While the task is running, the specified executable file with the defined settings of the command prompt will be run on target devices.

If you use installers in Microsoft Windows Installer (MSI) format, Kaspersky Security Center analyzes the installation results by means of standard tools.

If the Vulnerability and Patch Management license is available, Kaspersky Security Center (when creating an installation package for any supported application in the corporate environment) also uses rules for installation and analysis of installation results that are in its updatable database.

Otherwise, the default task for executable files waits for the completion of the running process, and of all its child processes. After completion of all of the running processes, the task will be completed successfully regardless of the return code of the initial process. To change such behavior of this task, before creating the task, you have to

manually modify the .kud file that was generated by Kaspersky Security Center in the folder of the newly created installation package.

For the task not to wait for the completion of the running process, set the value of the Wait setting to 0 in the [SetupProcessResult] section:

Example:

```
[SetupProcessResult]
Wait=0
```

For the task to wait only for the completion of the running process on Windows, not for the completion of all child processes, set the value of the WaitJob setting to 0 in the [SetupProcessResult], section, for example:

Example:

```
[SetupProcessResult]
WaitJob=0
```

For the task to complete successfully or return an error depending on the return code of the running process, list successful return codes in the [SetupProcessResult_SuccessCodes], section, for example:

Example:

```
[SetupProcessResult_SuccessCodes]
0=
3010=
```

In this case, any code other than those listed will result in an error returned.

To display a string with a comment on the successful completion of the task or an error in the task results, enter brief descriptions of errors corresponding to return codes of the process in the [SetupProcessResult_SuccessCodes] and [SetupProcessResult_ErrorCodes] sections, for example:

Example:

```
[SetupProcessResult_SuccessCodes]
0= Installation completed successfully
3010=A restart is required to complete the installation

[SetupProcessResult_ErrorCodes]
1602=Installation canceled by the user
1603=Fatal error during installation
```

To use Kaspersky Security Center tools for managing the device restart (if a restart is required to complete an operation), list the return codes of the process that indicate that a restart must be performed, in the [SetupProcessResult_NeedReboot] section:

Example:

[SetupProcessResult_NeedReboot]

3010=

Monitoring the deployment

To monitor the Kaspersky Security Center deployment and make sure that a security application and Network Agent are installed on managed devices, you have to check the traffic light in the **Deployment** section. This traffic light is located in the workspace of the Administration Server node in the main window of Administration Console (see section "Traffic lights in Administration Console" on page [503](#)). The traffic light reflects the current deployment status. The number of devices with Network Agent and security applications installed is displayed next to the traffic light. When any installation tasks are running, you can monitor their progress here. If any installation errors occur, the number of errors is displayed here. You can view the details of any error by clicking the link.

You can also use the deployment schema in the workspace of the **Managed devices** folder on the **Groups** tab. The chart reflects the deployment process, showing the number of devices without Network Agent, with Network Agent, or with Network Agent and a security application.

For more details on the progress of the deployment (or the operation of a specific installation task) open the results window of the relevant remote installation task: Right-click the task and select **Results** in the context menu. The window displays two lists: the upper one contains the task statuses on devices, while the lower one contains task events on the device that is currently selected in the upper list.

Information about deployment errors are added to the Kaspersky Event Log on Administration Server. Information about errors is also available through the corresponding event selection in the Administration Server node on the **Events** tab.

Configuring installers

This section provides information about the files of Kaspersky Security Center installers and the installation settings, as well as recommendations on how to install Administration Server and Network Agent in silent mode.

In this section

General information	163
Installation in silent mode (with a response file)	164
Installation of Network Agent in silent mode (without a response file)	164
Partial installation configuration through setup.exe	165
Administration Server installation parameters	166
Network Agent installation parameters	171

General information

Installers of Kaspersky Security Center 13 components (Administration Server, Network Agent, and Administration Console) are built on Windows Installer technology. An MSI package is the core of an installer. This format of packaging allows using all of the advantages provided by Windows Installer: scalability, availability of a patching

system, transformation system, centralized installation through third-party solutions, and transparent registration with the operating system.

See also:

Installation in silent mode (with a response file)	164
Installation of Network Agent in silent mode (without a response file)	164
Partial installation configuration through setup.exe	165
Administration Server installation parameters	166
Network Agent installation parameters	171

Installation in silent mode (with a response file)

The installers of Administration Server and Network Agent have the feature of working with the response file (ss_install.xml), where the parameters for installation in silent mode without user participation are integrated. The ss_install.xml file is located in the same folder as the msi package; it is used automatically during installation in silent mode. The silent installation mode is enabled with the command line key "/s".

An overview of an example run follows:

```
setup.exe /s
```

The ss_install.xml file is an instance of the internal format of parameters of the Kaspersky Security Center installer. Distribution packages contain the ss_install.xml file with the default parameters.

Please do not modify ss_install.xml manually. This file can be modified through the tools of Kaspersky Security Center when editing the parameters of installation packages in Administration Console.

See also:

General information	163
Installation of Network Agent in silent mode (without a response file)	164
Partial installation configuration through setup.exe	165
Administration Server installation parameters	166
Network Agent installation parameters	171

Installation of Network Agent in silent mode (without a response file)

You can install Network Agent with a single .msi package, specifying the values of MSI properties in the standard way. This scenario allows Network Agent to be installed by using group policies. To avoid conflicts between parameters defined through MSI properties and parameters defined in the response file, you can disable the response file by setting the property DONT_USE_ANSWER_FILE=1. An example of a run of the Network Agent installer with an .msi package is as follows.

Installation of Network Agent in non-interactive mode requires acceptance of the terms of the End User License Agreement (see section "About the End User License Agreement" on page [318](#)). Use the `EULA=1` parameter only if you have fully read, understand and accept the terms of the End User License Agreement.

Example:

```
msiexec /i "Kaspersky Network Agent.msi" /qn DONT_USE_ANSWER_FILE=1  
SERVERADDRESS=kscserver.mycompany.com EULA=1
```

You can also define the installation parameters for an .msi package by preparing the response file in advance (one with an .mst extension). This command appears as follows:

Example:

```
msiexec /i "Kaspersky Network Agent.msi" /qn  
TRANSFORMS=test.mst;test2.mst
```

You can specify several response files in a single command.

See also:

Installing Network Agent in non-interactive (silent) mode	179
Network Agent installation parameters.....	171
Ports used by Kaspersky Security Center	65
General information	163
Installation in silent mode (with a response file)	164
Partial installation configuration through setup.exe	165
Administration Server installation parameters	166

Partial installation configuration through setup.exe

When running installation of applications through setup.exe, you can add the values of any properties of MSI to the msi package.

This command appears as follows:

Example:

```
/v"PROPERTY_NAME1=PROPERTY_VALUE1 PROPERTYNAME2=PROPERTYVALUE2"
```

See also:

General information	163
Installation in silent mode (with a response file)	164
Installation of Network Agent in silent mode (without a response file)	164
Administration Server installation parameters	166
Network Agent installation parameters	171

Administration Server installation parameters

The table below describes the MSI properties that you can configure when installing Administration Server. All of the parameters are optional, except for EULA and PRIVACYPOLICY.

Table 31. Parameters of Administration Server installation in non-interactive mode

MSI property	Description	Available values
EULA	Acceptance of the licensing terms (required)	<ul style="list-style-type: none"> 1—I have fully read, understand and accept the terms of the End User License Agreement (see section "About the End User License Agreement" on page 318). Other value or no value—I do not accept the terms of the License Agreement (installation is not performed).
PRIVACYPOLICY	Acceptance of the terms of the Privacy Policy (required)	<ul style="list-style-type: none"> 1—I am aware and agree that my data will be handled and transmitted (including to third countries) as described in the Privacy Policy (see section "Viewing the Privacy Policy" on page 187). I confirm that I have fully read and understand the Privacy Policy. Other value or no value—I do not accept the terms of the Privacy Policy (installation is not performed).
INSTALLATIONMODETYPE	Type of Administration Server installation	<ul style="list-style-type: none"> Standard. Custom.
INSTALLDIR	Application installation folder	String value.
ADDLOCAL	List of components to install (separated by commas)	<p>CSAdminKitServer, NAgent, CSAdminKitConsole, NSAC, MobileSupport, KSNProxy, SNMPAgent, GdiPlusRedist, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86.</p> <p>Minimum list of components sufficient for proper Administration Server installation:</p> <pre>ADDLOCAL=CSAdminKitServer, CSAdminKitConsole, KSNProxy, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86</pre>
NETRANGETYPE	Network size	<ul style="list-style-type: none"> NRT_1_100—From 1 to 100 devices. NRT_100_1000—From 101 to 1000 devices. NRT_GREATER_1000—More than 1000 devices.
SRV_ACCOUNT_TYPE	Way of specifying the user for the operation of the Administration Server service	<ul style="list-style-type: none"> SrvAccountDefault—The user account will be created automatically. SrvAccountUser—The user account is defined manually.
SERVERACCOUNTNAME	User name for the service	String value.
SERVERACCOUNTPWD	User password for the service	String value.

MSI property	Description	Available values
DBTYPE	Database type	<ul style="list-style-type: none"> MySQL—MySQL or MariaDB database server will be used. MSSQL—Microsoft SQL Server (SQL Server Express) database server will be used.
MYSQLSERVERNAME	Full name of MySQL or MariaDB database server	String value.
MYSQLSERVERPORT	Number of port for connection to MySQL or MariaDB database server	Numerical value.
MYSQLDBNAME	Name of MySQL or MariaDB database server	String value.
MYSQLACCOUNTNAME	User name for connection to MySQL or MariaDB database server	String value.
MYSQLACCOUNTPWD	User password for connection to MySQL or MariaDB database server	String value.
MSSQLCONNECTIONTYPE	Type of use of MSSQL database	<ul style="list-style-type: none"> InstallMSSEE—Install from a package. ChooseExisting—Use the installed server.
MSSQLSERVERNAME	Full name of SQL Server instance	String value.
MSSQLDBNAME	Name of SQL Server database	String value.
MSSQLAUTHTYPE	Method of authentication for connection to SQL Server	<ul style="list-style-type: none"> Windows. SQLServer.
MSSQLACCOUNTNAME	User name for connection to SQL Server in SQLServer mode	String value.
MSSQLACCOUNTPWD	User password for connection to SQL Server in SQLServer mode	String value.

MSI property	Description	Available values
CREATE_SHARE_TYPE	Method of specifying the shared folder	<ul style="list-style-type: none"> • Create—Create a new shared folder; in this case, the following properties must be defined: <ul style="list-style-type: none"> • SHARELOCALPATH—Path to a local folder. • SHAREFOLDERNAME—Network name of a folder. • Null—EXISTSHAREFOLDERNAME property must be specified.
EXISTSHAREFOLDERNAME	Full path to an existing shared folder	String value.
SERVERPORT	Port number to connect to Administration Server	Numerical value.
SERVERSSLPORT	Number of port for establishing SSL connection to Administration Server	Numerical value.
SERVERADDRESS	Administration Server address	String value.
SERVERCERT2048BITS	Size of the key for the Administration Server certificate (bits)	<ul style="list-style-type: none"> • 1—The size of the key for the Administration Server certificate is 2 048 bit. • 0—The size of the key for the Administration Server certificate is 1 024 bit. • If no value is specified, the size of the key for the Administration Server certificate is 1 024 bit.
MOBILESERVERADDRESS	Address of the Administration Server for connection of mobile devices; ignored if the MobileSupport component has not been selected	String value.

See also:

General information	163
Installation in silent mode (with a response file)	164
Installation of Network Agent in silent mode (without a response file)	164
Network Agent installation parameters	171
Installing Network Agent in non-interactive (silent) mode	179
Partial installation configuration through setup.exe	165

Network Agent installation parameters

The table below describes the MSI properties that you can configure when installing Network Agent. All of the parameters are optional, except for EULA and SERVERADDRESS.

Table 32. *Parameters of Network Agent installation in non-interactive mode*

MSI property	Description	Available values
EULA	Acceptance of the terms of the License Agreement	<ul style="list-style-type: none"> • 1—I have fully read, understand and accept the terms of the End User License Agreement (see section "About the End User License Agreement" on page 318). • 0—I do not accept the terms of the License Agreement (installation is not performed). • No value—I do not accept the terms of the License Agreement (installation is not performed).
DONT_USE_ANSWER_FILE	Read installation settings from response file	<ul style="list-style-type: none"> • 1—Do not use. • Other value or no value—Read.
INSTALLDIR	Path to the Network Agent installation folder	String value.
SERVERADDRESS	Administration Server address (required)	String value.
SERVERPORT	Number of port for connection to Administration Server	Numerical value.
SERVERSSLPORT	Number of the port for encrypted connection to Administration Server by using SSL protocol	Numerical value.
USESSL	Whether to use SSL connection	<ul style="list-style-type: none"> • 1—Use. • Other value or no value—Do not use.
OPENUDPPORT	Whether to open a UDP port	<ul style="list-style-type: none"> • 1—Open. • Other value or no value—Do not open.
UDPPORT	UDP port number	Numerical value.
USEPROXY	Whether to use a proxy server	<ul style="list-style-type: none"> • 1—Use. • Other value or no value—Do not use.
PROXYADDRESS	Proxy address	String value.
PROXYPORT	Number of port for connection to proxy server	Numerical value.
PROXYLOGIN	Account for connection to proxy server	String value.

MSI property	Description	Available values
PROXYPASSWORD	Password of account for connection to proxy server (Do not specify any details of privileged accounts in the parameters of installation packages.)	String value.
GATEWAYMODE	Connection gateway use mode	<ul style="list-style-type: none"> • 0—Do not use connection gateway. • 1—Use this Network Agent as connection gateway. • 2—Connect to the Administration Server using connection gateway.
GATEWAYADDRESS	Connection gateway address	String value.
CERTSELECTION	Method of receiving a certificate	<ul style="list-style-type: none"> • GetOnFirstConnection—Receive a certificate from the Administration Server. • GetExistent—Select an existing certificate. If this option is selected, the CERTFILE property must be specified.
CERTFILE	Path to the certificate file	String value.
VMVDI	Enable dynamic mode for Virtual Desktop Infrastructure (VDI)	<ul style="list-style-type: none"> • 1—Enable. • 0—Do not enable. • No value—Do not enable.
LAUNCHPROGRAM	Whether to start the Network Agent service after installation	<ul style="list-style-type: none"> • 1—Start. • Other value or no value—Do not start.
NAGENTTAGS	Tag for Network Agent (has priority over the tag given in the answers file)	<ul style="list-style-type: none"> • String value.

See also:

General information	163
Installation in silent mode (with a response file)	164
Installing Network Agent in non-interactive (silent) mode	179
Installation of Network Agent in silent mode (without a response file)	164
Ports used by Kaspersky Security Center	65
Partial installation configuration through setup.exe	165
Administration Server installation parameters	166

Virtual infrastructure

Kaspersky Security Center supports the use of virtual machines. You can install Network Agent and the security application on each virtual machine, and you can protect virtual machines at the hypervisor level. In the first case, you can use either a standard security application or Kaspersky Security for Virtualization Light Agent to protect your virtual machines. In the second case, you can use Kaspersky Security for Virtualization Agentless.

Kaspersky Security Center supports rollbacks of virtual machines to their previous state (see section "Support of file system rollback for devices with Network Agent" on page [176](#)).

In this section

Tips on reducing the load on virtual machines	175
Support of dynamic virtual machines.....	175
Support of virtual machines copying.....	176

Tips on reducing the load on virtual machines

When installing Network Agent on a virtual machine, you are advised to consider disabling some Kaspersky Security Center features that seem to be of little use for virtual machines.

When installing Network Agent on a virtual machine or on a template intended for generation of virtual machines, it is useful to perform the following actions:

- If you are running a remote installation, in the properties window of the Network Agent installation package (section **Advanced**), select the **Optimize settings for VDI** check box.
- If you are running an interactive installation through a Wizard, in the Wizard window, select the **Optimize the Network Agent settings for the virtual infrastructure** check box.

Selecting those check boxes will alter the settings of Network Agent so that the following features remain disabled by default (before applying a policy):

- Retrieving information about software installed
- Retrieving information about hardware
- Retrieving information about vulnerabilities detected
- Retrieving information about updates required

Usually, those features are not necessary on virtual machines because they use uniform software and virtual hardware.

Disabling the features is invertible. If any of the disabled features is required, you can enable it through the policy of Network Agent, or through the local settings of Network Agent. The local settings of Network Agent are available through the context menu of the relevant device in Administration Console.

Support of dynamic virtual machines

Kaspersky Security Center supports dynamic virtual machines (only Windows). If a virtual infrastructure has been deployed on the organization's network, dynamic (temporary) virtual machines can be used in certain cases. The dynamic VMs are created under unique names based on a template that has been prepared by the administrator. The user works on a VM for a while and then, after being turned off, this virtual machine will be removed from the

virtual infrastructure. If Kaspersky Security Center has been deployed on the organization's network, a virtual machine with installed Network Agent will be added to the Administration Server database. After you turn off a virtual machine, the corresponding entry must also be removed from the database of Administration Server.

To make functional the feature of automatic removal of entries on virtual machines, when installing Network Agent on a template for dynamic virtual machines, select the **Enable dynamic mode for VDI** check box:

- For remote installation—In the properties window of the installation package of Network Agent (**Advanced** section) (see section "Network Agent installation package settings" on page [183](#))
- For interactive installation—In the Network Agent Installation Wizard

Avoid selecting the **Enable dynamic mode for VDI** check box when installing Network Agent on physical devices.

If you want events from dynamic virtual machines to be stored on the Administration Server for a while after you remove those virtual machines, then, in the Administration Server properties window, in the **Events repository** section, select the **Store events after devices are deleted** check box and specify the maximum storage term for events (in days).

Support of virtual machines copying

Copying a virtual machine with installed Network Agent or creating one from a template with installed Network Agent is identical to the deployment of Network Agents by capturing and copying a hard drive image. So, in general case, when copying virtual machines, you need to perform the same actions as when deploying Network Agent by copying a disk image (see section "Deployment by capturing and copying the hard drive image of a device" on page [154](#)).

However, the two cases described below showcase Network Agent, which detects the copying automatically. Owing to the above reasons, you do not have to perform the sophisticated operations described under "Deployment by capturing and copying the hard drive of a device":

- The **Enable dynamic mode for VDI** check box was selected when Network Agent was installed—After each restart of the operating system, this virtual machine will be recognized as a new device, regardless of whether it has been copied or not.
- One of the following hypervisors is in use: VMware™, HyperV®, or Xen®: Network Agent detects the copying of the virtual machine by the changed IDs of the virtual hardware.

Analysis of changes in virtual hardware is not absolutely reliable. Before applying this method widely, you must test it on a small pool of virtual machines for the version of the hypervisor currently used in your organization.

Support of file system rollback for devices with Network Agent

Kaspersky Security Center is a distributed application. Rolling back the file system to a previous state on a device with Network Agent installed will lead to data desynchronization and improper functioning of Kaspersky Security Center.

The file system (or a part of it) can be rolled back in the following cases:

- When copying an image of the hard drive.
- When restoring a state of the virtual machine by means of the virtual infrastructure.
- When restoring data from a backup copy or a recovery point.

Scenarios under which third-party software on devices with Network Agent installed affects the %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\ folder are only critical scenarios for Kaspersky Security Center. Therefore, you must always exclude this folder from the recovery procedure, if possible.

Because the workplace rules of some organizations provide for rollbacks of the file system on devices, support for the file system rollback on devices with Network Agent installed has been added to Kaspersky Security Center, starting with version 10 Maintenance Release 1 (Administration Server and Network Agents must be of version 10 Maintenance Release 1 or later). When detected, those devices are automatically reconnected to the Administration Server with full data cleansing and full synchronization.

By default, support of file system rollback detection is enabled in Kaspersky Security Center 13.

As much as possible, avoid rolling back the %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\ folder on devices with Network Agent installed, because full resynchronization of data requires a large amount of resources.

A rollback of the system state is absolutely not allowed on a device with Administration Server installed. Nor is a rollback of the database used by Administration Server.

You can restore a state of Administration Server from a backup copy only with the standard klbackup utility (see section "Backup and restoration of Administration Server settings" on page [615](#)).

Local installation of applications

This section provides an installation procedure for applications that can be installed on local devices only.

To perform local installation of applications on a specific client device, you must have administrator rights on this device.

► *To install applications locally on a specific client device:*

1. Install Network Agent on the client device and configure the connection between the client device and Administration Server.
2. Install the requisite applications on the device as described in the guides of these applications.
3. Install a management plug-in for each of the installed applications on the administrator's workstation.

Kaspersky Security Center also supports the option of local installation of applications using a stand-alone installation package. Kaspersky Security Center does not support installation of all Kaspersky applications (see section "List of supported Kaspersky applications" on page [41](#)).

In this chapter

Local installation of Network Agent	178
Installing Network Agent in non-interactive (silent) mode	179
Installing Network Agent for Linux in silent mode (with an answer file)	180
Local installation of the application management plug-in.....	181
Installing applications in non-interactive mode.....	181
Installing applications by using stand-alone packages.....	182
Network Agent installation package settings	183
Viewing the Privacy Policy.....	187

Local installation of Network Agent

► *To install Network Agent on a device locally:*

1. On the device, run the setup.exe file from the distribution package downloaded from the Internet.
A window opens prompting you to select Kaspersky applications to install.
2. In the application selection window, click the **Install only Kaspersky Security Center 13 Network Agent** link to start the Network Agent Setup Wizard. Follow the instructions of the Wizard.
While the Installation Wizard is running, you can specify the advanced settings of Network Agent (see below).
3. If you want to use your device as the connection gateway for a specific administration group, in the **Connection gateway** window of the Setup Wizard select **Use Network Agent as a connection gateway in DMZconnection gateway in DMZ**.

4. To configure Network Agent during installation on a virtual machine:

- a. If you plan to create dynamic virtual machines from the virtual machine image, enable dynamic mode of Network Agent for Virtual Desktop Infrastructure (VDI). To do this, in the **Advanced Settings** window of the Setup Wizard, select the **Enable dynamic mode for VDI** check box.

Skip this step if you do not plan to create dynamic virtual machines from the virtual machine image.

Using dynamic mode for VDI is available only for devices running Windows.

- b. Optimize the Network Agent operation for VDI. To do this, in the **Advanced Settings** window of the Setup Wizard, select the **Optimize the Kaspersky Security Center Network Agent settings for the virtual infrastructure** check box.

Scanning of executable files for vulnerabilities at the device startup will be disabled. Also, this disables the sending of information about the following objects to Administration Server:

- Hardware registry
- Applications installed on the device
- Microsoft Windows updates that must be installed on the local client device
- Software vulnerabilities detected on the local client device

Furthermore, you will be able to enable the sending of this information in the Network Agent properties or in the Network Agent policy settings.

When the Setup Wizard finishes, Network Agent will be installed on the device.

You can view the properties of the Kaspersky Security Center Network Agent service, and start, stop, and monitor Network Agent activity by means of standard Microsoft Windows tools: Computer Management\Services.

See also:

Support of dynamic virtual machines.....	175
Viewing the Privacy Policy.....	187

Installing Network Agent in non-interactive (silent) mode

Network Agent can be installed in non-interactive mode, that is, without the interactive input of installation parameters. Non-interactive installation uses a Windows Installer package (.msi) for Network Agent. The .msi file is located in the Kaspersky Security Center distribution package, in the Packages\NetAgent\exec folder.

► *To install Network Agent on a local device in non-interactive mode:*

1. Read the End User License Agreement (see section "About the End User License Agreement" on page [318](#)). Use the command below only if you understand and accept the terms of the End User License Agreement.
2. Run the command

```
msiexec /i "Kaspersky Network Agent.msi" /qn <setup_parameters>
```

where `setup_parameters` is a list of parameters and their respective values, separated by a space (PROP1=PROP1VAL PROP2=PROP2VAL).

In the list of parameters, you must include `EULA=1`. Otherwise Network Agent will not be installed.

If you are using the standard connection settings for Kaspersky Security Center 11 and later, and Network Agent on remote devices, run the command:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx  
c:\windows\temp\nag_inst.log SERVERADDRESS=kscserver.mycompany.com EULA=1
```

`/l*vx` is the key for writing logs. The log is created during the installation of Network Agent and saved at `C:\windows\temp\nag_inst.log`.

In addition to `nag_inst.log`, the application creates the `$klssinstlib.log` file, which contains the installation log. This file is stored in the `%windir%\temp` or `%temp%` folder. For troubleshooting purposes, you or a Kaspersky Technical Support specialist may need both log files—`nag_inst.log` and `$klssinstlib.log`.

If you need to additionally specify the port for connection to the Administration Server run the command:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx  
c:\windows\temp\nag_inst.log SERVERADDRESS=kscserver.mycompany.com EULA=1  
SERVERPORT=14000
```

The parameter `SERVERPORT` corresponds to the number of port for connection to Administration Server.

The names and possible values for parameters that can be used when installing Network Agent in non-interactive mode are listed in the Network Agent installation parameters (on page [171](#)) section.

See also:

Network Agent installation parameters.....	171
Administration Server installation parameters.....	166
Installation of Network Agent in silent mode (without a response file)	164
Viewing the Privacy Policy.....	187

Installing Network Agent for Linux in silent mode (with an answer file)

You can install Network Agent on Linux devices by using an answer file—a text file that contains a custom set of installation parameters: variables and their respective values. Using this answer file allows you to run an installation in the silent (non-interactive) mode, that is, without user participation.

► *To perform installation of Network Agent for Linux in silent mode:*

1. Prepare the relevant Linux device for remote installation. Download and create the remote installation package, by using a `.deb` or `.rpm` package of Network Agent, by means of any suitable package management system.
2. Read the End User License Agreement (see section "About the End User License Agreement" on page [318](#)). Follow the steps below only if you understand and accept the terms of the End User License Agreement.

3. Set the value of the KLAUTOANSWERS environment variable by entering the full name of the answer file (including the path), for example, as follows:

```
export KLAUTOANSWERS=/tmp/nagent_install/answers.txt
```

4. Create the answer file (in TXT format) in the directory that you have specified in the environment variable. Add to the answer file a list of variables in the VARIABLE_NAME=variable_value format, each one on a separate line.

For correct usage of the answer file, you must include in it a minimum set of the three required variables:

- KLNAGENT_SERVER
- KLNAGENT_AUTOINSTALL
- EULA_ACCEPTED

You can also add any optional variables to use more specific parameters of your remote installation. The following table lists all of the variables that can be included in the answer file:

Variables of the answer file used as parameters of Network Agent for Linux installation in silent mode

5. Run the postinstall.pl script by executing the following command:

- For a 32-bit operating system:

```
$ sudo /opt/kaspersky/klnagent/lib/bin/setup/postinstall.pl
```
- For a 64-bit operating system:

```
$ sudo /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl
```

Installation of Network Agent for Linux starts in silent mode; the user is not prompted for any actions during the process.

Local installation of the application management plug-in

- *To install the application management plug-in:*

On a device with Administration Console installed, run the klcfginst.exe executable file, which is included in the application distribution package.

The klcfginst.exe file is included in all applications that can be managed through Kaspersky Security Center. Installation is facilitated by a wizard and requires no manual configuration of settings.

Installing applications in non-interactive mode

- *To install an application in non-interactive mode:*

1. Open the main window of Kaspersky Security Center.
2. In the **Remote installation** folder of the console tree, in the **Installation packages** subfolder select the installation package of the relevant application or create a new one for that application.

The installation package will be stored on the Administration Server in the Packages service folder that is in the shared folder. A separate subfolder corresponds to each installation package.

3. Open the folder storing the required installation package in one of the following ways:

- By copying the folder corresponding to the relevant installation package from the Administration Server to the client device. Then open the copied folder on the client device.
- By opening from the client device the shared folder that corresponds to the requisite installation package on the Administration Server.

If the shared folder is located on a device that has Microsoft Windows Vista installed, you must set the **Disabled** value for the **User account control: Run all administrators in Admin Approval Mode** setting (**Start** → **Control Panel** → **Administration** → **Local security policy** → **Security settings**).

4. Depending on the selected application, do the following:
 - For Kaspersky Anti-Virus for Windows Workstations, Kaspersky Anti-Virus for Windows Servers, and Kaspersky Security Center, navigate to the `exec` subfolder and run the executable file (the file with the `.exe` extension) with the `/s` key.
 - For other Kaspersky applications, run the executable file (a file with the `.exe` extension) with the `/s` key from the open folder.

Running the executable file with the `EULA=1` and `PRIVACYPOLICY=1` keys means that you have fully read, understand and accept the terms of the End User License Agreement (see section "About the End User License Agreement" on page 318) and the Privacy Policy (see section "Viewing the Privacy Policy" on page 187), respectively. You are also aware that your data will be handled and transmitted (including to third countries) as described in the Privacy Policy. The text of the License Agreement and the Privacy Policy is included in the Kaspersky Security Center distribution kit. Accepting the terms of the License Agreement and the Privacy Policy is necessary for installing the application or upgrading a previous version of the application.

Installing applications by using stand-alone packages

Kaspersky Security Center lets you create stand-alone installation packages for applications. A stand-alone installation package is an executable file that can be located on the Web Server, sent by email, or transferred to a client device by another method. The received file can be run locally on the client device to install an application without involving Kaspersky Security Center.

► *To install an application using a stand-alone installation package:*

1. Connect to the necessary Administration Server.
2. In the **Remote installation** folder of the console tree, select the **Installation packages** subfolder.
3. In the workspace, select the installation package of the required application.
4. Start the process of creating a stand-alone installation package in one of the following ways:
 - By selecting **Create stand-alone installation package** in the context menu of the installation package.
 - By clicking the **Create stand-alone installation package** link in the workspace of the installation package.

The Stand-alone Installation Package Creation Wizard starts. Follow the instructions of the Wizard.

At the final step of the Wizard, select a method for transferring the stand-alone installation package to the client device.

5. Transfer the stand-alone installation package to the client device.

6. Run the stand-alone installation package on the client device.

The application is now installed on the client device with the settings specified in the stand-alone package.

When you create a stand-alone installation package, it is automatically published on Web Server. The link for downloading the stand-alone package is displayed in the list of created stand-alone installation packages. If necessary, you can cancel publication of the selected stand-alone package and republish it on the Web Server. By default, port 8060 is used for downloading stand-alone installation packages.

Network Agent installation package settings

► *To configure a Network Agent installation package:*

1. In the **Remote installation** folder of the console tree, select the **Installation packages** subfolder.

The **Remote installation** folder is a subfolder of the **Advanced** folder by default.

2. In the context menu of the Network Agent installation package, select **Properties**.

The Network Agent installation package properties window opens.

General

The **General** section displays general information about the installation package:

- Installation package name
- Name and version of the application for which the installation package has been created
- Installation package size
- Installation package creation date
- Path to the installation package folder

Settings

This section presents the settings required to ensure proper functioning of Network Agent immediately after it is installed. The settings in this section are available only on devices running Windows.

In the **Destination folder** group of settings, you can select the client device folder in which Network Agent will be installed.

- **Install in default folder**

If this option is selected, Network Agent will be installed in the <Drive>:\Program Files\Kaspersky Lab\NetworkAgent folder. If this folder does not exist, it will be created automatically.

By default, this option is selected.

- **Install in specified folder**

If this option is selected, Network Agent will be installed in the folder specified in the entry field.

In the following group of settings, you can set a password for the Network Agent remote uninstallation task:

- **Use uninstallation password**

If this check box is selected, by clicking the **Modify** button you can enter the uninstall password (only available for Network Agent on devices running Windows operating systems).

By default, this check box is cleared.

- **Status**

Status of the password: **Password set** or **Password not set**.

By default, this password is not installed.

- **Protect Network Agent service against unauthorized removal or termination, and to prevent changes to the settings**

After Network Agent is installed on a managed device, the component cannot be removed or reconfigured without required privileges. The Network Agent service cannot be stopped.

By default, this option is disabled.

- **Automatically install applicable updates and patches for components that have the Undefined status**

If this check box is selected, all downloaded updates and patches for Administration Server, Network Agent, Administration Console, Exchange Mobile Device Server, and iOS MDM Server will be installed automatically (automatic updating and patching is only available starting from Kaspersky Security Center 10 Service Pack 2 version).

If this check box is cleared, all downloaded updates and patches will only be installed after you change their status to *Approved*. Updates and patches with *Undefined* status will not be installed.

By default, this check box is selected.

Connection

In this section you can configure connection of Network Agent to the Administration Server:

- **Administration Server**

Address of the device with Administration Server installed.

- **Port**

Port number that is used for connection.

- **SSL port**

Port number that is used for connection over the SSL protocol.

- **Use Server certificate**

If this check box is selected, authentication of Network Agent access to the Administration Server will use the certificate file that you can specify by clicking the **Browse** button.

If this check box is cleared, the certificate file will be received from the Administration Server at the first connection of Network Agent to the address specified in the **Server address** field.

We recommend that you not clear the check box, because automatic receipt of an Administration Server certificate by Network Agent upon connection to the Administration Server is considered insecure.

By default, this check box is selected.

- **Use SSL**

If this check box is selected, connection to the Administration Server is established

through a secure port via SSL.

By default, this check box is cleared.

- **Use UDP port**

If this check box is selected, the Network Agent is connected to Administration Server through a UDP port.

By default, this check box is selected.

- **UDP port number**

In this field you can specify the port to connect Network Agent to Administration Server using UDP protocol.

The default UDP port is 15000.

- **Open Network Agent ports in Microsoft Windows Firewall**

If this check box is selected, after you install Network Agent on the client device, a UDP port is added to the list of Microsoft Windows Firewall exclusions. This UDP port is required for Network Agent to run properly.

By default, this check box is selected.

Advanced

In the **Advanced** section, you can configure how the connection gateway is used:

- **Use Network Agent as connection gateway in DMZ**

If this check box is selected, Network Agent is used as a connection gateway in the DMZ.

By default, this check box is cleared.

- **Connect to Administration Server by using connection gateway**

If this check box is selected, Network Agent will use connection gateway to connect to Administration Server.

By default, this check box is cleared.

- **Connection gateway address**

In this field, you can enter the address of the device that will act as connection gateway.

This field is not available if the **Connect to Administration Server using connection gateway** check box is cleared.

- **Enable dynamic mode for VDI**

If this check box is selected, dynamic mode for Virtual Desktop Infrastructure (VDI) will be enabled for Network Agent installed on a virtual machine.

By default, this check box is cleared.

- **Optimize settings for VDI**

If this check box is selected, the following features are disabled in the Network Agent settings:

- Retrieving information about software installed
- Retrieving information about hardware
- Retrieving information about vulnerabilities detected
- Retrieving information about updates required

By default, this check box is cleared.

Additional components

In this section you can select additional components for concurrent installation with Network Agent.

Tags

The **Tags** section displays a list of keywords (tags) that can be added to client devices after Network Agent installation. You can add and remove tags from the list, as well as rename them.

If the check box is selected next to a tag, this tag is automatically added to managed devices during Network Agent installation.

If the check box is cleared next to a tag, the tag will not automatically be added to managed devices during Network Agent installation. You can manually add this tag to devices.

When removing a tag from the list, it is automatically removed from all devices to which it was added.

Revision history

In this section, you can view the history of the installation package revisions (see section "Managing object revisions" on page [719](#)). You can compare revisions, view revisions, save revisions to a file, and add and edit revision descriptions.

Network Agent installation package settings available to a specific operating system are given in the table below.

Table 33. Network Agent installation package settings

Property section	Windows	Mac	Linux
General	+	+	+
Settings	+	No	No
Connection	+	+ * except the check boxes: Open Network Agent ports in Microsoft Windows Firewall Use only automatic detection of proxy server	+ * except the check boxes: Open Network Agent ports in Microsoft Windows Firewall Use only automatic detection of proxy server
Advanced	+	+	+
Additional components	+	+	+
Tags	+	+ * except the automatic tagging rules	+ * except the automatic tagging rules
Revision history	+	+	+

Viewing the Privacy Policy

The Privacy Policy is available online at <https://www.kaspersky.com/Products-and-Services-Privacy-Policy>; it is also available offline. You can read the Privacy Policy, for example, before installing Network Agent.

► *To read the Privacy Policy offline:*

1. Start the installer of Kaspersky Security Center.
2. In the installer window, proceed to the **Extract installation packages** link.
3. In the list that opens, select Kaspersky Security Center 13 Network Agent, and then click **Next**.

The `privacy_policy.txt` file appears on your device, in the folder that you specified, in the `NetAgent_<current version>` subfolder.

Deploying mobile device management systems

This section describes the deployment of mobile device management systems using Exchange ActiveSync, iOS MDM, and Kaspersky Endpoint Security protocols.

In this chapter

Deploying a system for management via Exchange ActiveSync protocol	188
Deploying a system for management using iOS MDM protocol.....	192
Adding a KES device to the list of managed devices	207
Connecting KES devices to the Administration Server	208
Integration with Public Key Infrastructure	212
Kaspersky Security Center Web Server	212

Deploying a system for management via Exchange ActiveSync protocol

Kaspersky Security Center allows you to manage mobile devices that are connected to the Administration Server using the Exchange ActiveSync protocol. Exchange ActiveSync (EAS) mobile devices are those connected to an Exchange Mobile Device Server and managed by Administration Server.

The following operating systems support Exchange ActiveSync protocol:

- Windows Phone® 8
- Windows Phone 8.1
- Windows 10 Mobile
- Android
- iOS

The set of management settings for an Exchange ActiveSync device is dependent on the operating system under which the mobile device is running. For details on the support features of Exchange ActiveSync protocol for a specific operating system, please refer to the documentation enclosed with the operating system.

Deployment of a mobile device management system using Exchange ActiveSync protocol includes the following steps:

1. The administrator installs Exchange Mobile Device Server (see section "Installing Mobile Device Server for Exchange ActiveSync" on page [189](#)) on the selected client device.
2. The administrator creates a management profile(s) in Administration Console for managing EAS devices and adds the profile(s) to the mailboxes of Exchange ActiveSync users.

Management profile of Exchange ActiveSync mobile devices is an ActiveSync policy used on a Microsoft Exchange server for managing Exchange ActiveSync mobile devices. Only one EAS device management profile (see section "Managing Exchange ActiveSync mobile devices" on page 749) can only be assigned to a Microsoft Exchange mailbox.

Users of mobile EAS devices connect to their Exchange mailboxes. Any management profile imposes some restrictions on mobile devices (see section "Connecting mobile devices to an Exchange Mobile Device Server" on page 190).

In this section

Installing Mobile Device Server for Exchange ActiveSync	189
Connecting mobile devices to an Exchange Mobile Device Server	190
Configuring the Internet Information Services web server	190
Local installation of an Exchange Mobile Device Server.....	191
Remote installation of Exchange Mobile Device Server.....	191

Installing Mobile Device Server for Exchange ActiveSync

An Exchange Mobile Device Server is installed on a client device with a Microsoft Exchange server installed. We recommend that you install the Exchange Mobile Device Server on a Microsoft Exchange server with the Client Access role assigned. If several Microsoft Exchange servers with the Client Access role in the same domain are combined into a Client Access Array, it is recommended to install the Exchange Mobile Device Server on each Microsoft Exchange server in that array in cluster mode.

► To install an Exchange Mobile Device Server on a local device:

1. Run the setup.exe executable file.

A window opens prompting you to select Kaspersky applications to install.

2. In the applications selection window, click the **Install Exchange Mobile Device Server** link to run the Setup Wizard of Exchange Mobile Device Server.
3. In the **Installation settings** window, select the type of Exchange Mobile Device Server installation:
 - To install Exchange Mobile Device Server with the default settings, select **Standard installation** and click the **Next** button.
 - To define the settings for installation of the Exchange Mobile Device Server manually, select **Custom installation** and click **Next**. Then do the following:
 - a. Select destination folder in **Destination Folder** window. The default folder is <Disk>:\Program Files\Kaspersky Lab\Mobile Device Management for Exchange. If such a folder does not exist, it is created automatically during the installation. You can change the destination folder by using the **Browse** button.
 - b. Choose the type of Exchange Mobile Device Server installation in the **Installation mode** window: normal mode or cluster mode.
 - c. In **Select Account** window, choose an account that will be used to manage mobile devices:
 - **Create account and role group automatically**. Account will be created automatically.

- **Specify an account.** The account should be selected manually. Click the **Browse** button to select the user whose account will be used and specify the password. The selected user must belong to a group that has rights to manage mobile devices using ActiveSync.
- d. In the **IIS settings** window, allow or prohibit automatic configuration of the Internet Information Services (IIS) web server properties.

If you have prohibited automatic configuration of the Internet Information Services (IIS) properties, enable the "Windows authentication" mechanism manually in the IIS settings for Microsoft PowerShell Virtual Directory. If "Windows authentication" mechanism is disabled, Exchange Mobile Device Server will not operate correctly. Please refer to IIS documentation for more information about configuring IIS.

- e. Click **Next**.
4. In the window that opens, verify the Exchange Mobile Device Server installation properties, and then click **Install**.

When the Wizard finishes, the Exchange Mobile Device Server is installed on the local device. The Exchange Mobile Device Server will be displayed in the **Mobile Device Management** folder in the console tree.

Connecting mobile devices to an Exchange Mobile Device Server

Before connecting any mobile devices, you must configure Microsoft Exchange Server in order to allow the devices to be connected using ActiveSync protocol.

To connect a mobile device to an Exchange Mobile Device Server, the user connects to his or her Microsoft Exchange mailbox from the mobile device through ActiveSync. When connecting, the user must specify the connection settings in the ActiveSync client, such as email address and email password.

The user's mobile device, connected to the Microsoft Exchange server, is displayed in the **Mobile devices** subfolder contained in the **Mobile Device Management** folder in the console tree.

After the Exchange ActiveSync mobile device is connected to an Exchange Mobile Device Server, the administrator can manage the connected Exchange ActiveSync mobile device (see section "Managing Exchange ActiveSync mobile devices" on page [749](#)).

Configuring the Internet Information Services web server

When using Microsoft Exchange Server (versions 2010 and 2013), you have to activate the Windows authentication mechanism for a Windows PowerShell™ virtual directory in the settings of the Internet Information Services (IIS) web server. This authentication mechanism is activated automatically if the **Configure Microsoft Internet Information Services (IIS) automatically** check box is selected in the Exchange Mobile Device Server Installation Wizard (default option).

Otherwise, you will have to activate the authentication mechanism on your own.

► *To activate the Windows authentication mechanism for a PowerShell virtual directory manually:*

1. In Internet Information Services (IIS) Manager console, open the properties of the PowerShell virtual directory.
2. Go to the **Authentication** section.
3. Select **Microsoft Windows Authentication**, and then click the **Enable** button.

4. Open **Advanced Settings**.
5. Select the **Enable Kernel-mode authentication** check box.
6. In the **Extended protection** drop-down list, select **Required**.

When using Microsoft Exchange Server 2007, the IIS web server requires no configuration.

Local installation of an Exchange Mobile Device Server

For a local installation of an Exchange Mobile Device Server, the administrator must perform the following operations:

1. Copy the contents of the \Server\Packages\MDM4Exchange\ folder from the Kaspersky Security Center distribution package to a client device.
2. Run the setup.exe executable file.

Local installation includes two types of installation:

- Standard installation is a simplified installation that does not require the administrator to define any settings; it is recommended in most cases.
- Extended installation is an installation that requires from the administrator to define the following settings:
 - Path for Exchange Mobile Device Server installation.
 - Exchange Mobile Device Server operation mode: standard mode or cluster mode (see section "How to deploy an Exchange Mobile Device Server" on page [142](#)).
 - Possibility of specifying the account under which the Exchange Mobile Device Server service will run (see section "Account for Exchange ActiveSync service" on page [143](#)).
 - Enabling / disabling automatic configuration of the IIS web server.

The Exchange Mobile Device Server Installation Wizard must be run under an account that has all of the required rights (see section "Rights required for deployment of Exchange Mobile Device Server" on page [142](#)).

Remote installation of Exchange Mobile Device Server

► *To configure the remote installation of Exchange Mobile Device Server, the administrator must perform the following actions:*

1. In the tree of Kaspersky Security Center Administration Console, select the **Remote installation** folder, then the **Installation packages** subfolder.
2. In the **Installation packages** subfolder, open the properties of the **Exchange Mobile Device Server** package.
3. Go to the **Settings** section.

This section contains the same settings as those used for the local installation of the application.

After the remote installation is configured, you can start installing Exchange Mobile Device Server.

► *To install Exchange Mobile Device Server:*

1. In the tree of Kaspersky Security Center Administration Console, select the **Remote installation** folder, then the **Installation packages** subfolder.
2. In the **Installation packages** subfolder, select the **Exchange Mobile Device Server** package.

3. Open the context menu of the package and select **Install application**.
4. In the Remote Installation Wizard that opens, select a device (or multiple devices for installation in cluster mode).
5. In the **Run application Setup Wizard under specified account** field, specify the account under which the installation process will be run on the remote device.

The account must have the required rights (see section "Rights required for deployment of Exchange Mobile Device Server" on page [142](#)).

Deploying a system for management using iOS MDM protocol

Kaspersky Security Center allows you to manage mobile devices running iOS. iOS MDM mobile devices refer to iOS mobile devices that are connected to an iOS MDM Server and managed by an Administration Server.

Connection of mobile devices to an iOS MDM Server is performed in the following sequence:

1. The administrator installs iOS MDM Server on the selected client device. Installation of iOS MDM Server is performed using the standard tools of the operating system.
2. The administrator retrieves an Apple Push Notification Service (APNs) certificate (see section "Receiving an APNs certificate" on page [201](#)).

The APNs certificate allows Administration Server to connect to the APNs server to send push notifications to iOS MDM mobile devices.

3. The administrator installs the APNs certificate on the iOS MDM Server (see section "Installing an APNs certificate on an iOS MDM Server" on page [205](#)).
4. The administrator creates an iOS MDM profile for the user of the iOS mobile device.
The iOS MDM profile contains a collection of settings for connecting iOS mobile devices to Administration Server.
5. The administrator issues a shared certificate to the user (see section "Issuing and installing a shared certificate on a mobile device" on page [207](#)).
The shared certificate is required to confirm that the mobile device is owned by the user.
6. The user clicks the link sent by the administrator and downloads an installation package to the mobile device.

The installation package contains a certificate and an iOS MDM profile.

After the iOS MDM profile is downloaded and the iOS MDM mobile device is synchronized with the Administration Server, the device is displayed in the **Mobile devices** folder, which is a subfolder of the **Mobile Device Management** folder in the console tree.

7. The administrator adds a configuration profile on the iOS MDM Server and installs the configuration profile on the mobile device after it is connected.
The configuration profile contains a collection of settings and restrictions for the iOS MDM mobile device, for example, settings for installation of applications, settings for the use of various features of the device, email and scheduling settings. A configuration profile allows you to configure iOS MDM mobile devices in accordance with the organization's security policies.
8. If necessary, the administrator adds provisioning profiles on the iOS MDM Server and then installs these provisioning profiles on mobile devices.

Provisioning profile is a profile that is used for managing applications distributed in ways other than through App Store®. A provisioning profile contains information about the license; it is linked to a specific application.

In this section

Installing iOS MDM Server	193
Installing iOS MDM Server in non-interactive mode.....	194
iOS MDM Server deployment scenarios	198
Simplified deployment scheme	199
Deployment scheme involving Kerberos constrained delegation (KCD).....	199
Use of iOS MDM Server by multiple virtual Servers.....	201
Receiving an APNs certificate	201
Renewing an APNs certificate	203
Configuring a reserve iOS MDM Server certificate	204
Installing an APNs certificate on an iOS MDM Server	205
Configuring access to Apple Push Notification service	206
Issuing and installing a shared certificate on a mobile device	207

Installing iOS MDM Server

► *To install iOS MDM Server on a local device:*

1. Run the setup.exe executable file.

A window opens prompting you to select Kaspersky applications to install.

In the applications selection window, click the **Install iOS MDM Server** link to run the iOS MDM Server Setup Wizard.

2. Select a destination folder.

The default destination folder is <Disk>:\Program Files\Kaspersky Lab\Mobile Device Management for iOS. If such a folder does not exist, it is created automatically during the installation. You can change the destination folder by using the **Browse** button.

3. In the **Specify the settings for connection to iOS MDM Server** window of the Wizard, in the **External port for connection to iOS MDM service** field, specify an external port for connecting mobile devices to the iOS MDM service.

External port 5223 is used by mobile devices for communication with the APNs server. Make sure that port 5223 is open in the firewall for connection with the address range 17.0.0.0/8. Port 443 is used for connection to iOS MDM Server by default. If port 443 is already in use by another service or application, it can be replaced with, for example, port 9443. The iOS MDM Server uses external port 2195 to send notifications to the APNs server.

APNs servers run in load-balancing mode. Mobile devices do not always connect to the same IP addresses to receive notifications. The 17.0.0.0/8 address range is reserved for Apple, and it is therefore recommended to specify this entire range as an allowed range in Firewall settings.

4. If you want to configure interaction ports for application components manually, select the **Set up local ports manually** check box and then specify values for the following settings:
 - **Port for connection to Network Agent.** In this field, specify a port for connecting the iOS MDM service to Network Agent. The default port number is 9799.
 - **Local port to connect to iOS MDM service.** In this field, specify a local port for connecting Network Agent to the iOS MDM service. The default port number is 9899.

It is recommended to use default values.

5. In the **External address of Mobile Device Server** window of the Wizard, in the **Web address for remote connection to Mobile Device Server** field, specify the address of the client device on which iOS MDM Server is to be installed.

This address will be used for connecting managed mobile devices to the iOS MDM service. The client device must be available for connection of iOS MDM devices.

You can specify the address of a client device in any of the following formats:

- Device FQDN (such as `mdm.example.com`)
- Device NetBIOS name
- Device IP address

Please avoid adding the URL scheme and the port number in the address string: these values will be added automatically.

When the Wizard finishes, iOS MDM Server is installed on the local device. The iOS MDM Server is displayed in the **Mobile Device Management** folder in the console tree.

Installing iOS MDM Server in non-interactive mode

Kaspersky Security Center allows you to install iOS MDM Server on a local device in non-interactive mode, that is, without the interactive input of installation settings.

► *To install iOS MDM Server on a local device in non-interactive mode:*

1. Read the End User License Agreement (see section "About the End User License Agreement" on page [318](#)). Use the command below only if you understand and accept the terms of the End User License Agreement.
2. Run the following command:

```
.\exec\setup.exe /s /v"DONT_USE_ANSWER_FILE=1 EULA=1  
<setup_parameters>"
```

where `setup_parameters` is a list of settings and their respective values, separated with spaces (`PRO1=PROP1VAL PROP2=PROP2VAL`). The `setup.exe` file is located in the `Server` folder, which is part of the Kaspersky Security Center distribution kit.

The names and possible values for parameters that can be used when installing iOS MDM Server in non-interactive mode are listed in the table below. Parameters can be specified in any convenient order.

Table 34. Parameters of iOS MDM Server installation in non-interactive mode

Parameter name	Parameter description	Available values
EULA	Acceptance of the terms of the End User License Agreement. This parameter is mandatory.	<ul style="list-style-type: none"> 1—I have fully read, understand and accept the terms of the End User License Agreement. Other value or no value—I do not accept the terms of the License Agreement (installation is not performed).
DONT_USE_ANSWER_FILE	Whether or not to use an XML file with iOS MDM Server installation settings. The XML file is included in the installation package or stored on the Administration Server. You do not have to specify an additional path to the file. This parameter is mandatory.	<ul style="list-style-type: none"> 1—Do not use the XML file with parameters. Other value or no value—Use the XML file with parameters.
INSTALLDIR	The iOS MDM Server installation folder. This parameter is optional.	String value, for example, <code>INSTALLDIR="C:\install\"</code>
CONNECTORPORT	Local port for connecting the iOS MDM service to Network Agent. The default port number is 9799. This parameter is optional.	Numerical value.
LOCALSERVERPORT	Local port for connecting Network Agent to the iOS MDM service. The default port number is 9899. This parameter is optional.	Numerical value.
EXTERNALSERVERPORT	Port for connecting a device to iOS MDM Server. The default port number is 443. This parameter is optional.	Numerical value.
EXTERNAL_SERVER_URL	External address of the client device on which iOS MDM Server is to be installed. This address will be used for connecting managed mobile devices to the iOS MDM service. The client device must be available for connection through iOS MDM. The address must not include the URL scheme and number of the port because these values will be added automatically. This parameter is optional.	<ul style="list-style-type: none"> Device FQDN (such as <code>mdm.example.com</code>) Device NetBIOS name Device IP address
WORKFOLDER	Work folder of iOS MDM Server. If no work folder is specified, data will be written to the default folder. This parameter is optional.	String value, for example, <code>WORKFOLDER="C:\work\"</code>

Parameter name	Parameter description	Available values
MTNCY	Use of iOS MDM Server by multiple virtual Servers. This parameter is optional.	<ul style="list-style-type: none"> • 1—iOS MDM Server will be used by multiple virtual Administration Servers. • Other value or no value—iOS MDM Server will not be used by multiple virtual Administration Servers.

Example:

```
\exec\setup.exe /s /v"EULA=1 DONT_USE_ANSWER_FILE=1
EXTERNALSERVERPORT=9443 EXTERNAL_SERVER_URL=\"www.test-mdm.com\""
```

The iOS MDM Server installation parameters are given in detail in section "Installing iOS MDM Server (on page [193](#))".

iOS MDM Server deployment scenarios

The number of copies of iOS MDM Server to be installed can be selected either based on available hardware or on the total number of mobile devices covered.

Please keep in mind that the recommended maximum number of mobile devices for a single installation of Kaspersky Device Management for iOS is 50,000 at most. In order to reduce the load, the entire pool of devices can be distributed among several servers that have iOS MDM Server installed.

Authentication of iOS MDM devices is performed through user certificates (any profile installed on a device contains the certificate of the device owner). Thus, two deployment schemes are possible for an iOS MDM Server:

- Simplified scheme
- Deployment scheme involving Kerberos constrained delegation (KCD)

See also:

Installing iOS MDM Server	193
Installing iOS MDM Server in non-interactive mode.....	194
Simplified deployment scheme	199
Deployment scheme involving Kerberos constrained delegation (KCD).....	199
Use of iOS MDM Server by multiple virtual Servers.....	201
Receiving an APNs certificate	201
Renewing an APNs certificate	203
Configuring a reserve iOS MDM Server certificate	204
Installing an APNs certificate on an iOS MDM Server	205
Configuring access to Apple Push Notification service	206
Issuing and installing a shared certificate on a mobile device.....	207

Simplified deployment scheme

When deploying an iOS MDM Server under the simplified scheme, mobile devices connect to the iOS MDM web service directly. In this case, user certificates issued by Administration Server can only be applied for devices authentication. Integration with Public Key Infrastructure (PKI) is impossible for user certificates (see section "Standard configuration: Kaspersky Device Management for iOS in DMZ" on page [145](#)).

Deployment scheme involving Kerberos constrained delegation (KCD)

The deployment scheme with Kerberos constrained delegation (KCD) requires the Administration Server and the iOS MDM Server to be located on the internal network of the organization.

This deployment scheme provides for the following:

- Integration with Microsoft Forefront TMG
- Use of KCD for authentication of mobile devices
- Integration with the PKI for applying user certificates

When using this deployment scheme, you must do the following:

- In Administration Console, in the settings of the iOS MDM web service, select the **Ensure compatibility with Kerberos constrained delegation** check box.
- As the certificate for the iOS MDM web service, specify the customized certificate that was defined when the iOS MDM web service was published on TMG.
- User certificates for iOS devices must be issued by the Certificate Authority (CA) of the domain. If the domain contains multiple root CAs, user certificates must be issued by the CA that was specified when the iOS MDM web service was published on TMG.

You can ensure that the user certificate is in compliance with the this CA-issuance requirement by using one of the following methods:

- Specify the user certificate in the New iOS MDM Profile Wizard and in the Certificate Installation Wizard.
- Integrate the Administration Server with the domain's PKI and define the corresponding setting in the rules for issuance of certificates:
 1. In the console tree, expand the **Mobile Device Management** folder and select the **Certificates** subfolder.
 2. In the workspace of the **Certificates** folder, click the **Configure certificate issuance rules** button to open the **Certificate issuance rules** window.
 3. In the **Integration with PKI** section, configure integration with the Public Key Infrastructure.
 4. In the **Issuance of mobile certificates** section, specify the source of certificates.

Below is an example of setup of Kerberos Constrained Delegation (KCD) with the following assumptions:

- The iOS MDM web service is running on port 443.
- The name of the device with TMG is tmg.mydom.local.
- The name of device with the iOS MDM web service is iosmdm.mydom.local.
- The name of external publishing of the iOS MDM web service is iosmdm.mydom.global.

Service Principal Name for http/iosmdm.mydom.local

In the domain, you have to register the service principal name (SPN) for the device with the iOS MDM web service (iosmdm.mydom.local):

```
setspn -a http/iosmdm.mydom.local iosmdm
```

Configuring the domain properties of the device with TMG (tmg.mydom.local)

To delegate traffic, trust the device with TMG (tmg.mydom.local) to the service that is defined by the SPN (http/iosmdm.mydom.local).

► *To trust the device with TMG to the service defined by the SPN (http/iosmdm.mydom.local), the administrator must perform the following actions:*

1. In the Microsoft Management Console snap-in named "Active Directory Users and Computers", select the device with TMG installed (tmg.mydom.local).
2. In the device properties, on the **Delegation** tab, set the **Trust this computer for delegation to specified service only** toggle to **Use any authentication protocol**.
3. Add the SPN (http/iosmdm.mydom.local) to the **Services to which this account can present delegated credentials** list.

Special (customized) certificate for the published web service (iosmdm.mydom.global)

You have to issue a special (customized) certificate for the iOS MDM web service on the FQDN iosmdm.mydom.global and specify that it replaces the default certificate in the settings of iOS MDM web service in Administration Console.

Please note that the certificate container (file with the p12 or pfx extension) must also contain a chain of root certificates (public keys).

Publishing the iOS MDM web service on TMG

On TMG, for traffic that goes from a mobile device to port 443 of iosmdm.mydom.global, you have to configure KCD on the SPN (http/iosmdm.mydom.local), using the certificate issued for the FQDN (iosmdm.mydom.global). Please note that publishing, and the published web service must share the same server certificate.

See also:

Standard configuration: Kaspersky Device Management for iOS in DMZ	145
Integration with Public Key Infrastructure	212

Use of iOS MDM Server by multiple virtual Servers

► To enable the use of iOS MDM Server by multiple virtual Administration Servers:

1. Open the system registry of the client device with iOS MDM Server installed (for example, locally, using the regedit command in the **Start** → **Run** menu).
2. Go to the following hive:
HKEY_LOCAL_MACHINE\SOFTWAREWow6432Node\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0
3. For the ConnectorFlags (DWORD) key, set the 02102482 value.
4. Go to the following hive:
HKEY_LOCAL_MACHINE\SOFTWAREWow6432Node\KasperskyLab\Components\34\1103\1.0.0.0
5. For the ConnInstalled (DWORD) key, set the 00000001 value.
6. Restart the iOS MDM Server service.

Key values must be entered in the specified sequence.

Receiving an APNs certificate

When the Certificate Signing Request (CSR) is created at the first step of the APNs Certificate Wizard, its private key is stored in the RAM of your device. Therefore, all wizard steps must be completed within a single session of the application.

► To receive an APNs certificate:

1. In the console tree, in the **Mobile Device Management** folder select the **Mobile Device Servers** nested folder.
2. In the workspace of the **Mobile Device Servers** folder, select an iOS MDM Server.
3. In the context menu of the iOS MDM Server, select **Properties**.
This opens the properties window of the iOS MDM Server.
4. In the properties window of the iOS MDM Server, select the **Certificates** section.

5. In the **Certificates** section, in the **Apple Push Notification certificate** group of settings, click the **Request new** button.

The Receive APNs Certificate Wizard starts and the **Request new** window opens.

6. Create a Certificate Signing Request (hereinafter referred to as CSR). To do this, perform the following actions:
 - a. Click the **Create CSR** button.
 - b. In the **Create CSR** window that opens, specify a name for your request, the names of your company and department, your city, region, and country.
 - c. Click the **Save** button and specify a name for the file to which your CSR will be saved.

The private key of the certificate is saved in the device memory.

7. Use your CompanyAccount to send the file with the CSR you have created to Kaspersky to be signed.

Signing of your CSR will only be available after you upload to CompanyAccount portal a key that allows using Mobile Device Management.

After your online request is processed, you will receive a CSR file signed by Kaspersky.

8. Send the signed CSR file to Apple Inc. website <https://identity.apple.com/pushcert>, using a random Apple ID.

We recommend that you avoid using a personal Apple ID. Create a dedicated Apple ID to make it your corporate ID. After you have created an Apple ID, link it with the organization's mailbox, not a mailbox of an employee.

After your CSR is processed in Apple Inc., you will receive the public key of the APNs certificate. Save the file on disk.

9. Export the APNs certificate together with the private key created when generating the CSR, in PFX file format. To do this:
 - a. In the **Request new APNs certificate** window, click the **Complete CSR** button.
 - b. In the **Open** window, choose a file with the public key of the certificate, received from Apple Inc. as the result of CSR processing, and click the **Open** button.

The certificate export process will start.

- c. In the next window, enter the private key password and click **OK**.

This password will be used for the APNs certificate installation on the iOS MDM Server.

- d. In the **Save APNs certificate** window, specify a file name for APNs certificate, choose a folder, and click **Save**.

The private and public keys of the certificate are combined, and the APNs certificate is saved in PFX format. After this, you can install the APNs certificate on the iOS MDM Server (see section "Installing an APNs certificate on an iOS MDM Server" on page [205](#)).

See also:

Renewing an APNs certificate	203
------------------------------------	-----

Renewing an APNs certificate

► To renew an APNs certificate:

1. In the console tree, in the **Mobile Device Management** folder select the **Mobile Device Servers** nested folder.
2. In the workspace of the **Mobile Device Servers** folder, select an iOS MDM Server.
3. In the context menu of the iOS MDM Server, select **Properties**.
This opens the properties window of the iOS MDM Server.
4. In the properties window of the iOS MDM Server, select the **Certificates** section.
5. In the **Certificates** section, in the **Apple Push Notification certificate** group of settings click the **Renew** button.

The APNs Certificate Renewal Wizard starts, the **Renew APNs certificate** window opens.

6. Create a Certificate Signing Request (hereinafter referred to as CSR). To do this, perform the following actions:
 - a. Click the **Create CSR** button.
 - b. In the **Create CSR** window that opens, specify a name for your request, the names of your company and department, your city, region, and country.
 - c. Click the **Save** button and specify a name for the file to which your CSR will be saved.

The private key of the certificate is saved in the device memory.

7. Use your CompanyAccount to send the file with the CSR you have created to Kaspersky to be signed.

Signing of your CSR will only be available after you upload to CompanyAccount portal a key that allows using Mobile Device Management.

After your online request is processed, you will receive a CSR file signed by Kaspersky.

8. Send the signed CSR file to Apple Inc. website <https://identity.apple.com/pushcert>, using a random Apple ID.

We recommend that you avoid using a personal Apple ID. Create a dedicated Apple ID to make it your corporate ID. After you have created an Apple ID, link it with the organization's mailbox, not a mailbox of an employee.

After your CSR is processed in Apple Inc., you will receive the public key of the APNs certificate. Save the file on disk.

9. Request the public key of the certificate. To do this, perform the following actions:

- a. Proceed to Apple Push Certificates portal <https://identity.apple.com/pushcert>. To log in to the portal, use the Apple Id received at the initial request of the certificate.
 - b. In the list of certificates, select the certificate whose APSP name (in "APSP: <number>" format) matches the APSP name of the certificate used by iOS MDM Server and click the **Renew** button.
The APNs certificate is renewed.
 - c. Save the certificate created on the portal.
10. Export the APNs certificate together with the private key created when generating the CSR, in PFX file format. To do this, perform the following actions:
- a. In the **Renew APNs certificate** window, click the **Complete CSR** button.
 - b. In the **Open** window, choose a file with the public key of the certificate, received from Apple Inc. as the result of CSR processing, and click the **Open** button.
The certificate export process will start.
 - c. In the next window, enter the private key password and click **OK**.
This password will be used for the APNs certificate installation on the iOS MDM Server.
 - d. In the **Renew APNs certificate** window that opens, specify a file name for APNs certificate, choose a folder, and click **Save**.

The private and public keys of the certificate are combined, and the APNs certificate is saved in PFX format.

See also:

Receiving an APNs certificate[201](#)

Configuring a reserve iOS MDM Server certificate

The iOS MDM Server functionality (see section "Mobile Device Server" on page [47](#)) enables you to issue a reserve certificate. This certificate is intended for use in iOS MDM configuration profiles (see section "Adding a configuration profile" on page [757](#)), to ensure seamless switching of managed iOS devices after the iOS MDM Server certificate expires.

If your iOS MDM Server uses a default certificate issued by Kaspersky, you can issue a reserve certificate (or specify your own custom certificate as reserve) before the iOS MDM Server certificate expires. By default, the reserve certificate is automatically issued 60 days before the iOS MDM Server certificate expiration. The reserve iOS MDM Server certificate becomes the main certificate immediately after the iOS MDM Server certificate expiration. The public key is distributed to all managed devices through configuration profiles, so you do not have to transmit it manually.

► *To issue an iOS MDM Server reserve certificate or specify a custom reserve certificate:*

1. In the console tree, in the **Mobile Device Management** folder, select the **Mobile Device Servers** subfolder.
2. In the list of Mobile Device Servers, select the relevant iOS MDM Server, and on the right pane, click the **Configure iOS MDM Server** button.
3. In the iOS MDM Server settings window that opens, select the **Certificates** section.
4. In the **Reserve certificate** block of settings, do one of the following:

- If you plan to continue using a self-signed certificate (that is, the one issued by Kaspersky):
 - a. Click the **Issue** button.
 - b. In the **Activation date** window that opens, select one of the two options for the date when the reserve certificate must be applied:
 - If you want to apply the reserve certificate at the time of expiration of the current certificate, select the **When current certificate expires** option.
 - If you want to apply the reserve certificate before the current certificate expires, select the **After specified period (days)** option. In the entry field next to this option, specify the duration of the period after which the reserve certificate must replace the current certificate.

The validity period of the reserve certificate that you specify cannot exceed the validity term of the current iOS MDM Server certificate.

- c. Click the **OK** button.

The reserve iOS MDM Server certificate is issued.

- If you plan to use a custom certificate issued by your certification authority:
 - a. Click the **Add** button.
 - b. In the File Explorer window that opens, specify a certificate file in the *.pem, *.pfx, or *.p12 format, which is stored on your device, and then click the **Open** button.

Your custom certificate is specified as the reserve iOS MDM Server certificate.

You have a reserve iOS MDM Server certificate specified. The details of the reserve certificate are displayed in the **Reserve certificate** block of settings (certificate name, issuer name, expiration date, and the date the reserve certificate must be applied, if any).

See also

About Kaspersky Security Center certificates[86](#)

Installing an APNs certificate on an iOS MDM Server

After you receive the APNs certificate, you must install it on the iOS MDM Server.

► *To install the APNs certificate on the iOS MDM Server:*

1. In the console tree, in the **Mobile Device Management** folder select the **Mobile Device Servers** nested folder.
2. In the workspace of the **Mobile Device Servers** folder, select an iOS MDM Server.
3. In the context menu of the iOS MDM Server, select **Properties**.

This opens the properties window of the iOS MDM Server.

4. In the properties window of the iOS MDM Server, select the **Certificates** section.

In the **Certificates** section, in the **Apple Push Notification certificate** group of settings click the **Install** button.

1. Select the PFX file that contains the APNs certificate.
2. Enter the password of the private key specified when exporting the APNs certificate (see section "Receiving an APNs certificate" on page [201](#)).

The APNs certificate will be installed on the iOS MDM Server. The certificate details will be displayed in the properties window of the iOS MDM Server, in the **Certificates** section.

Configuring access to Apple Push Notification service

To ensure a proper functioning of the iOS MDM web service and timely responses of mobile devices to the administrator's commands, you need to specify an Apple Push Notification Service certificate (hereinafter referred to as APNs certificate) in the iOS MDM Server settings.

Interacting with Apple Push Notification (hereinafter referred to as APNs), the iOS MDM web service connects to the external address gateway.push.apple.com through port 2195 (outbound). Therefore, the iOS MDM web service requires access to port TCP 2195 for the range of addresses 17.0.0.0/8. From the iOS device side is access to port TCP 5223 for the range of addresses 17.0.0.0/8.

If you intend to access APNs from the iOS MDM web service side through a proxy server, you must perform the following actions on the device with the iOS MDM web service installed:

1. Add the following strings to the registry:

- For a 32-bit operating system:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0\Conset  
"ApnProxyHost"="<Proxy Host Name>"  
"ApnProxyPort"="<Proxy Port>"  
"ApnProxyLogin"="<Proxy Login>"  
"ApnProxyPwd"="<Proxy Password>"
```

- For a 64-bit operating system:

```
[HKEY_LOCAL_MACHINE\SOFTWAREWow6432Node\KasperskyLab\Components\34\Connectors\KLIOSMDM  
"ApnProxyHost"="<Proxy Host Name>"  
"ApnProxyPort"="<Proxy Port>"  
"ApnProxyLogin"="<Proxy Login>"  
"ApnProxyPwd"="<Proxy Password>"
```

2. Restart the iOS MDM web service.

See also:

Receiving an APNs certificate[201](#)

Issuing and installing a shared certificate on a mobile device

► *To issue a shared certificate to a user:*

1. In the console tree, in the **User accounts** folder, select a user account.
2. In the context menu of the user account, select **Install certificate**.

The Certificate Installation Wizard starts. Follow the instructions of the Wizard.

When the Wizard finishes, a certificate will be created and added to the list of the user's certificates (see section "Working with certificates" on page [737](#)).

The issued certificate will be downloaded by the user, along with the installation package that contains the iOS MDM profile.

After the mobile device is connected to the iOS MDM Server, the iOS MDM profile settings will be applied on the user's device. The administrator will be able to manage the device after connection.

The user's mobile device connected to the iOS MDM Server is displayed in the **Mobile Devices** subfolder within the **Mobile Device Management** folder in the console tree.

Adding a KES device to the list of managed devices

► *To add the KES device of a user to the list of managed devices using a link to Google Play™:*

1. In the console tree, select the **User accounts** folder.
By default, the **User accounts** folder is a subfolder of the **Advanced** folder.
2. Select the account of the user whose mobile device you want add to the list of managed devices.
3. In the context menu of the user account, select **Add mobile device**.

The New Mobile Device Connection Wizard starts. In the **Certificate source** window of the Wizard, you have to specify the method for creating the shared certificate that Administration Server will use to identify the mobile device. You can specify a shared certificate in one of the following ways:

- Create a shared certificate automatically, by means of Administration Server tools, and then deliver the certificate to the device.
 - Specify a shared certificate file.
4. In the **Device type** window of the Wizard, select **Link to Google Play**.
 5. In the **User notification method** window of the Wizard, define the settings for notification of the mobile device user of certificate creation (with an SMS message, by email, or by displaying the information when the Wizard has finished).
 6. In the certificate info window of the Wizard, click the **Finish** button to close the Wizard.

After the Wizard finishes its activities, a link and a QR code will be sent to the mobile device of the user, allowing the user to download Kaspersky Endpoint Security from Google Play. The user proceeds to Google Play by using the link or by scanning the QR code. After this, the operating system of the device prompts the user to accept Kaspersky Endpoint Security for Android installation. After Kaspersky Endpoint Security for Android is downloaded and installed, the mobile device connects to the Administration Server and downloads a shared certificate. After the certificate is installed on the mobile device, the device is displayed in the **Mobile devices** folder, which is a subfolder of the **Mobile Device Management** folder in the console tree.

If Kaspersky Endpoint Security for Android has already been installed on the device, the user has to receive the Administration Server connection settings from the administrator and then enter them independently. After the connection settings are defined, the mobile device connects to the Administration Server. The administrator issues a shared certificate for the device and sends the user an email message or an SMS message with a login and password for the certificate download. The user downloads and installs the shared certificate. After the certificate is installed on the mobile device, the device is displayed in the **Mobile devices** folder, which is a subfolder of the **Mobile Device Management** folder in the console tree. In this case, Kaspersky Endpoint Security for Android will not be downloaded and installed again.

Connecting KES devices to the Administration Server

Depending on the method used for connection of devices to the Administration Server, two deployment schemes are possible for Kaspersky Device Management for iOS for KES devices:

- Scheme of deployment with direct connection of devices to the Administration Server
- Scheme of deployment involving Forefront® Threat Management Gateway (TMG)

In this section

Direct connection of devices to the Administration Server	208
Scheme for connecting KES devices to the Server involving Kerberos constrained delegation (KCD)	209
Using Google Firebase Cloud Messaging	211

Direct connection of devices to the Administration Server

KES devices can connect directly to port 13292 of the Administration Server.

Depending on the method used for authentication, two options are possible for connection of KES devices to the Administration Server:

- Connecting devices with a user certificate
- Connecting devices without a user certificate

Connecting a device with a user certificate

When connecting a device with a user certificate, that device is associated with the user account to which the corresponding certificate has been assigned through Administration Server tools.

In this case, two-way SSL authentication (mutual authentication) will be used. Both the Administration Server and the device will be authenticated with certificates.

Connecting a device without a user certificate

When connecting a device without a user certificate, that device is associated with none of the user's accounts on the Administration Server. However, when the device receives any certificate, the device will be associated with the user to which the corresponding certificate has been assigned through Administration Server tools.

When connecting that device to the Administration Server, one-way SSL authentication will be applied, which means that only the Administration Server is authenticated with the certificate. After the device retrieves the user

certificate, the type of authentication will change to two-way SSL authentication (2-way SSL authentication, mutual authentication (see section "Providing Internet access to the Administration Server" on page [130](#))).

Scheme for connecting KES devices to the Server involving Kerberos constrained delegation (KCD)

The scheme for connecting KES devices to the Administration Server involving Kerberos constrained delegation (KCD) provides for the following:

- Integration with Microsoft Forefront TMG.
- Use of Kerberos Constrained Delegation (hereinafter referred to as KCD) for authentication of mobile devices.
- Integration with Public Key Infrastructure (hereinafter referred to as PKI) for applying user certificates.

When using this connection scheme, please note the following:

- The type of connection of KES devices to TMG must be "two-way SSL authentication", that is, a device must connect to TMG through its proprietary user certificate. To do this, you need to integrate the user certificate into the installation package of Kaspersky Endpoint Security for Android, which has been installed on the device. This KES package must be created by the Administration Server specifically for this device (user).
- You must specify the special (customized) certificate instead of the default server certificate for the mobile protocol:
 1. In the Administration Server properties window, in the **Settings** section select the **Open port for mobile devices** check box and select **Add certificate** in the drop-down list.
 2. In the window that opens, specify the same certificate that was set on TMG when the point of access to the mobile protocol was published on the Administration Server.
- User certificates for KES devices must be issued by the Certificate Authority (CA) of the domain. Keep in mind that if the domain includes multiple root CAs, user certificates must be issued by the CA, which has been set in the publication on TMG.

You can make sure the user certificate is in compliance with the above-described requirement, using one of the following methods:

- Specify the special user certificate in the New Installation Package Wizard and in the Certificate Installation Wizard.
- Integrate the Administration Server with the domain's PKI and define the corresponding setting in the rules for issuance of certificates:
 1. In the console tree, expand the **Mobile Device Management** folder and select the **Certificates** subfolder.
 2. In the workspace of the **Certificates** folder, click the **Configure certificate issuance rules** button to open the **Certificate issuance rules** window.
 3. In the **Integration with PKI** section, configure integration with the Public Key Infrastructure.
 4. In the **Issuance of mobile certificates** section, specify the source of certificates.

See sections:

- Integration with Public Key Infrastructure (on page [212](#)).
- Providing Internet access to the Administration Server (on page [130](#)).

Below is an example of setup of Kerberos Constrained Delegation (KCD) with the following assumptions:

- Point of access to the mobile protocol on the Administration Server is set up on port 13292.
- The name of the device with TMG is `tmg.mydom.local`.
- The name of the device with Administration Server is `ksc.mydom.local`.
- Name of the external publishing of the point of access to the mobile protocol is `kes4mob.mydom.global`.

Domain account for Administration Server

You must create a domain account (for example, `KSCMobileSvcUsr`) under which the Administration Server service will run. You can specify an account for the Administration Server service when installing the Administration Server or through the `klsvswch` utility. The `klsvswch` utility is located in the installation folder of Administration Server.

A domain account must be specified by the following reasons:

- The feature for management of KES devices is an integral part of Administration Server.
- To ensure a proper functioning of Kerberos Constrained Delegation (KCD), the receive side (i.e., the Administration Server) must run under a domain account.

Service Principal Name for `http/kes4mob.mydom.local`

In the domain, under the `KSCMobileSvcUsr` account, add an SPN for publishing the mobile protocol service on port 13292 of the device with Administration Server. For the `kes4mob.mydom.local` device with Administration Server, this will appear as follows:

```
setspn -a http/kes4mob.mydom.local:13292 mydom\KSCMobileSvcUsr
```

Configuring the domain properties of the device with TMG (`tmg.mydom.local`)

To delegate traffic, you must trust the device with TMG (`tmg.mydom.local`) to the service defined by the SPN (`http/kes4mob.mydom.local:13292`).

To trust the device with TMG to the service defined by the SPN (`http/kes4mob.mydom.local:13292`), the administrator must perform the following actions:

1. In the Microsoft Management Console snap-in named "Active Directory Users and Computers", select the device with TMG installed (`tmg.mydom.local`).
2. In the device properties, on the **Delegation** tab, set the **Trust this computer for delegation to specified service only** toggle to **Use any authentication protocol**.
3. In the **Services to which this account can present delegated credentials** list, add the SPN `http/kes4mob.mydom.local:13292`.

Special (customized) certificate for the publishing (`kes4mob.mydom.global`)

To publish the mobile protocol of Administration Server, you must issue a special (customized) certificate for the FQDN `kes4mob.mydom.global` and specify it instead of the default server certificate in the settings of the mobile protocol of Administration Server in Administration Console. To do this, in the properties window of the Administration Server, in the **Settings** section select the **Open port for mobile devices** check box and then select **Add certificate** in the drop-down list.

Please note that the server certificate container (file with the `p12` or `pfx` extension) must also contain a chain of root certificates (public keys).

Configuring publication on TMG

On TMG, for traffic that goes from the mobile device side to port 13292 of kes4mob.mydom.global, you have to configure KCD on the SPN (<http://kes4mob.mydom.local:13292>), using the server certificate issued for the FQDN kes4mob.mydom.global. Please note that publishing and the published access point (port 13292 of the Administration Server) must share the same server certificate.

Using Google Firebase Cloud Messaging

To ensure timely responses of KES devices on Android to the administrator's commands, you must enable the use of Google™ Firebase Cloud Messaging (hereinafter referred to as FCM) in the Administration Server properties.

► *To enable the use of FCM:*

1. In Administration Console, select the **Mobile Device Management** node, and the **Mobile devices** folder.
2. In the context menu of the **Mobile devices** folder, select **Properties**.
3. In the folder properties, select the **Google Firebase Cloud Messaging settings** section.
4. In the **Sender ID** and **Server key** fields, specify the FCM settings: SENDER_ID and API Key.

FCM service runs in the following address ranges:

- From the KES device's side, access is required to ports 443 (HTTPS), 5228 (HTTPS), 5229 (HTTPS), and 5230 (HTTPS) of the following addresses:
 - google.com
 - android.googleapis.com
 - android.apis.google.com
 - All of the IP addresses listed in Google's ASN of 15169
- From the Administration Server side, access is required to port 443 (HTTPS) of the following addresses:
 - android.googleapis.com
 - All of the IP addresses listed in Google's ASN of 15169

If the proxy server settings (**Advanced / Configuring Internet access**) have been specified in the Administration Server properties in Administration Console, they will be used for interaction with FCM.

Configuring FCM: retrieving SENDER_ID and API Key

To configure FCM, the administrator must perform the following actions:

1. Register on Google portal <https://accounts.google.com>.
2. Go to Developers portal <https://console.developers.google.com/project>.
3. Create a new project by clicking the **Create Project** button, specify the project's name, and specify the ID.
4. Wait for the project to be created.

On the first page of the project, in the upper part of the page, the **Project Number** field shows the relevant SENDER_ID.

5. Go to the **APIs & auth / APIs** section and enable **Google Firebase Cloud Messaging for Android**.
6. Go to the **APIs & auth / Credentials** section and click the **Create New Key** button.
7. Click the **Server key** button.

8. Impose restrictions (if any), click the **Create** button.
9. Retrieve the API Key from the properties of the newly created key (**Server key** field).

Integration with Public Key Infrastructure

Integration with Public Key Infrastructure (hereinafter referred to as PKI) is primarily intended for simplifying the issuance of domain user certificates by Administration Server.

The administrator can assign a domain certificate for a user in Administration Console. This can be done using one of the following methods:

- Assign the user a special (customized) certificate from a file in the New Device Connection Wizard or in the Certificate Installation Wizard.
- Perform integration with PKI and assign PKI to act as the source of certificates for a specific type of certificates or for all types of certificates.

The settings of integration with PKI are available in the workspace of the **Mobile Device Management / Certificates** folder by clicking the **Integrate with public key infrastructure** link.

General principle of integration with PKI for issuance of domain user certificates

In Administration Console, click the **Integrate with public key infrastructure** link in the workspace of the **Mobile Device Management / Certificates** folder to specify a domain account that will be used by Administration Server to issue domain user certificates through the domain's CA (hereinafter referred to as the account under which integration with PKI is performed).

Please note the following:

- The settings of integration with PKI provide you the possibility to specify the default template for all types of certificates. Note that the rules for issuance of certificates (available in the workspace of the **Mobile Device Management / Certificates** folder by clicking the **Configure certificate issuance rules** button) allow you to specify an individual template for every type of certificates.
- A special Enrollment Agent (EA) certificate must be installed on the device with Administration Server, in the certificates repository of the account under which integration with PKI is performed. The Enrollment Agent (EA) certificate is issued by the administrator of the domain's CA (Certificate Authority).

The account under which integration with PKI is performed must meet the following criteria:

- It is a domain user.
- It is a local administrator of the device with Administration Server from which integration with PKI is initiated.
- It has the right to *Log On As Service*.
- The device with Administration Server installed must be run at least once under this account to create a permanent user profile.

Kaspersky Security Center Web Server

Kaspersky Security Center Web Server (hereinafter referred to as Web Server) is a component of Kaspersky Security Center. Web Server is designed for publishing stand-alone installation packages, stand-alone installation packages for mobile devices, iOS MDM profiles, and files from the shared folder.

The iOS MDM profiles and installation packages that have been created are published on Web Server automatically and then removed after the first download. The administrator can send the new link to the user in any convenient way, such as by email.

By clicking the link, the user can download the required information to a mobile device.

Web Server settings

If a fine-tuning of Web Server is required, the properties of Administration Console Web Server provide the possibility to change ports for HTTP (8060) and HTTPS (8061). In addition to changing ports, you can replace the server certificate for HTTPS and change the FQDN of Web Server for HTTP.

Installation of Kaspersky Security Center

This section describes local installation of Kaspersky Security Center components. Two installation options are available:

- **Standard.** This option is recommended if you want to try out Kaspersky Security Center by, for example, testing its operation on a small area within your network. During standard installation, you only configure the database. You can also install only the default set of management plug-ins for Kaspersky applications. You can also use standard installation if you already have some experience working with Kaspersky Security Center and are able to specify all relevant settings after standard installation.
- **Custom.** This option is recommended if you plan to modify the Kaspersky Security Center settings, such as a path to the shared folder, accounts and ports for connection to the Administration Server, and database settings. Custom installation enables you to specify which Kaspersky management plug-ins to install. If necessary, you can start custom installation in non-interactive mode (see section "Installing Administration Server in non-interactive mode" on page [253](#)).

If at least one Administration Server is installed on the network, Servers can be installed on other devices remotely through the remote installation task using forced installation (see section "Installing applications using a remote installation task" on page [334](#)). When creating the remote installation task, you must use the Administration Server installation package.

You can use one of the following installation package types:

- `ksc_<version_number>.<build number>_full_<localization language>.exe`. Contains the full set of components to install. Use this package if you want to install all the components required for full functionality of Kaspersky Security Center, or to upgrade the current versions of these components.
- `ksc_<version_number>.<build number>_lite_<localization language>.exe`. Contains the minimum set of components required for Kaspersky Security Center to function. For example, this package does not contain any management plug-ins of Kaspersky Endpoint Security for Windows.

Use this installation package in the following cases:

- You want to upgrade Administration Server.
- You already have installed the components required for full functionality of Kaspersky Security Center, and you intend to continue to use existing versions of these components.
- You want to use Kaspersky Security Center with limited functionality.
- You intend to use Kaspersky Security Center in enterprises where Internet traffic is limited and distribution kits are downloaded separately.

See also:

Main installation scenario	59
Preparing for installation	214
Accounts for work with the DBMS	215
Scenario: Authenticating Microsoft SQL Server	222
Recommendations on Administration Server installation	224
Standard installation	226
Custom installation	232
Installing Administration Server on a failover cluster	243
Installing Administration Server in non-interactive mode	253
Installing Administration Console on the administrator's workstation	258
Changes in the system after Administration Server installation on the device	259
Removing the application	261

Preparing for installation

Before launching installation, make sure that the hardware and software on the device meet the requirements for Administration Server and Administration Console (see section "Hardware and software requirements" on page [31](#)).

It is recommended to install the Administration Server on a dedicated server instead of a domain controller.

Kaspersky Security Center stores its information in a SQL Server database. To do this, you have to install the SQL Server database on your own (learn more about how to select a DBMS (see section "How to select a DBMS for Administration Server" on page [128](#))). Other versions of SQL Server can also be used for storing data. They must be installed on the network before Kaspersky Security Center. Installation of Kaspersky Security Center requires administrator rights on the device on which the installation is performed.

Install Administration Server, Network Agent, and Administration Console in folders where case sensitivity is disabled. Also, case sensitivity must be disabled for the Administration Server shared folder and the Kaspersky Security Center hidden folder (%ALLUSERSPROFILE%\KasperskyLab\adminkit). The server version of Network Agent is installed on the device together with Administration Server. Administration Server cannot be installed together with the regular version of Network Agent. If the server version of Network Agent is already installed on your device, remove it and start installation of Administration Server again.

Starting from version 10 Service Pack 3, Kaspersky Security Center supports managed service accounts and group managed service accounts. If these types of accounts are used in your domain, and you want to specify one of them as the account for the Administration Server service, then first install the account on the same device on which you want to install Administration Server. For details about installation of managed service accounts on a

local device, refer to the official Microsoft documentation <https://docs.microsoft.com/en-us/powershell/module/addsadministration/install-adserviceaccount?view=win10-ps>.

Accounts for work with the DBMS

The following tables provide information about how selecting a database management system (DBMS) affects the properties of accounts chosen for work with the DBMS.

A *local DBMS* is a DBMS installed on the same device as Administration Server. A *remote DBMS* is a DBMS installed on a different device.

Please grant all rights required for the Administration Server account before you start the Administration Server service.

SQL Server with Windows authentication and with SQL Server authentication

Table 35. DBMS: SQL Server (including Express Edition) with Windows authentication

DBMS location	Local	Local	Remote	Remote
Who creates the KAV database	The installer (automatically)	Administrator (manually)	The installer (automatically)	Administrator (manually).
Account under which the installer is running	Local or domain	Local or domain	Domain	Domain.
Rights of the account under which the installer is running	<ul style="list-style-type: none"> System: Local administrator rights SQL Server: System administrator role 	<ul style="list-style-type: none"> System: Local administrator rights SQL Server: Server-level roles: public and dbcreator VIEW ANY DEFINITION permission VIEW SERVER STATE permission (if AlwaysOn is set) For master and tempdb databases: public role and dbo schema For KAV database (only if an existing KAV database is used): db_owner role and dbo schema 	<ul style="list-style-type: none"> System: Local administrator rights SQL Server: Sysadmin role 	<ul style="list-style-type: none"> System: Local administrator rights. SQL Server: Server-level roles: public and dbcreator VIEW ANY DEFINITION permission VIEW SERVER STATE permission (if AlwaysOn is set) For master and tempdb databases: public role and dbo schema For KAV database (only if an existing KAV database is used): db_owner role and dbo schema

<p>Administration Server account</p>	<ul style="list-style-type: none"> • Created automatically in KL-AK-* format • Local account selected by the administrator • Domain account selected by the administrator 	<ul style="list-style-type: none"> • Created automatically in KL-AK-* format • Local account selected by the administrator • Domain account selected by the administrator 	<p>Domain.</p>	<p>Domain.</p>
<p>Rights of the Administration Server service account</p>	<ul style="list-style-type: none"> • System: required rights assigned by the installer • SQL Server: required rights assigned by the installer 	<ul style="list-style-type: none"> • System: Required rights assigned by the installer. • SQL Server: <ul style="list-style-type: none"> Server-level role: public VIEW ANY DEFINITION permission VIEW SERVER STATE permission (if AlwaysOn is set) For master and tempdb databases: public role and dbo schema For KAV database: db_owner role and dbo schema 	<ul style="list-style-type: none"> • System: required rights assigned by the installer • SQL Server: required rights assigned by the installer 	<ul style="list-style-type: none"> • System: Required rights assigned by the installer. • SQL Server: <ul style="list-style-type: none"> Server-level role: public VIEW ANY DEFINITION permission VIEW SERVER STATE permission (if AlwaysOn is set) For master and tempdb databases: public role and dbo schema For KAV database: db_owner role and dbo schema

Table 36. DBMS: SQL Server (including Express Edition) with SQL Server authentication

DBMS location	Local.	Remote.
Who creates the KAV database	Administrator (manually) or the installer (automatically).	Administrator (manually) or the installer (automatically).
Account under which the installer is running	Local.	Domain.
Rights of the account under which the installer is running	<ul style="list-style-type: none"> System: Local administrator rights. SQL Server: Installer account does not require access to SQL Server. 	<ul style="list-style-type: none"> System: Local administrator rights. SQL Server: Installer account does not require access to SQL Server.
Administration Server service account	Local or domain.	Domain.
Rights of the Administration Server service account	<ul style="list-style-type: none"> System: Required rights assigned by the installer. SQL Server: Administration Server service account does not require access to SQL Server. 	<ul style="list-style-type: none"> System: Required rights assigned by the installer. SQL Server: Administration Server service account does not require access to SQL Server.
Additional information	The administrator explicitly specifies in the installer a SQL Server internal account that requires the sysadmin role.	The administrator explicitly specifies in the installer a SQL Server internal account that requires the sysadmin role.

MySQL

Table 37. DBMS: MySQL

DBMS location	Local or remote.	Local or remote.
Who creates the KAV database	The installer (automatically).	Administrator (manually).
Account under which the installer is running	Local or domain.	Local or domain.
Rights of the account under which the installer is running	<ul style="list-style-type: none"> • System: Local administrator rights. • MySQL Server: Installer account does not require access to MySQL. 	<ul style="list-style-type: none"> • System: Local administrator rights. • MySQL Server: Installer account does not require access to MySQL.
Administration Server service account	Local or domain.	Local or domain.
Rights of the Administration Server service account	<ul style="list-style-type: none"> • System: Required rights assigned by the installer. • MySQL Server: Administration Server service account does not require access to MySQL. 	<ul style="list-style-type: none"> • System: Required rights assigned by the installer. • MySQL Server: Administration Server service account does not require access to MySQL.

<p>Additional information</p>	<p>The administrator explicitly specifies in the installer a SQL Server internal account that requires root access.</p>	<p>The administrator explicitly specifies in the installer a MySQL internal account that requires GRANT ALL for the KAV database and SELECT, SHOW VIEW, or PROCESS for the system tables. Required permissions for MySQL Server are:</p> <ul style="list-style-type: none"> • SELECT • INSERT • UPDATE • DELETE • CREATE • DROP • PROCESS • REFERENCES • INDEX • ALTER • SHOW DATABASES • CREATE TEMPORARY TABLES • LOCK TABLES • EXECUTE • CREATE VIEW • SHOW VIEW • CREATE ROUTINE • ALTER ROUTINE • EVENT • TRIGGER • SUPER <p>The SUPER permission is required only for restoring from a backup.</p>
-------------------------------	---	---

MariaDB

Table 38. DBMS: MariaDB

DBMS location	Local or remote.	Local or remote.
Who creates the KAV database	The installer (automatically).	Administrator (manually).
Account under which the installer is running	Local or domain.	Local or domain.
Rights of the account under which the installer is running	<ul style="list-style-type: none"> • System: Local administrator rights. • MariaDB Server: Installer account does not require access to MariaDB. 	<ul style="list-style-type: none"> • System: Local administrator rights. • MariaDB Server: Installer account does not require access to MariaDB.
Administration Server service account	Local or domain.	Local or domain.
Rights of the Administration Server service account	<ul style="list-style-type: none"> • System: Required rights assigned by the installer. • MariaDB Server: Administration Server service account does not require access to MariaDB. 	<ul style="list-style-type: none"> • System: Required rights assigned by the installer. • MariaDB Server: Administration Server service account does not require access to MariaDB.
Additional information	The administrator explicitly specifies in the installer a SQL Server internal account that requires root access.	The administrator explicitly specifies in the installer a MariaDB internal account that requires <code>GRANT ALL</code> for the KAV database and <code>SELECT, SHOW VIEW, PROCESS</code> for the system tables.

Scenario: Authenticating Microsoft SQL Server

Information in this section is only applicable to configurations in which Kaspersky Security Center uses Microsoft SQL Server as a database management system.

To protect Kaspersky Security Center data transferred to or from the database and data stored in the database from unauthorized access, you must secure communication between Kaspersky Security Center and SQL Server. The most reliable way to provide secure communication is to install Kaspersky Security Center and SQL Server on the same device and use the shared memory mechanism for both applications. In all other cases, we recommend that you use a SSL or TLS certificate to authenticate the SQL Server instance. You can use a certificate from a trusted certification authority (CA) or a self-signed certificate. We recommend that you use a certificate from a trusted CA because a self-signed certificate provides only limited protection.

SQL Server authentication proceeds in stages:

- a. **Generating a self-signed SSL or TLS certificate for SQL Server according to the certificate requirements <https://docs.microsoft.com/en-us/sql/database-engine/configure->**

windows/enable-encrypted-connections-to-the-database-engine?view=sql-server-2017#certificate-requirements

If you already have a certificate for SQL Server, skip this step.

An SSL certificate is only applicable to SQL Server versions earlier than 2016 (13.x). In SQL Server 2016 (13.x) and later versions, use a TLS certificate.

For example, to generate a TLS certificate, enter the following command in PowerShell:

```
New-SelfSignedCertificate -DnsName SQL_HOST_NAME -CertStoreLocation
cert:\LocalMachine -KeySpec KeyExchange
```

In the command, instead of SQL_HOST_NAME you must type the SQL Server host name if the host is included in the domain or type the *fully qualified domain name (FQDN)* of the host if the host is not included in the domain. The same name—host name or FQDN—must be specified as an SQL Server instance name in the Administration Server Setup Wizard (see section "Step 7. Configuring the SQL Server" on page 237).

b. Adding the certificate on the SQL Server instance

The instructions for this stage depend on the platform on which SQL Server is running. Refer to the official documentation for details:

Windows <https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/enable-encrypted-connections-to-the-database-engine?view=sql-server-2017>

Linux <https://docs.microsoft.com/en-us/sql/linux/sql-server-linux-encrypted-connections?view=sql-server-2017>

Amazon Relational Database Service https://docs.aws.amazon.com/en_us/AmazonRDS/latest/UserGuide/UsingWithRDS.SSL.html

Windows Azure <https://azure.microsoft.com/en-us/blog/windows-azure-root-certificate-migration/>

To use the certificate on a failover cluster, you must install the certificate on each node of the failover cluster. For details, refer to the Microsoft documentation <https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/manage-certificates?view=sql-server-2017>.

c. Assigning the service account permissions

Ensure that the service account under which the SQL Server service is run has the Full control permission to access private keys. For details, refer to the Microsoft documentation <https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/enable-encrypted-connections-to-the-database-engine?view=sql-server-2017#to-provision-install-a-certificate-on-a-single-server>.

d. Adding the certificate to the list of trusted certificates for Kaspersky Security Center

On the Administration Server device, add the certificate to the list of trusted certificates. For details, refer to the Microsoft documentation <https://docs.microsoft.com/en-us/skype-sdk/sdn/articles/installing-the-trusted-root-certificate>.

e. Enabling encrypted connections between the SQL Server instance and Kaspersky Security Center

On the Administration Server device, set value 1 to the environment variable *KLDBADO_UseEncryption*. For example, in Windows Server 2012 R2, you can change environment variables by clicking **Environment Variables** on the **Advanced** tab of the **System Properties** window. Add a new variable, name it *KLDBADO_UseEncryption*, and then set value 1.

f. Additional configuration to use TLS 1.2 protocol

If you use the TLS 1.2 protocol, then additionally do the following:

- Ensure that the installed version of SQL Server is a 64-bit application.
- Install Microsoft OLE DB Driver on the Administration Server device. For details, refer to the Microsoft documentation <https://docs.microsoft.com/en-us/sql/connect/oledb/oledb-driver-for-sql-server?view=sql-server-2017>.

- On the Administration Server device, set value 1 to the environment variable `KLDBADO_UseMSOLEDBSQL`. For example, in Windows Server 2012 R2, you can change environment variables by clicking **Environment Variables** on the **Advanced** tab of the **System Properties** window. Add a new variable, name it `KLDBADO_UseMSOLEDBSQL`, and then set value 1.

g. Enabling usage of TCP/IP protocol on a named instance of SQL Server

If you use a named instance of SQL Server, then additionally enable usage of TCP/IP protocol <https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/enable-or-disable-a-server-network-protocol?view=sql-server-ver15> and assign a TCP/IP port number <https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/configure-a-server-to-listen-on-a-specific-tcp-port?view=sql-server-ver15> to the SQL Server Database Engine. When you configure SQL Server connection in the Administration Server Setup Wizard (see section "Step 7. Configuring the SQL Server" on page [237](#)), specify the SQL Server host name and the port number in the **SQL Server instance name** field.

Recommendations on Administration Server installation

This section contains recommendations on how to install Administration Server. This section also provides scenarios for using a shared folder on the Administration Server device in order to deploy Network Agent on client devices.

In this section

Creating accounts for the Administration Server services on a failover cluster	224
Defining a shared folder.....	224
Remote installation with Administration Server tools through Active Directory group policies	225
Remote installation through delivery of the UNC path to a stand-alone package.....	225
Updating from the Administration Server shared folder	225
Installing images of operating systems.....	225
Specifying the address of the Administration Server.....	226

Creating accounts for the Administration Server services on a failover cluster

By default, the installer automatically creates non-privileged accounts for services of Administration Server. This behavior is the most convenient for Administration Server installation on an ordinary device.

However, installation of Administration Server on a failover cluster requires a different scenario:

1. Create non-privileged domain accounts for services of Administration Server and make them members of a global domain security group named `KLAdmins`.
2. In the Administration Server Installer, specify the domain accounts (see section "Step 10. Selecting the account for running the Kaspersky Security Center services" on page [240](#)) that have been created for the services.

Defining a shared folder

When installing Administration Server, you can specify the location of the shared folder. You can also specify the location of the shared folder after installation, in the Administration Server properties. By default, the shared folder

will be created on the device with Administration Server (with read rights for the **Everyone** subgroup). However, in some cases (such as high load or a need for access from an isolated network), it is useful to locate the shared folder on a dedicated file resource.

The shared folder is used occasionally in Network Agent deployment.

Case sensitivity for the shared folder must be disabled.

See also:

Remote installation with Administration Server tools through Active Directory group policies	225
Remote installation through delivery of the UNC path to a stand-alone package.....	225
Updating from the Administration Server shared folder	225
Installing images of operating systems.....	714

Remote installation with Administration Server tools through Active Directory group policies

If the target devices are located within a Windows domain (no workgroups), initial deployment (installation of Network Agent and the security application on devices that are not yet managed) has to be performed through group policies of Active Directory. Deployment is performed by using the standard task for remote installation of Kaspersky Security Center. If the network is large-scale, it is useful to locate the shared folder on a dedicated file resource to reduce the load on the disk subsystem of the Administration Server device.

Remote installation through delivery of the UNC path to a stand-alone package

If the users of networked devices in the organization have local administrator rights, another method of initial deployment is to create a stand-alone Network Agent package (or even a "coupled" Network Agent package together with the security application). After you create a stand-alone package, send users a link to that package, which is stored in the shared folder. Installation starts when users click the link.

Updating from the Administration Server shared folder

In the Anti-Virus update task, you can configure updating from the shared folder of Administration Server. If the task has been assigned to a large number of devices, it is useful to locate the shared folder on a dedicated file resource.

Installing images of operating systems

Operating system images are always installed through the shared folder: devices read operating system images from the shared folder. If deployment of images is planned on a large number of corporate devices, it is useful to locate the shared folder on a dedicated file resource.

See also:

Deploying Network Agent and the security application[150](#)

Specifying the address of the Administration Server

When installing Administration Server, you can specify the address of the Administration Server. This address will be used as the default address when creating installation packages of Network Agent. By default, the NetBIOS name of the Administration Server device is used. If the Domain Name System (DNS) on the organization's network has been configured and is functioning properly, specify in the DNS the FQDN of the Administration Server device. If Administration Server is installed in the DMZ, it may be useful to specify the external address of the Administration Server. After that, you will be able to change the address of the Administration Server by using Administration Console tools; the address will not change automatically in Network Agent installation packages that have been already created.

See also:

Internet access: Administration Server in DMZ[131](#)

Standard installation

Standard installation is an Administration Server installation that uses the default paths for application files, installs the default set of plug-ins, and does not enable Mobile Device Management.

► *To install Kaspersky Security Center Administration Server on a local device:*

Run the `ksc_13.<build number>_full_<localization language>.exe` executable file.

A window opens prompting you to select Kaspersky applications to install. In the application selection window, click the **Install Kaspersky Security Center 13 Administration Server** link to start the Administration Server Setup Wizard. Follow the instructions of the Wizard.

Below are the steps of the Setup Wizard and actions that you can perform at each step.

In this section

Step 1. Reviewing the License Agreement and Privacy Policy	227
Step 2. Selecting an installation method	227
Step 3. Installing Kaspersky Security Center 13 Web Console	227
Step 4. Selecting network size	228
Step 5. Selecting a database.....	230
Step 6. Configuring the SQL Server	230
Step 7. Selecting an authentication mode	231
Step 8. Unpacking and installing files on the hard drive.....	232

Step 1. Reviewing the License Agreement and Privacy Policy

At this step of the Setup Wizard, you must read the License Agreement, which is to be concluded between you and Kaspersky, as well as the Privacy Policy.

You may also be prompted to view the License Agreements and Privacy Policies for application management plug-ins that are available in the Kaspersky Security Center distribution kit.

Please carefully read the License Agreement and Privacy Policy. If you agree with all the terms of the License Agreement and the Privacy Policy, select the following check boxes in the **I confirm I have fully read, understood, and accept the following** section:

- **The terms and conditions of this EULA**
- **Privacy Policy describing the handling of data**

Installation of the application on your device will continue after you select both check boxes.

If you do not accept the License Agreement or the Privacy Policy, cancel installation by clicking the **Cancel** button.

Step 2. Selecting an installation method

In the installation type selection window, select **Standard**.

Standard installation is recommended if you want to try out Kaspersky Security Center by, for example, testing its operation on a small area within your enterprise network. During standard installation, you only configure the database. You do not specify any Administration Server settings: their respective default values are used instead. Standard installation does not allow you to select management plug-ins to install; only the default set of plug-ins is installed. During standard installation, no installation packages for mobile devices are created. However, you can create them later in Administration Console.

Step 3. Installing Kaspersky Security Center 13 Web Console

This step is displayed only if you are using a 64-bit operating system. Otherwise, this step is not displayed, because Kaspersky Security Center 13 Web Console does not work with 32-bit operating systems.

By default, both Kaspersky Security Center 13 Web Console and MMC-based Administration Console will be installed.

► *If you want to install only Kaspersky Security Center 13 Web Console:*

1. Select **Install only this one**.
2. Choose **Web-based console** in the drop-down list.

Installation of Kaspersky Security Center 13 Web Console (see section "Installation" on page [964](#)) starts automatically after completion of Administration Server installation.

► *If you want to install only the MMC-based console:*

1. Select **Install only this one**.
2. Choose **MMC-based console** in the drop-down list.

Step 4. Selecting network size

Specify the size of the network on which Kaspersky Security Center is to be installed. Depending on the number of devices on the network, the Wizard configures the installation and appearance of the application interface so that they match.

The following table lists the application installation settings and interface appearance settings, which are adjusted based on various network sizes.

Table 39. Dependence of installation settings on the network scale selected

Settings	1—100 devices	100—1000 devices	1000—5000 devices	More than 5000 devices
Display with the node for secondary and virtual Administration Servers, and all settings related to the secondary and virtual Administration Servers in the console tree	not available	not available	available	available
Display with the Security sections in the properties windows of the Administration Server and administration groups	not available	not available	available	available
Random distribution of startup time for the update task on client devices	not available	Over an interval of 5 minutes	Over an interval of 10 minutes	Over an interval of 10 minutes

If you connect Administration Server to a MySQL or SQL Express database server, it is not recommended to use the application to manage more than 10 000 devices. For the MariaDB database management system, the maximum recommended number of managed devices is 20 000.

Step 5. Selecting a database

At this step of the Wizard, you must select the mechanism—Microsoft SQL Server (SQL Express) or MySQL—that will be used to store the Administration Server database. The MySQL option is relevant to both MySQL and MariaDB.

It is recommended to install the Administration Server on a dedicated server instead of a domain controller. However, if you install Kaspersky Security Center on a server that acts as a read-only domain controller (RODC), Microsoft SQL Server (SQL Express) must not be installed locally (on the same device). In this case, we recommend that you install Microsoft SQL Server (SQL Express) remotely (on a different device), or that you use MySQL or MariaDB, if you need to install the DBMS locally.

The Administration Server database structure is provided in the klakdb.chm file, which is located in the Kaspersky Security Center installation folder (this file is also available in an archive on the Kaspersky portal: klakdb.zip (<https://media.kaspersky.com/utilities/CorporateUtilities/klakdb.zip>)).

See also:

Selecting a DBMS.....129

Step 6. Configuring the SQL Server

At this step of the Wizard, you configure SQL Server.

Depending on the database that you have selected, specify the following settings:

- If you selected **Microsoft SQL Server (SQL Server Express)** in the previous step:
 - In the **SQL Server instance name** field, specify the name of the SQL Server on the network. To view a list of all SQL Servers that are on the network, click the **Browse** button. This field is blank by default.

If you connect to the SQL Server through a custom port, then together with the SQL Server host name specify the port number separated with a comma, for example:

`SQL_Server_host_name,1433`

If you secure communication between the Administration Server and SQL Server by means of a certificate (see section "Scenario: Authenticating Microsoft SQL Server" on page 222), specify in the **SQL Server instance name** field the same host name that was used at the certificate generating. If you use a named instance of SQL Server, then together with the SQL Server host name specify the port number separated with a comma, for example:

`SQL_Server_name,1433`

If you use several instances of SQL Server on the same host, then additionally specify the instance name separated with a backslash, for example:

`SQL_Server_name\SQL_Server_instance_name,1433`

If a SQL Server that has AlwaysON support enabled is on the enterprise network, in the **SQL Server instance name** field specify the name of the availability group listener.

- In the **Database name** field, specify the name of the database that has been created to store Administration Server data. The default value is *KAV*.
- If you selected **MySQL** in the previous step:
 - In the **SQL Server instance name** field, specify the name of the SQL Server instance. By default, the name is the IP address of the device on which Kaspersky Security Center is to be installed.
 - In the **Port** field, specify the port for Administration Server connection to the SQL Server database. The default port number is 3306.
 - In the **Database name** field, specify the name of the database that has been created to store Administration Server data. The default value is *KAV*.

If at this stage you want to install SQL Server on the device from which you are installing Kaspersky Security Center, you must stop installation and restart it after SQL Server is installed. The supported SQL Server versions are listed in the system requirements.

If you want to install SQL Server on a remote device, you do not have to interrupt the Kaspersky Security Center Setup Wizard. Install SQL Server and resume installation of Kaspersky Security Center.

Step 7. Selecting an authentication mode

Determine the authentication mode that will be used when Administration Server connects to the SQL Server.

Depending on the database that is selected, you can choose from the following authentication modes.

- For SQL Express or Microsoft SQL Server select one of the following options:
 - **Microsoft Windows Authentication mode.** Verification of rights uses the account used for starting Administration Server.
 - **SQL Server Authentication mode.** If you select this option, the account specified in the window is used to verify access rights. Fill in the **Account** and **Password** fields.

To see the entered password, click and hold the **Show** button.

For both authentication modes, the application checks if the database is available. If the database is not available, an error message is displayed, and you have to provide correct credentials.

If the Administration Server database is stored on another device and the Administration Server account does not have access to the database server, you must use SQL Server authentication mode when installing or upgrading Administration Server. This may occur when the device that stores the database is outside the domain or when Administration Server is installed under a LocalSystem account.

- For the MySQL server or MariaDB server, specify the account and password.

Step 8. Unpacking and installing files on the hard drive

After the installation of Kaspersky Security Center components is configured, you can start installing files on the hard drive.

If installation requires additional programs, the Setup Wizard will notify you, on the **Installing Prerequisites** page, before installation of Kaspersky Security Center begins. The required programs are installed automatically after you click the **Next** button.

On the last page, you can select which console to start for work with Kaspersky Security Center:

- **Start MMC-based Administration Console**
- **Start Kaspersky Security Center Web Console**

This option is available only if you opted to install Kaspersky Security Center 13 Web Console in one of the previous steps.

You can also click **Finish** to close the Wizard without starting work with Kaspersky Security Center. You can start the work later at any time.

At the first startup of Administration Console or Kaspersky Security Center 13 Web Console, you can perform the initial setup of the application (on page [265](#)).

When the Setup Wizard finishes, the following application components are installed on the hard drive on which the operating system was installed:

- Administration Server (together with the server version of Network Agent)
- Microsoft Management Console-based Administration Console
- Kaspersky Security Center 13 Web Console (if you chose to install it)
- Application management plug-ins available in the distribution kit

Additionally, Microsoft Windows Installer 4.5 will be installed if it was not installed previously.

Custom installation

Custom installation is an Administration Server installation during which you are prompted to select components to install and specify the folder in which the application must be installed.

Using this type of installation, you can configure the database and Administration Server, as well as install components that are not included in standard installation or management plug-ins for various Kaspersky security applications. You can also enable Mobile Device Management.

► *To install Kaspersky Security Center Administration Server on a local device:*

Run the `ksc_13.<build number>_full_<localization language>.exe` executable file.

A window opens prompting you to select Kaspersky applications to install. In the application selection window, click the **Install Kaspersky Security Center 13 Administration Server** link to start the Administration Server Setup Wizard. Follow the instructions of the Wizard.

Below are the steps of the Setup Wizard and actions that you can perform at each step.

See also:

Scenario: Upgrading Kaspersky Security Center and managed applications	405
Step 1. Reviewing the License Agreement and Privacy Policy	233
Step 2. Selecting an installation method	233
Step 3. Selecting the components to be installed	234
Step 4. Installing Kaspersky Security Center 13 Web Console	234
Step 5. Selecting network size	235
Step 6. Selecting a database.....	236
Step 7. Configuring the SQL Server	237
Step 8. Selecting an authentication mode	238
Step 9. Selecting the account to start Administration Server	238
Step 10. Selecting the account for running the Kaspersky Security Center services	240
Step 11. Selecting a shared folder	240
Step 12. Configuring the connection to Administration Server.....	241
Step 13. Defining the Administration Server address.....	241
Step 14. Administration Server address for connection of mobile devices	242
Step 15. Selecting application management plug-ins	242
Step 16. Unpacking and installing files on the hard drive.....	242

Step 1. Reviewing the License Agreement and Privacy Policy

At this step of the Setup Wizard, you must read the License Agreement, which is to be concluded between you and Kaspersky, as well as the Privacy Policy.

You may also be prompted to view the License Agreements and Privacy Policies for application management plug-ins that are available in the Kaspersky Security Center distribution kit.

Please carefully read the License Agreement and Privacy Policy. If you agree with all the terms of the License Agreement and the Privacy Policy, select the following check boxes in the **I confirm I have fully read, understood, and accept the following** section:

- **The terms and conditions of this EULA**
- **Privacy Policy describing the handling of data**

Installation of the application on your device will continue after you select both check boxes.

If you do not accept the License Agreement or the Privacy Policy, cancel installation by clicking the **Cancel** button.

Step 2. Selecting an installation method

In the installation type selection window, specify **Custom**.

Custom installation allows you to modify the Kaspersky Security Center settings, such as the path to the shared folder, accounts and ports for connection to the Administration Server, and database settings. Custom installation allows you to specify which Kaspersky management plug-ins to install. During custom installation, you can create installation packages for mobile devices by enabling the corresponding option.

Step 3. Selecting the components to be installed

Select the components of Kaspersky Security Center Administration Server that you want to install:

- **Mobile Device Management.** Select this check box if you must create installation packages for mobile devices when the Kaspersky Security Center Setup Wizard is running. You can also create installation packages for mobile devices manually, after Administration Server installation, by using Administration Console tools (see section "Creating installation packages of applications" on page [717](#)).
- **SNMP agent.** This component receives statistical information for the Administration Server over the SNMP protocol. The component is available if the application is installed on a device with SNMP installed.

After Kaspersky Security Center is installed, the .mib files required for receiving statistics are located in the SNMP subfolder of the application installation folder.

Network Agent and Administration Console are not displayed in the component list. These components are installed automatically and you cannot cancel their installation.

At this step you must specify a folder for installation of Administration Server components. By default, the components are installed to <Disk>:\Program Files\Kaspersky Lab\Kaspersky Security Center. If no such folder exists, this folder is created automatically during installation. You can change the destination folder by using the **Browse** button.

Step 4. Installing Kaspersky Security Center 13 Web Console

This step is displayed only if you are using a 64-bit operating system. Otherwise, this step is not displayed, because Kaspersky Security Center 13 Web Console does not work with 32-bit operating systems.

By default, both Kaspersky Security Center 13 Web Console and MMC-based Administration Console will be installed.

► *If you want to install only Kaspersky Security Center 13 Web Console:*

1. Select **Install only this one**.
2. Choose **Web-based console** in the drop-down list.

Installation of Kaspersky Security Center 13 Web Console (see section "Installation" on page [964](#)) starts automatically after completion of Administration Server installation.

► *If you want to install only the MMC-based console:*

1. Select **Install only this one**.
2. Choose **MMC-based console** in the drop-down list.

Step 5. Selecting network size

Specify the size of the network on which Kaspersky Security Center is to be installed. Depending on the number of devices on the network, the Wizard configures the installation and appearance of the application interface so that they match.

The following table lists the application installation settings and interface appearance settings, which are adjusted based on various network sizes.

Table 40. Dependence of installation settings on the network scale selected

Settings	1—100 devices	100—1000 devices	1000—5000 devices	More than 5000 devices
Display with the node for secondary and virtual Administration Servers, and all settings related to the secondary and virtual Administration Servers in the console tree	not available	not available	available	available
Display with the Security sections in the properties windows of the Administration Server and administration groups	not available	not available	available	available
Random distribution of startup time for the update task on client devices	not available	Over an interval of 5 minutes	Over an interval of 10 minutes	Over an interval of 10 minutes

If you connect Administration Server to a MySQL or SQL Express database server, it is not recommended to use the application to manage more than 10 000 devices. For the MariaDB database management system, the maximum recommended number of managed devices is 20 000.

Step 6. Selecting a database

At this step of the Wizard, you must select the mechanism—Microsoft SQL Server (SQL Express) or MySQL—that will be used to store the Administration Server database. The MySQL option is relevant to both MySQL and MariaDB.

It is recommended to install the Administration Server on a dedicated server instead of a domain controller. However, if you install Kaspersky Security Center on a server that acts as a read-only domain controller (RODC), Microsoft SQL Server (SQL Express) must not be installed locally (on the same device). In this case, we recommend that you install Microsoft SQL Server (SQL Express) remotely (on a different device), or that you use MySQL or MariaDB, if you need to install the DBMS locally.

The Administration Server database structure is provided in the `klakdb.chm` file, which is located in the Kaspersky Security Center installation folder (this file is also available in an archive on the Kaspersky portal: `klakdb.zip`) (<https://media.kaspersky.com/utilities/CorporateUtilities/klakdb.zip>).

Step 7. Configuring the SQL Server

At this step of the Wizard, you configure SQL Server.

Depending on the database that you have selected, specify the following settings:

- If you selected **Microsoft SQL Server (SQL Server Express)** in the previous step:
 - In the **SQL Server instance name** field, specify the name of the SQL Server on the network. To view a list of all SQL Servers that are on the network, click the **Browse** button. This field is blank by default.

If you connect to the SQL Server through a custom port, then together with the SQL Server host name specify the port number separated with a comma, for example:

```
SQL_Server_host_name,1433
```

If you secure communication between the Administration Server and SQL Server by means of a certificate (see section "Scenario: Authenticating Microsoft SQL Server" on page [222](#)), specify in the **SQL Server instance name** field the same host name that was used at the certificate generating. If you use a named instance of SQL Server, then together with the SQL Server host name specify the port number separated with a comma, for example:

```
SQL_Server_name,1433
```

If you use several instances of SQL Server on the same host, then additionally specify the instance name separated with a backslash, for example:

```
SQL_Server_name\SQL_Server_instance_name,1433
```

If a SQL Server that has AlwaysON support enabled is on the enterprise network, in the **SQL Server instance name** field specify the name of the availability group listener.

- In the **Database name** field, specify the name of the database that has been created to store Administration Server data. The default value is `KAV`.
- If you selected **MySQL** in the previous step:
 - In the **SQL Server instance name** field, specify the name of the SQL Server instance. By default, the name is the IP address of the device on which Kaspersky Security Center is to be installed.
 - In the **Port** field, specify the port for Administration Server connection to the SQL Server database. The default port number is 3306.

- In the **Database name** field, specify the name of the database that has been created to store Administration Server data. The default value is *KAV*.

If at this stage you want to install SQL Server on the device from which you are installing Kaspersky Security Center, you must stop installation and restart it after SQL Server is installed. The supported SQL Server versions are listed in the system requirements.

If you want to install SQL Server on a remote device, you do not have to interrupt the Kaspersky Security Center Setup Wizard. Install SQL Server and resume installation of Kaspersky Security Center.

Step 8. Selecting an authentication mode

Determine the authentication mode that will be used when Administration Server connects to the SQL Server.

Depending on the database that is selected, you can choose from the following authentication modes.

- For SQL Express or Microsoft SQL Server select one of the following options:
 - **Microsoft Windows Authentication mode.** Verification of rights uses the account used for starting Administration Server.
 - **SQL Server Authentication mode.** If you select this option, the account specified in the window is used to verify access rights. Fill in the **Account** and **Password** fields.

To see the entered password, click and hold the **Show** button.

For both authentication modes, the application checks if the database is available. If the database is not available, an error message is displayed, and you have to provide correct credentials.

If the Administration Server database is stored on another device and the Administration Server account does not have access to the database server, you must use SQL Server authentication mode when installing or upgrading Administration Server. This may occur when the device that stores the database is outside the domain or when Administration Server is installed under a LocalSystem account.

- For the MySQL server or MariaDB server, specify the account and password.

Step 9. Selecting the account to start Administration Server

Select the account that will be used to start Administration Server as a service.

- **Generate the account automatically.** The application creates an account named KL-AK-*, under which the kladminserver service will run.

You can select this option if you plan to locate the shared folder (see section "Step 11. Selecting a shared folder" on page [240](#)) and the DBMS (see section "Step 6. Selecting a database" on page [236](#)) on the same device as Administration Server.

- **Select an account.** The Administration Server service (kladminserver) will run under the account that you selected.

You will have to select a domain account if, for example, you plan to use as the DBMS a SQL Server instance of any version, including SQL Express (see section "Step 6. Selecting a database" on page [236](#)), that is located on another device, and/or you plan to locate the shared folder (see section "Step 11. Selecting a shared folder" on page [240](#)) on another device.

Starting from version 10 Service Pack 3, Kaspersky Security Center supports managed service accounts (MSA) and group managed service accounts (gMSA). If these types of accounts are used in your domain, you can select one of them as the account for the Administration Server service.

Before specifying MSA or gMSA, you must install the account on the same device on which you want to install Administration Server. If the account is not installed yet, then cancel the Administration Server installation, install the account, and then restart the Administration Server installation. For details about installation of managed service accounts on a local device, refer to the official Microsoft documentation <https://docs.microsoft.com/en-us/powershell/module/addsadministration/install-adserviceaccount?view=win10-ps>.

To specify MSA or gMSA:

1. Click the **Browse** button.
2. In the window that opens, click the **Object type** button.
3. Select the **Account for services** type and click **OK**.
4. Select the relevant account and click **OK**.

The account that you selected must have different permissions, depending on the DBMS that you plan for use (see section "Accounts for work with the DBMS" on page [215](#)).

For security reasons, please do not assign the privileged status to the account under which you run Administration Server.

If later you decide to change the Administration Server account, you can use the utility for Administration Server account switching (klsrvswch) (see section "Changing an Administration Server service account. Utility tool klsrvswch" on page [606](#)).

See also:

Accounts for work with the DBMS	215
Changes in the system after Administration Server installation on the device.....	259

Step 10. Selecting the account for running the Kaspersky Security Center services

Select the account under which the services of Kaspersky Security Center will run on this device:

- **Generate the account automatically.** Kaspersky Security Center creates a local account named KIScSvc on this device in the kladmins group. The services of Kaspersky Security Center will be run under the account that has been created.
- **Select an account.** The Kaspersky Security Center services will be run under the account that you selected.

You will have to select a domain account if, for example, you intend to save reports to a folder located on a different device or if this is required by your organization's security policy. You may also have to select a domain account if you install Administration Server on a failover cluster (see section "Creating accounts for the Administration Server services on a failover cluster" on page [224](#)).

For security reasons, do not grant privileged status to the account under which the services are run.

The KSN proxy server service (ksnproxy), Kaspersky activation proxy server service (klactprx), and Kaspersky authentication portal service (klwebsrv) will be run under the selected account.

See also:

Changes in the system after Administration Server installation on the device.....[259](#)

Step 11. Selecting a shared folder

Define the location and name of the shared folder that will be used to do the following:

- Store the files necessary for remote installation of applications (these files are copied to Administration Server during creation of installation packages).
- Store updates that have been downloaded from an update source to Administration Server.

File sharing (read-only) will be enabled for all users.

You can select either of the following options:

- **Create a shared folder.** Create a new folder. In the text box, specify the path to the folder.
- **Select an existing shared folder.** Select a shared folder that already exists.

The shared folder can be a local folder on the device that is used for installation or a remote directory on any client device on the corporate network. You can click the **Browse** button to select the shared folder, or specify the shared folder manually by entering its UNC path (for example, \\server\Share) in the corresponding field.

By default, the installer creates a local Share subfolder in the application folder that contains the components of Kaspersky Security Center.

Step 12. Configuring the connection to Administration Server

Configure the connection to Administration Server:

- **Port**
The number of the port used to connect to the Administration Server.
The default port number is 14000.
- **SSL port**
Secure Sockets Layer (SSL) port number used to securely connect to the Administration Server via SSL.
The default port number is 13000.
- **Encryption key length**

Select the length of the encryption key: 1024 bit or 2048 bit.

A 1024-bit encryption key places a smaller load on the CPU, but it is considered obsolete because it cannot provide reliable encryption due to its technical specifications. Also, the existing hardware probably will turn out to be incompatible with SSL certificates featuring 1024-bit keys.

A 2048-bit encryption key meets all state-of-the-art encryption standards. However, use of a 2048-bit encryption key may add to the load on a CPU.

By default, **2048 bit (best security)** is selected.

If Administration Server is installed on a device running Microsoft Windows XP Service Pack 2, the built-in system Firewall blocks TCP ports 13000 and 14000. Therefore, to allow access to Administration Server on the device after installation, these ports must be opened manually.

See also:

Ports used by Kaspersky Security Center	65
Interaction of Kaspersky Security Center components and security applications: more information.....	108

Step 13. Defining the Administration Server address

Specify the Administration Server address. You can select one of the following options:

- **DNS domain name.** This method is helpful in cases when the network includes a DNS server and client devices can use it to receive the Administration Server address.

- **NetBIOS name.** This method is used if client devices receive the Administration Server address using the NetBIOS protocol or if a WINS server is available on the network.
- **IP address.** This option is used if Administration Server has a static IP address that will not be subsequently changed.

Step 14. Administration Server address for connection of mobile devices

This Setup Wizard step is available if you have selected Mobile Device Management for installation.

Specify the external address of the Administration Server for connection of mobile devices that are outside of the local network.

Step 15. Selecting application management plug-ins

Select the application management plug-ins that need to be installed with Kaspersky Security Center.

For ease of search, plug-ins are divided into groups depending on the type of secured objects.

Step 16. Unpacking and installing files on the hard drive

After the installation of Kaspersky Security Center components is configured, you can start installing files on the hard drive.

If installation requires additional programs, the Setup Wizard will notify you, on the **Installing Prerequisites** page, before installation of Kaspersky Security Center begins. The required programs are installed automatically after you click the **Next** button.

On the last page, you can select which console to start for work with Kaspersky Security Center:

- **Start MMC-based Administration Console**
- **Start Kaspersky Security Center Web Console**

This option is available only if you opted to install Kaspersky Security Center 13 Web Console in one of the previous steps.

You can also click **Finish** to close the Wizard without starting work with Kaspersky Security Center. You can start the work later at any time.

At the first startup of Administration Console or Kaspersky Security Center 13 Web Console, you can perform the initial setup of the application (on page [265](#)).

Installing Administration Server on a failover cluster

The procedure of installing Administration Server on a failover cluster differs from both standard and custom installation on a stand-alone device.

Perform the procedure described in this section on the node that contains a common data storage of the cluster.

► *To install Kaspersky Security Center Administration Server on a cluster:*

Run the `ksc_13.<build number>_full_<localization language>.exe` executable file.

A window opens prompting you to select Kaspersky applications to install. In the application selection window, click the **Install Kaspersky Security Center 13 Administration Server** link to start the Administration Server Setup Wizard. Follow the instructions of the Wizard.

Below are the steps of the Setup Wizard and actions that you can perform at each step.

In this section

Step 1. Reviewing the License Agreement and Privacy Policy	243
Step 2. Selecting the type of installation on a cluster	244
Step 3. Specifying the name of the virtual Administration Server	244
Step 4. Specifying the network details of the virtual Administration Server	244
Step 5. Specifying a cluster group	245
Step 6. Selecting a cluster data storage	245
Step 7. Specifying an account for remote installation	245
Step 8. Selecting the components to be installed	245
Step 9. Selecting network size	246
Step 10. Selecting a database	247
Step 11. Configuring the SQL Server	248
Step 12. Selecting an authentication mode	249
Step 13. Selecting the account to start Administration Server	249
Step 14. Selecting the account for running the Kaspersky Security Center services	250
Step 15. Selecting a shared folder	251
Step 16. Configuring the connection to Administration Server	251
Step 17. Defining the Administration Server address	252
Step 18. Administration Server address for connection of mobile devices	252
Step 19. Unpacking and installing files on the hard drive	252

Step 1. Reviewing the License Agreement and Privacy Policy

At this step of the Setup Wizard, you must read the License Agreement, which is to be concluded between you and Kaspersky, as well as the Privacy Policy.

You may also be prompted to view the License Agreements and Privacy Policies for application management plugins that are available in the Kaspersky Security Center distribution kit.

Please carefully read the License Agreement and Privacy Policy. If you agree with all the terms of the License Agreement and the Privacy Policy, select the following check boxes in the **I confirm I have fully read, understood, and accept the following** section:

- **The terms and conditions of this EULA**
- **Privacy Policy describing the handling of data**

Installation of the application on your device will continue after you select both check boxes.

If you do not accept the License Agreement or the Privacy Policy, cancel installation by clicking the **Cancel** button.

Step 2. Selecting the type of installation on a cluster

Select the type of installation on the cluster:

- **Cluster (install on all cluster nodes)**

This is the recommended option. If you select this option, Administration Server will be installed on all nodes of the cluster simultaneously.

- **Locally (install on this device only)**

If you select this option, Administration Server will be installed only on the current node, as if on a stand-alone server, and Administration Server will not work as a cluster-aware application. For example, you may want to choose this option to save shared storage space, if fault tolerance is not needed for Administration Server. In case of the current node failure, you will have to install Administration Server on another node and restore the Administration Server state from a backup.

Further steps are the same as when you use the standard (see section "Standard installation" on page [226](#)) or custom (see section "Custom installation" on page [232](#)) installation method, starting from the installation method selection step.

Step 3. Specifying the name of the virtual Administration Server

Specify the network name of the new virtual Administration Server. You will be able to use this name to connect Administration Console or Kaspersky Security Center 13 Web Console to Administration Server.

The name that you specify must differ from the cluster name.

Step 4. Specifying the network details of the virtual Administration Server

► *To specify the network details of the new virtual Administration Server instance:*

1. In **Network to use**, select the domain network to which the current cluster node is connected.
2. Do either of the following:
 - If DHCP is used in the selected network to assign IP addresses, select the **Use DHCP** check box.
 - If DHCP is not used in the selected network, specify the required IP address.

The IP address that you specify must differ from the cluster IP address.

3. Click **Add** to apply the specified settings.

You will be able to use the automatically assigned or the specified IP address to connect Administration Console or Kaspersky Security Center Web Console to Administration Server.

Step 5. Specifying a cluster group

A cluster group is a special failover cluster role that contains common resources for all nodes. You have two options:

- **Creating a new cluster group.**
This option is recommended in most cases. The new cluster group will contain all common resources that relate to the Administration Server instance.
- **Selecting an existing cluster group.**
Select this option if you want to use a common resource that is already associated with an existing cluster group. For example, you may want to use this option if you want to use a storage associated with an existing cluster group and if there are no other available storage for a new cluster group.

Step 6. Selecting a cluster data storage

► *To select a cluster data storage:*

1. In **Available repositories**, select the data storage to which the common resources of the virtual Administration Server instance will be installed.
2. If the selected data storage contains several volumes, under **Available sections on disk drive**, select the required volume.
3. In **Installation path**, enter the path on the common data storage to which the resources of the virtual Administration Server instance will be installed.

The data storage is selected.

Step 7. Specifying an account for remote installation

Specify the user name and password that will be used for remote installation of the virtual Administration Server instance on a passive node of the cluster.

The account that you specify must be granted administrative privileges on all nodes of the cluster.

Step 8. Selecting the components to be installed

Select the components of Kaspersky Security Center Administration Server that you want to install:

- **Mobile Device Management.** Select this check box if you must create installation packages for mobile devices when the Kaspersky Security Center Setup Wizard is running. You can also create installation packages for mobile devices manually, after Administration Server installation, by using Administration Console tools (see section "Creating installation packages of applications" on page [717](#)).

- **SNMP agent.** This component receives statistical information for the Administration Server over the SNMP protocol. The component is available if the application is installed on a device with SNMP installed.

After Kaspersky Security Center is installed, the .mib files required for receiving statistics are located in the SNMP subfolder of the application installation folder.

Network Agent and Administration Console are not displayed in the component list. These components are installed automatically and you cannot cancel their installation.

At this step you must specify a folder for installation of Administration Server components. By default, the components are installed to <Disk>:\Program Files\Kaspersky Lab\Kaspersky Security Center. If no such folder exists, this folder is created automatically during installation. You can change the destination folder by using the **Browse** button.

Step 9. Selecting network size

Specify the size of the network on which Kaspersky Security Center is to be installed. Depending on the number of devices on the network, the Wizard configures the installation and appearance of the application interface so that they match.

The following table lists the application installation settings and interface appearance settings, which are adjusted based on various network sizes.

Table 41. Dependence of installation settings on the network scale selected

Settings	1—100 devices	100—1000 devices	1000—5000 devices	More than 5000 devices
Display with the node for secondary and virtual Administration Servers, and all settings related to the secondary and virtual Administration Servers in the console tree	not available	not available	available	available
Display with the Security sections in the properties windows of the Administration Server and administration groups	not available	not available	available	available
Random distribution of startup time for the update task on client devices	not available	Over an interval of 5 minutes	Over an interval of 10 minutes	Over an interval of 10 minutes

If you connect Administration Server to a MySQL or SQL Express database server, it is not recommended to use the application to manage more than 10 000 devices. For the MariaDB database management system, the maximum recommended number of managed devices is 20 000.

Step 10. Selecting a database

At this step of the Wizard, you must select the mechanism—Microsoft SQL Server (SQL Express) or MySQL—that will be used to store the Administration Server database. The MySQL option is relevant to both MySQL and MariaDB.

It is recommended to install the Administration Server on a dedicated server instead of a domain controller. However, if you install Kaspersky Security Center on a server that acts as a read-only domain controller (RODC), Microsoft SQL Server (SQL Express) must not be installed locally (on the same device). In this case, we recommend that you install Microsoft SQL Server (SQL Express) remotely (on a different device), or that you use MySQL or MariaDB, if you need to install the DBMS locally.

The Administration Server database structure is provided in the `klakdb.chm` file, which is located in the Kaspersky Security Center installation folder (this file is also available in an archive on the Kaspersky portal: `klakdb.zip`) (<https://media.kaspersky.com/utilities/CorporateUtilities/klakdb.zip>).

Step 11. Configuring the SQL Server

At this step of the Wizard, you configure SQL Server.

Depending on the database that you have selected, specify the following settings:

- If you selected **Microsoft SQL Server (SQL Server Express)** in the previous step:
 - In the **SQL Server instance name** field, specify the name of the SQL Server on the network. To view a list of all SQL Servers that are on the network, click the **Browse** button. This field is blank by default.

If you connect to the SQL Server through a custom port, then together with the SQL Server host name specify the port number separated with a comma, for example:

```
SQL_Server_host_name,1433
```

If you secure communication between the Administration Server and SQL Server by means of a certificate (see section "Scenario: Authenticating Microsoft SQL Server" on page [222](#)), specify in the **SQL Server instance name** field the same host name that was used at the certificate generating. If you use a named instance of SQL Server, then together with the SQL Server host name specify the port number separated with a comma, for example:

```
SQL_Server_name,1433
```

If you use several instances of SQL Server on the same host, then additionally specify the instance name separated with a backslash, for example:

```
SQL_Server_name\SQL_Server_instance_name,1433
```

If a SQL Server that has AlwaysON support enabled is on the enterprise network, in the **SQL Server instance name** field specify the name of the availability group listener.

- In the **Database name** field, specify the name of the database that has been created to store Administration Server data. The default value is `KAV`.
- If you selected **MySQL** in the previous step:
 - In the **SQL Server instance name** field, specify the name of the SQL Server instance. By default, the name is the IP address of the device on which Kaspersky Security Center is to be installed.
 - In the **Port** field, specify the port for Administration Server connection to the SQL Server database. The default port number is 3306.

- In the **Database name** field, specify the name of the database that has been created to store Administration Server data. The default value is *KAV*.

If at this stage you want to install SQL Server on the device from which you are installing Kaspersky Security Center, you must stop installation and restart it after SQL Server is installed. The supported SQL Server versions are listed in the system requirements.

If you want to install SQL Server on a remote device, you do not have to interrupt the Kaspersky Security Center Setup Wizard. Install SQL Server and resume installation of Kaspersky Security Center.

Step 12. Selecting an authentication mode

Determine the authentication mode that will be used when Administration Server connects to the SQL Server.

Depending on the database that is selected, you can choose from the following authentication modes.

- For SQL Express or Microsoft SQL Server select one of the following options:
 - **Microsoft Windows Authentication mode.** Verification of rights uses the account used for starting Administration Server.
 - **SQL Server Authentication mode.** If you select this option, the account specified in the window is used to verify access rights. Fill in the **Account** and **Password** fields.

To see the entered password, click and hold the **Show** button.

For both authentication modes, the application checks if the database is available. If the database is not available, an error message is displayed, and you have to provide correct credentials.

If the Administration Server database is stored on another device and the Administration Server account does not have access to the database server, you must use SQL Server authentication mode when installing or upgrading Administration Server. This may occur when the device that stores the database is outside the domain or when Administration Server is installed under a LocalSystem account.

- For the MySQL server or MariaDB server, specify the account and password.

Step 13. Selecting the account to start Administration Server

Select the account that will be used to start Administration Server as a service.

- **Generate the account automatically.** The application creates an account named KL-AK-*, under which the kladminserver service will run.

You can select this option if you plan to locate the shared folder (see section "Step 11. Selecting a shared folder" on page [240](#)) and the DBMS (see section "Step 6. Selecting a database" on page [236](#)) on the same device as Administration Server.

- **Select an account.** The Administration Server service (kladminsrv) will run under the account that you selected.

You will have to select a domain account if, for example, you plan to use as the DBMS a SQL Server instance of any version, including SQL Express (see section "Step 6. Selecting a database" on page [236](#)), that is located on another device, and/or you plan to locate the shared folder (see section "Step 11. Selecting a shared folder" on page [240](#)) on another device.

Starting from version 10 Service Pack 3, Kaspersky Security Center supports managed service accounts (MSA) and group managed service accounts (gMSA). If these types of accounts are used in your domain, you can select one of them as the account for the Administration Server service.

Before specifying MSA or gMSA, you must install the account on the same device on which you want to install Administration Server. If the account is not installed yet, then cancel the Administration Server installation, install the account, and then restart the Administration Server installation. For details about installation of managed service accounts on a local device, refer to the official Microsoft documentation <https://docs.microsoft.com/en-us/powershell/module/addsadministration/install-adserviceaccount?view=win10-ps>.

To specify MSA or gMSA:

1. Click the **Browse** button.
2. In the window that opens, click the **Object type** button.
3. Select the **Account for services** type and click **OK**.
4. Select the relevant account and click **OK**.

The account that you selected must have different permissions, depending on the DBMS that you plan for use (see section "Accounts for work with the DBMS" on page [215](#)).

For security reasons, please do not assign the privileged status to the account under which you run Administration Server.

If later you decide to change the Administration Server account, you can use the utility for Administration Server account switching (klsrvswch) (see section "Changing an Administration Server service account. Utility tool klsrvswch" on page [606](#)).

Step 14. Selecting the account for running the Kaspersky Security Center services

Select the account under which the services of Kaspersky Security Center will run on this device:

- **Generate the account automatically.** Kaspersky Security Center creates a local account named KIScSvc on this device in the kladmins group. The services of Kaspersky Security Center will be run under the account that has been created.
- **Select an account.** The Kaspersky Security Center services will be run under the account that you selected.

You will have to select a domain account if, for example, you intend to save reports to a folder located on a different device or if this is required by your organization's security policy. You may also have to select a

domain account if you install Administration Server on a failover cluster (see section "Creating accounts for the Administration Server services on a failover cluster" on page [224](#)).

For security reasons, do not grant privileged status to the account under which the services are run.

The KSN proxy server service (ksnproxy), Kaspersky activation proxy server service (klactprx), and Kaspersky authentication portal service (klwebsrv) will be run under the selected account.

Step 15. Selecting a shared folder

Define the location and name of the shared folder that will be used to do the following:

- Store the files necessary for remote installation of applications (these files are copied to Administration Server during creation of installation packages).
- Store updates that have been downloaded from an update source to Administration Server.

File sharing (read-only) will be enabled for all users.

You can select either of the following options:

- **Create a shared folder.** Create a new folder. In the text box, specify the path to the folder.
- **Select an existing shared folder.** Select a shared folder that already exists.

The shared folder can be a local folder on the device that is used for installation or a remote directory on any client device on the corporate network. You can click the **Browse** button to select the shared folder, or specify the shared folder manually by entering its UNC path (for example, \\server\Share) in the corresponding field.

By default, the installer creates a local Share subfolder in the application folder that contains the components of Kaspersky Security Center.

Step 16. Configuring the connection to Administration Server

Configure the connection to Administration Server:

- **Port**

The number of the port used to connect to the Administration Server.
The default port number is 14000.
- **SSL port**

Secure Sockets Layer (SSL) port number used to securely connect to the Administration Server via SSL.
The default port number is 13000.
- **Encryption key length**

Select the length of the encryption key: 1024 bit or 2048 bit.

A 1024-bit encryption key places a smaller load on the CPU, but it is considered obsolete because it cannot provide reliable encryption due to its technical specifications. Also, the existing hardware probably will turn out to be incompatible with SSL certificates featuring 1024-bit keys.

A 2048-bit encryption key meets all state-of-the-art encryption standards. However, use of a 2048-bit encryption key may add to the load on a CPU.

By default, **2048 bit (best security)** is selected.

If Administration Server is installed on a device running Microsoft Windows XP Service Pack 2, the built-in system Firewall blocks TCP ports 13000 and 14000. Therefore, to allow access to Administration Server on the device after installation, these ports must be opened manually.

Step 17. Defining the Administration Server address

Specify the Administration Server address. You can select one of the following options:

- **DNS domain name.** This method is helpful in cases when the network includes a DNS server and client devices can use it to receive the Administration Server address.
- **NetBIOS name.** This method is used if client devices receive the Administration Server address using the NetBIOS protocol or if a WINS server is available on the network.
- **IP address.** This option is used if Administration Server has a static IP address that will not be subsequently changed.

Step 18. Administration Server address for connection of mobile devices

This Setup Wizard step is available if you have selected Mobile Device Management for installation.

Specify the external address of the Administration Server for connection of mobile devices that are outside of the local network.

Step 19. Unpacking and installing files on the hard drive

After the installation of Kaspersky Security Center components is configured, you can start installing files on the hard drive.

If installation requires additional programs, the Setup Wizard will notify you, on the **Installing Prerequisites** page, before installation of Kaspersky Security Center begins. The required programs are installed automatically after you click the **Next** button.

On the last page, you can select which console to start for work with Kaspersky Security Center:

- **Start MMC-based Administration Console**
- **Start Kaspersky Security Center Web Console**

This option is available only if you opted to install Kaspersky Security Center 13 Web Console in one of the previous steps.

You can also click **Finish** to close the Wizard without starting work with Kaspersky Security Center. You can start the work later at any time.

At the first startup of Administration Console or Kaspersky Security Center 13 Web Console, you can perform the initial setup of the application (on page [265](#)).

Installing Administration Server in non-interactive mode

Administration Server can be installed in non-interactive mode, that is, without the interactive input of installation settings.

► *To install Administration Server on a local device in non-interactive mode:*

1. Read the End User License Agreement (see section "About the End User License Agreement" on page [318](#)). Use the command below only if you understand and accept the terms of the End User License Agreement.
2. Read the Privacy Policy (see section "Viewing the Privacy Policy" on page [187](#)). Use the command below only if you understand and agree that your data will be handled and transmitted (including to third countries) as described in the Privacy Policy.
3. Run the command

```
setup.exe /s /v"DONT_USE_ANSWER_FILE=1 EULA=1 PRIVACYPOLICY=1  
<setup_parameters>"
```

where `setup_parameters` is a list of parameters and their respective values, separated with spaces (`PARAM1=PARAM1VAL PARAM2=PARAM2VAL`). The `setup.exe` file is located in the `Server` folder, which is part of the Kaspersky Security Center distribution kit.

The names and possible values for parameters that can be used when installing Administration Server in non-interactive mode are listed in the table below.

Table 42. Parameters of Administration Server installation in non-interactive mode

Parameter name	Parameter description	Available values
EULA	Acceptance of the terms of the License Agreement.	<ul style="list-style-type: none"> • 1—I have fully read, understand and accept the terms of the End User License Agreement. • Other value or no value—I do not accept the terms of the License Agreement (installation is not performed).
PRIVACYPOLICY	Acceptance of the terms of the Privacy Policy.	<ul style="list-style-type: none"> • 1—I am aware and agree that my data will be handled and transmitted (including to third countries) as described in the Privacy Policy. I confirm that I have fully read and understand the Privacy Policy. • Other value or no value—I do not accept the terms of the Privacy Policy (installation is not performed).
INSTALLATIONMODETYPE	Type of Administration Server installation.	<ul style="list-style-type: none"> • Standard—Standard installation. • Custom—Custom installation.
INSTALLDIR	Path to the Administration Server installation folder.	String value.
ADDLOCAL	List of Administration Server components (separated with commas) to be installed.	<p>CSAdminKitServer, NAgent, CSAdminKitConsole, NSAC, MobileSupport, KSNProxy, SNMPAgent, GdiPlusRedist, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86.</p> <p>Minimum list of components sufficient for proper Administration Server installation:</p> <pre>ADDLOCAL=CSAdminKitServer, CSAdminKitConsole, KSNProxy, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86.</pre>
NETRANGETYPE	Network size (number of devices on the network).	<ul style="list-style-type: none"> • NRT_1_100—From 1 to 100 devices. • NRT_100_1000—From 101 to 1,000 devices. • NRT_GREATER_1000—More than 1,000 devices.
SRV_ACCOUNT_TYPE	Mode for specifying the account under which Administration Server will be run as a service.	<ul style="list-style-type: none"> • SrvAccountDefault —The account is created automatically. • SrvAccountUser —The account is specified manually. In this case, you must specify values for the SERVERACCOUNTNAME and SERVERACCOUNTPWD parameters.

Parameter name	Parameter description	Available values
SERVERACCOUNTNAME	Name of the account under which Administration Server will be run as a service. You must specify a value for the parameter if SRV_ACCOUNT_TYPE=SrvAccountUser.	String value.
SERVERACCOUNTPWD	Password of the account that will be used to start Administration Server as a service. You must specify a value for the parameter if SRV_ACCOUNT_TYPE=SrvAccountUser.	String value.
SERVERCER	Size of the key for the Administration Server certificate (bits).	<ul style="list-style-type: none"> • 1—The size of the key for the Administration Server certificate is 2,048 bits. • No value —The size of the key for the Administration Server certificate is 1,024 bits.
DBTYPE	Type of database that will be used to store the Administration Server database. This parameter is mandatory.	<ul style="list-style-type: none"> • MySQL—A MySQL or MariaDB database will be used; in this case, you must specify values for the MYSQLSERVERNAME, MYSQLSERVERPORT, MYSQLDBNAME, MYSQLACCOUNTNAME, and MYSQLACCOUNTPWD parameters. • MSSQL —A Microsoft SQL Server (SQL Express) database will be used. In this case, you must specify values for the MSSQLSERVERNAME, MSSQLDBNAME, and MSSQLAUTHTYPE parameters.
MYSQLSERVERNAME	Full name of the SQL Server. You must specify a value for the parameter if DBTYPE=MySQL.	String value.
MYSQLSERVERPORT	Number of the port for connecting to the SQL Server. You must specify a value for the parameter if DBTYPE=MySQL.	Numerical value.
MYSQLDBNAME	Name of the database that will be created to store Administration Server data. You must specify a value for the parameter if DBTYPE=MySQL.	String value.

Parameter name	Parameter description	Available values
MYSQLACCOUNTNAME	Name of the account for connection to the database. You must specify a value for the parameter if DBTYPE=MySQL.	String value.
MYSQLACCTPWDPWD	Password of the account for connecting to the database. You must specify a value for the parameter if DBTYPE=MySQL.	String value.
MSSQLSERVERNAME	Full name of the SQL Server. You must specify a value for the parameter if DBTYPE=MSSQL.	String value.
MSSQLDBNAME	Name of the database. You must specify a value for the parameter if DBTYPE=MSSQL.	String value.
MSSQLAUTHTYPE	Type of authorization when connecting to the SQL Server. You must specify a value for the parameter if DBTYPE=MSSQL	<ul style="list-style-type: none"> • Windows—Microsoft Windows Authentication mode. • SQLServer—SQL Server Authentication mode. In this case, you must specify values for the MSSQLACCOUNTNAME and MSSQLACCTPWDPWD parameters.
MSSQLACCOUNTNAME	Name of the account for connection to the SQL Server. You must specify a value for the parameter if MSSQLAUTHTYPE=SQLServer.	String value.
MSSQLACCTPWDPWD	Password of the account for connection to the SQL Server. You must specify a value for the parameter if MSSQLAUTHTYPE=SQLServer.	String value.
CREATE_SHARE_TYPE	Method of specifying the shared folder.	<ul style="list-style-type: none"> • Create—Create a new shared folder. In this case, you must specify values for the SHARELOCALPATH and SHAREFOLDERNAME parameters. • ChooseExisting—Select an existing folder. In this case, you must specify a value for the EXISTSHAREFOLDERNAME parameter.

Parameter name	Parameter description	Available values
SHARELOCALPATH	Full path to a local folder. You must specify a value for the parameter if CREATE_SHARE_TYPE=Create	String value.
SHAREFOLDERNAME	Network name of a shared folder. You must specify a value for the parameter if CREATE_SHARE_TYPE=Create.	String value.
EXISTSHAREFOLDERNAME	Full path to an existing shared folder. You must specify a value for the parameter if CREATE_SHARE_TYPE=ChooseExisting.	String value.
SERVERPORT	Port number to connect to Administration Server.	Numerical value.
SERVERSSLPORT	Number of the port for encrypted connection to Administration Server by using SSL protocol.	Numerical value.
SERVERADDRESS	Administration Server address.	String value.
MOBILESERVERADDRESS	Administration Server address for connection of mobile devices.	String value.

For a detailed description of the Administration Server setup parameters, please refer to the Custom installation (on page [232](#)) section.

Installing Administration Console on the administrator's workstation

You can install Administration Console on the administrator's workstation separately and manage Administration Server over the network using that Console.

► *To install Administration Console on the administrator's workstation:*

1. Run the setup.exe executable file.
A window opens prompting you to select Kaspersky applications to install.
2. In the application selection window, click the **Install only Kaspersky Security Center 13 Administration Console** link to run the Administration Console Setup Wizard. Follow the instructions of the Wizard.

3. Select a destination folder. By default, this will be <Disk>:\Program Files\Kaspersky Lab\Kaspersky Security Center Console. If such a folder does not exist, it is created automatically during the installation. You can change the destination folder by using the **Browse** button.
4. On the last page of the Setup Wizard click the **Start** button to start installation of Administration Console. When the Wizard completes, Administration Console will be installed on the administrator's workstation.

► *To install Administration Console on the administrator's workstation in non-interactive mode:*

1. Read the End User License Agreement (see section "About the End User License Agreement" on page [318](#)). Use the command below only if you understand and accept the terms of the End User License Agreement.
2. In the `Distrib\Console` folder of the Kaspersky Security Center distribution kit, run the `setup.exe` file by using the following command:

```
setup.exe /s /v"EULA=1"
```

If you want to install all management plug-ins from the `Distrib\Console\Plugins` folder together with the Administration Console, run the following command:

```
setup.exe /s /v"EULA=1" /pALL
```

If you want to specify which management plug-ins to install from the `Distrib\Console\Plugins` folder together with the Administration Console, specify the plug-ins after the `/p` key and separate them with a semicolon:

```
setup.exe /s /v"EULA=1" /pP1;P2;P3
```

where `P1`, `P2`, `P3` are plug-in names that correspond to the plug-in folder names in the `Distrib\Console\Plugins` folder. For example:

```
setup.exe /s /v"EULA=1" /pKES4Mac;KESS;MDM4IOS
```

Administration Console and the management plug-ins (if any) will be installed on the administrator's workstation.

After installing Administration Console, you must connect to the Administration Server. To do this, run Administration Console and, in the window that opens, specify the name or the IP address of the device on which Administration Server is installed, as well as the settings of the account used to connect to it. After connection to Administration Server is established, you can manage the anti-virus protection system using this Administration Console.

You can remove Administration Console with standard Microsoft Windows add / remove tools.

Changes in the system after Administration Server installation on the device

Administration Console icon

After Administration Console is installed on your device, its icon appears, allowing you to start Administration Console. You can find Administration Console in the **Start** → **Programs** → **Kaspersky Security Center** menu.

Administration Server and Network Agent services

Administration Server and Network Agent are installed on the device as services with the properties listed below. The table also contains the attributes of other services that apply on the device after Administration Server installation.

Table 43. Properties of Kaspersky Security Center services

Component	Service name	Displayed service name	Account
Administration Server	kladminsrv	Kaspersky Security Center Administration Server	User-defined or dedicated non-privileged account in KL-AK-* format created during installation
Network Agent	klagent	Kaspersky Security Center Network Agent	Local system
Web Server for accessing Kaspersky Security Center 13 Web Console and administering the organization's intranet	klwebsrv	Kaspersky web server	Dedicated unprivileged KIScSvc account
Activation proxy server	klactprx	Kaspersky activation proxy server	Dedicated unprivileged KIScSvc account
KSN proxy server	ksnproxy	Kaspersky Security Network proxy server	Dedicated unprivileged KIScSvc account

Network Agent server version

The server version of Network Agent will be installed on the device together with Administration Server. The server version of Network Agent is part of Administration Server, is installed and removed together with Administration Server, and can only interact with a locally installed Administration Server. You do not have to configure the connection of Network Agent to Administration Server: configuration is implemented programmatically because the components are installed on the same device. The server version of Network Agent is installed with the same properties as the standard Network Agent and performs the same application management functions. This version will be managed by the policy of the administration group to which the client device of Administration Server belongs. For the server version of Network Agent all tasks are created from the scope of those provided for Administration Server, except for the Server change task.

Network Agent cannot be installed separately on a device that already has Administration Server installed.

You can view the properties of each service of Administration Server and Network Agent, as well as monitor their operation using standard Microsoft Windows management tools: Computer management\Services. Information about the activity of the Kaspersky Administration Server service is stored in the Microsoft Windows system log in a separate Kaspersky Event Log branch on the device where the Administration Server is installed.

We recommend that you avoid starting and stopping services manually and leave service accounts in the service settings unchanged. If necessary, you can modify the Administration Server service account using the `klsvswch` utility.

User accounts and user groups

The Administration Server Installer creates the following accounts by default:

- KL-AK-*: Administration Server service account
- KIScSvc: Account for other services from the Administration Server pool
- KIPxeUser: Account for deployment of operating systems

If you selected other accounts for the Administration Server service and other services while running the Installer, the specified accounts are used.

Local security groups named KLAdmins and KLOperators are also created automatically on the device that has Administration Server installed.

It is not recommended to install the Administration Server on a domain controller; however, if you install Administration Server on the domain controller, you must start the installer with the domain administrator rights. In this case, the installer automatically creates domain security groups named KLAdmins and KLOperators. If you install Administration Server on a computer that is not the domain controller, you must start the installer with the local administrator rights instead. In this case, the installer automatically creates local security groups named KLAdmins and KLOperators.

When configuring email notifications, the administrator may have to create an account on the mail server for ESMTP authentication.

See also:

Accounts for work with the DBMS[215](#)

Removing the application

You can remove Kaspersky Security Center with standard Microsoft Windows add/remove tools. Removing the application requires starting a wizard that removes all application components from the device (including plug-ins). If you have not selected removal of the shared folder (Share) during the wizard operation, you can delete it manually after completion of all related tasks.

After the application is removed, some of its files may remain in the system's temporary folder.

The Application Removal Wizard will suggest that you store a backup copy of Administration Server.

When the application is removed from Microsoft Windows 7 and Microsoft Windows 2008, premature termination of the Removal Wizard might occur. This can be avoided by disabling the User Account Control (UAC) in the operating system and restarting application removal.

Upgrading Kaspersky Security Center from a previous version

You can install version 13 of Administration Server on a device that has an earlier version of Administration Server installed (starting from version 10 Service Pack 1). When upgrading to version 13, all data and settings from the previous version of Administration Server are preserved.

Concurrent use of the DBMS by Administration Server and another application is strictly forbidden.

► *To upgrade an earlier version of Administration Server to version 13:*

1. Run the setup.exe executable file for version 13.

A window opens prompting you to select Kaspersky applications to install.

In the application selection window, click the **Install Kaspersky Security Center 13 Administration Server** link to start the Administration Server Setup Wizard. Follow the instructions of the Wizard.

Please carefully read the License Agreement and Privacy Policy. If you agree with all the terms of the License Agreement and the Privacy Policy, select the following check boxes in the **I confirm I have fully read, understood, and accept the following** section:

- **The terms and conditions of this EULA**
- **Privacy Policy describing the handling of data**

Installation of the application on your device will continue after you select both check boxes. The Setup Wizard prompts you to create a backup copy of the Administration Server data for the earlier version.

Kaspersky Security Center supports data recovery from a backup copy of Administration Server created with an older version of the application.

2. If you have to create a backup copy, in the **Administration Server Backup** window that opens, select the **Create backup copy of Administration Server** check box.

A backup copy of Administration Server data is created by the klbackup utility. This utility is included in the distribution kit, and is located at the root of the Kaspersky Security Center installation folder (see section "Backup copying and restoration of Administration Server data" on page [617](#)).

3. Install Administration Server version 13, following the Setup Wizard.

We recommend that you avoid terminating the Setup Wizard. Canceling the upgrade at the step of Administration Server installation may cause the upgraded version of Kaspersky Security Center to fail.

4. For devices on which the earlier version of Network Agent was installed, create and run the task for remote installation of the new version of Network Agent (see section "Installing applications using a remote installation task" on page [334](#)).

After completion of the remote installation task, the Network Agent version will be upgraded.

If problems occur during Administration Server installation, you can restore the previous version of Administration Server using the backup copy of the Administration Server data created before the upgrade.

If at least one Administration Server of the new version has been installed on the network, other Administration Servers on the network can be upgraded using the remote installation task that uses the Administration Server installation package.

When upgrading Kaspersky Security Center from a previous version, all the installed management plug-ins are not uninstalled. You can configure policies and tasks corresponding to the managed plug-ins.

Administration Server plug-in and Network Agent plug-in are upgraded automatically.

Initial setup of Kaspersky Security Center

This section describes steps you must take after the Kaspersky Security Center installation to perform its initial setup.

In this chapter

Administration Server Quick Start Wizard	265
Configuring the connection of Administration Console to Administration Server	278
Requirements to custom certificates used in Kaspersky Security Center	279
Connecting out-of-office devices	282
Encrypt communication with SSL/TLS	294
Notifications of events.....	297
Configuring the interface.....	300

Administration Server Quick Start Wizard

This section provides information about the Administration Server Quick Start Wizard.

In this section

About Quick Start Wizard	265
Starting Administration Server Quick Start Wizard.....	266
Step 1. Getting acquainted with Quick Start Wizard	266
Step 2. Configuring a proxy server	266
Step 3. Selecting the application activation method	267
Step 4. Selecting the protection scopes and platforms	268
Step 5. Selecting plug-ins for managed applications	269
Step 6. Downloading distribution packages and creating installation packages	269
Step 7. Configuring Kaspersky Security Network usage.....	270
Step 8. Configuring email notifications	271
Step 9. Configuring update management.....	271
Step 10. Connecting mobile devices	272
Step 11. Creating an initial protection configuration	277
Step 12. Downloading updates.....	277
Step 13. Device discovery	277
Step 14. Closing the Quick Start Wizard	278

About Quick Start Wizard

This section provides information about the Administration Server Quick Start Wizard.

Administration Server Quick Start Wizard allows you to create a minimum of necessary tasks and policies, adjust a minimum of settings, download and install plug-ins for managed Kaspersky applications, and create installation packages of managed Kaspersky applications. When the Wizard is running, you can make the following changes to the application:

- Download and install plug-ins for managed applications. After the Quick Start Wizard has finished, the list of installed management plug-ins is displayed in the **Advanced** → **Details of application management plug-ins installed** section of the Administration Server properties window.
- Create installation packages of managed Kaspersky applications. After the Quick Start Wizard has finished, installation packages of Network Agent for Windows and managed Kaspersky applications are displayed in the **Administration Server** → **Advanced** → **Remote installation** → **Installation packages** list.
- Add key files or enter activation codes that can be automatically distributed to devices within administration groups. After the Quick Start Wizard has finished, information about license keys is displayed in the **Administration Server** → **Kaspersky Licenses** list and in the **License keys** section of the Administration Server properties window.
- Configure interaction with Kaspersky Security Network (KSN).

- Set up email delivery of notifications of events that occur during operation of Administration Server and managed applications (successful notification delivery requires that the Messenger service run on the Administration Server and all recipient devices). After the Quick Start Wizard has finished, the email notifications settings are displayed in the **Notification** section of the Administration Server properties window.
- Adjust the update settings and vulnerability fix settings for applications installed on devices.
- Create a protection policy for workstations and servers, as well as virus scan tasks, update download tasks, and data backup tasks, for the top level of the hierarchy of managed devices. After the Quick Start Wizard has finished, the created tasks are displayed in the **Administration Server** → **Tasks** list, the policies corresponding to the plug-ins for managed applications are displayed in the **Administration Server** → **Policies** list.

The Quick Start Wizard creates policies for managed applications, such as Kaspersky Endpoint Security for Windows, unless such policies are already created for the **Managed devices** group. The Quick Start Wizard creates tasks if tasks with the same names do not exist for the **Managed devices** group.

In Administration Console, Kaspersky Security Center automatically prompts you to run the Quick Start Wizard after you have started it for the first time. You can also start the Quick Start Wizard manually at any time.

Starting Administration Server Quick Start Wizard

The application automatically prompts you to run the Quick Start Wizard after Administration Server installation, at the first connection to it. You can also start the Quick Start Wizard manually at any time.

► *To start the Quick Start Wizard manually:*

1. In the console tree, select the **Administration Server** node.
2. In the context menu of the node, select **All Tasks** → **Administration Server Quick Start Wizard**.

The Wizard prompts you to perform initial configuration of the Administration Server. Follow the instructions of the Wizard.

If you start the Quick Start Wizard again, tasks and policies created at the previous run of the Wizard cannot be created again.

Step 1. Getting acquainted with Quick Start Wizard

Read information about the actions that Quick Start Wizard performs.

Step 2. Configuring a proxy server

Specify the Internet access settings for Administration Server. You must configure Internet access to use Kaspersky Security Network and to download updates of anti-virus databases for Kaspersky Security Center and managed Kaspersky applications.

Select the **Use proxy server** check box if you want to use a proxy server when connecting to the Internet. If this check box is selected, the fields are available for entering settings. Specify the following settings for proxy server connection:

- **Address**

Address of the proxy server used for Kaspersky Security Center connection to the Internet.

- **Port number**

Number of the port through which Kaspersky Security Center proxy connection will be established.

- **Bypass proxy server for local addresses**

No proxy server will be used to connect to devices in the local network.

- **Proxy server authentication**

If this check box is selected, in the entry fields you can specify the credentials for proxy server authentication.

This entry field is available if the **Use proxy server** check box is selected.

- **User name**

User account under which connection to the proxy server is established (this field is available if the **Proxy server authentication** check box is selected).

- **Password**

Password set by the user under whose account the proxy server connection is established (this field is available if the **Proxy server authentication** check box is selected).

To see the entered password, click and hold the **Show** button for as long as you require.

Step 3. Selecting the application activation method

Select one of the following Kaspersky Security Center activation options:

- By inserting your activation code

Activation code is a unique sequence of 20 alphanumeric characters. You enter an activation code to add a key that activates Kaspersky Security Center. You receive the activation code through the email address that you specified after purchasing Kaspersky Security Center.

To activate the application with an activation code, you need Internet access to establish connection with Kaspersky activation servers.

If you have selected this activation option, you can enable the **Automatically deploy license key to managed devices** option.

If this option is enabled, the license key will be deployed automatically to managed devices.

If this option is disabled, you can deploy license key to managed devices later, in the **Kaspersky Licenses** node of the Administration Console tree.

- By specifying a key file

Key file is a file with the .key extension provided to you by Kaspersky. A key file is intended for adding a key that activates the application.

You receive your key file through the email address that you specified after purchasing Kaspersky Security Center.

To activate the application using a key file, you do not have to connect to Kaspersky activation servers.

If you have selected this activation option, you can enable the **Automatically deploy license key to managed devices** option.

If this option is enabled, the license key will be deployed automatically to managed devices.

If this option is disabled, you can deploy license key to managed devices later, in the **Kaspersky Licenses** node of the Administration Console tree.

- By postponing the application activation

The application will operate with basic functionality, without Mobile Device Management and without Vulnerability and Patch Management.

If you choose to postpone application activation, you can add a license key later at any time.

► *To add a license key after the Quick Start Wizard is finished:*

1. In the console tree, select the **Kaspersky Licenses** folder.
2. Click the **Add activation code or key file** button.

The Add License Key Wizard opens.

3. Follow the instructions of the Wizard.

Step 4. Selecting the protection scopes and platforms

Select the protection scopes and platforms that are in use on your network. When you select these options, you specify the filters for application management plug-ins and distribution packages on Kaspersky servers that you can download to install on client devices on your network. Select the options:

- **Areas**

You can select the following protection scopes:

- **Workstations.** Select this option if you want to protect workstations in your network. By default, the Workstation option is selected.
- **File Servers and Storage.** Select this option if you want to protect file servers in your network.
- **Mobile devices.** Select this option if you want to protect mobile devices owned by the company or by the company employees. If you select this option but you have not provided a license with the Mobile Device Management feature (see section "Kaspersky Security Center licensing options" on page [320](#)), a message is displayed informing you about necessity to provide a license with the Mobile Device Management feature. If you do not provide a license, you cannot use the Mobile device feature.
- **Virtualization.** Select this option if you want to protect virtual machines in your network.
- **Kaspersky Anti-Spam.** Select this option if you want to protect mail servers in your organization from spam, fraud and malware delivery.

- **Operating systems**

You can select the following platforms:

- Microsoft Windows
- Linux
- macOS
- Android
- iOS

After you have selected protection scopes and platforms, management plug-ins and distribution packages for Kaspersky applications automatically start to download.

Step 5. Selecting plug-ins for managed applications

Select plug-ins for managed applications to install. A list of plug-ins located on Kaspersky servers is displayed. The list is filtered according to the options selected on the previous step (see section "Step 4. Selecting the protection scopes and platforms" on page [268](#)) of the Wizard. By default, a full list include plug-ins of all languages. To display only plug-in of specific language, select the language from **Show the Administration Console localization language** or drop-down list. The list of plug-ins includes the following columns:

- **Application name**

The plug-ins depending of the components and platforms that you have selected on the previous step are selected.

- **Application version**

The list includes plug-ins of all the versions placed on Kaspersky servers. By default, the plug-ins of the latest versions are selected.

- **Localization language**

By default, the localization language of a plug-in is defined by the Kaspersky Security Center language that you have selected at installation. You can specify other languages in **Show the Administration Console localization language** or drop-down list.

After the plug-ins are selected, their installation starts automatically in a separate window. To install some plug-ins you must accept the terms of the EULA. Read the text of EULA, select the **I accept the terms of the License Agreement** check box and click the **Install** button. If you do not accept the terms of the EULA, the plug-in is not installed.

After the installation completes, close the installation window.

Step 6. Downloading distribution packages and creating installation packages

Kaspersky Endpoint Security for Windows includes encryption tool for the information stored on client devices. To download a distribution package of Kaspersky Endpoint Security for Windows valid for the needs of your organization, consult the legislation of the country where the client devices of your organization are located. In the **Encryption type** window, select one of the following encryption types:

- Strong encryption. This encryption type uses 256-bit key length.
- Lite encryption. This encryption type uses 56-bit key length.

The **Encryption type** window is displayed only if you have selected **Workstations** as a protection area and **Microsoft Windows** as a platform (see section "Step 4. Selecting the protection scopes and platforms" on page [268](#)).

After you have selected an encryption type, a list of distribution packages of both encryption types is displayed. A distribution package with selected encryption type, is selected in the list. The distribution package language corresponds to the Kaspersky Security Center language. If a distribution package of Kaspersky Endpoint Security for Windows for the Kaspersky Security Center language does not exist, English distribution package is selected.

In the list, you can select distribution package languages by means **Show the Administration Console localization language** or drop-down list.

Updates of managed applications may require a specific minimum version of Kaspersky Security Center to be installed.

In the list, you can select distribution packages of any encryption type, different of that you have selected in the **Encryption type** window. After you have selected a distribution package for Kaspersky Endpoint Security for Windows, downloading of the distribution packages, corresponding to the components and platforms (see section "Step 4. Selecting the protection scopes and platforms" on page [268](#)), starts. You can monitor the downloading progress in the **Download status** column. After the Quick Start Wizard has finished, installation packages of Network Agent for Windows and managed Kaspersky applications are displayed in the **Administration Server** → **Advanced** → **Remote installation** → **Installation packages** list.

To finish downloading of some distribution packages you must accept EULA. When you click the **Accept** button, the text of EULA is displayed. To proceed to the next step of the Wizard, you must accept the terms and conditions of the EULA and the terms and conditions of Kaspersky Privacy Policy. Select the check boxes relating to the EULA and Kaspersky Privacy Policy and click the **Accept all** button. If you do not accept the terms and conditions, the downloading of the package is canceled.

After you have accepted the terms and conditions of the EULA and the terms and conditions of Kaspersky Privacy Policy, the downloading of the distribution packages continues. When the downloading is finished, the **Installation package is created** status is displayed. Later, you can use installation packages to deploy Kaspersky applications on client devices.

If you prefer not to run the Wizard, you can create installation packages manually by going to **Administration Server** → **Advanced** → **Remote installation** → **Installation packages** in the Administration Console tree.

Step 7. Configuring Kaspersky Security Network usage

Read the Kaspersky Security Network (KSN) statement, which is displayed in the window. Specify the settings for relaying information about Kaspersky Security Center operations to the Kaspersky Security Network knowledge base. Select one of the following options:

- **I agree to use Kaspersky Security Network**

Kaspersky Security Center and managed applications installed on client devices will automatically transfer their operation details to Kaspersky Security Network (see section "About KSN" on page [785](#)). Participation in Kaspersky Security Network ensures faster updates of databases containing information about viruses and other threats, which ensures a faster response to emergent security threats.

- **I do not agree to use Kaspersky Security Network**

Kaspersky Security Center and managed applications will provide no information to Kaspersky Security Network.

If you select this option, the use of Kaspersky Security Network will be disabled.

If you downloaded the Kaspersky Endpoint Security for Windows plug-in, both KSN statements—the KSN statement for Kaspersky Security Center and the KSN statement for Kaspersky Endpoint Security for Windows—are displayed. KSN statements for other managed Kaspersky applications whose plug-ins were downloaded are displayed in separate windows and you must accept (or not accept) each of the statements separately.

Step 8. Configuring email notifications

Configure the sending of notifications about events registered during the operation of Kaspersky applications on managed devices. These settings are used as the default settings for Administration Server.

To configure the delivery of notifications about events occurring in Kaspersky applications, use the following settings:

- **Recipients (email addresses)**

The email addresses of users to whom the application will send notifications. You can enter one or more addresses; if you enter more than one address, separate them with a semicolon.

- **SMTP servers**

The address or addresses of your organization's mail servers.

If you enter more than one address, separate them with a semicolon. You can use the IP address or the Windows network name (NetBIOS name) of a device as the address.

- **SMTP server port**

Communication port number of the SMTP server. The default port number is 25.

- **Use ESMTP authentication**

Enables support of ESMTP authentication. When the check box is selected, in the **User name** and **Password** fields you can specify the ESMTP authentication settings. By default, this check box is cleared, and the ESMTP authentication settings are not available.

You can test the new email notification settings by clicking the **Send test message** button.

Step 9. Configuring update management

Configure the settings for managing updates of applications installed on client devices.

You can configure these settings only if you have provided a license key with the Vulnerabilities and Patch management option.

In the **Search for updates and install them** group of settings, you can select a mode of Kaspersky Security Center update search and installation:

- **Search for required updates**

The *Find vulnerabilities and required updates* task is created.

This option is selected by default.

- **Find and install required updates**

The *Find vulnerabilities and required updates* and *Install required updates and fix vulnerabilities* tasks are created automatically, if you do not have ones.

In the **Windows Server Update Services** group of settings, you can select the update synchronization method:

- **Use update sources defined in the domain policy**
- **Use Administration Server as a WSUS server**

Client devices will download Windows Update updates from the Administration Server. The *Perform Windows Update synchronization* task and Network Agent policy are created automatically, if you do not have ones.

Step 10. Connecting mobile devices

If you previously enabled the **Mobile devices** (see section "**Step 4. Selecting the protection scopes and platforms**" on page 268) protection area in the Wizard settings, specify the settings for connecting the enterprise mobile devices of the managed organization. If you did not enable **Mobile devices** protection area, this step is skipped.

At this step of the Wizard, do the following:

- Configure ports for connection of mobile devices
- Configure Administration Server authentication
- Create or manage certificates
- Set up issuance, automatic updating, and encryption of general-type certificates
- Create a moving rule for mobile devices

► *To set up the ports for connection of mobile devices:*

1. Click the **Configure** button to the right of the **Mobile device connection** field.
2. In the drop-down list, select **Configure ports**.

The Administration Server properties window opens, displaying the **Additional ports** section.

3. In the **Additional ports** section, you can specify the mobile device connection settings:

- **SSL port for the activation proxy server**

The number of an SSL port for connection of Kaspersky Endpoint Security for Windows to activation servers of Kaspersky.

The default port number is 17000.

- **Open port for mobile devices**

A port opens for mobile devices to connect to the Licensing Server. You can define the port number and other settings in the fields below.

By default, this option is enabled.

- **Port for mobile device synchronization**

Number of the port through which mobile devices connect to the Administration Server and exchange data with it. The default port number is 13292.

You can assign a different port if port 13292 is being used for other purposes.

- **Port for mobile device activation**

The port for connection of Kaspersky Endpoint Security for Android to activation servers of Kaspersky.

The default port number is 17100.

- **Open port for UEFI protection devices**

UEFI protection devices can connect to the Administration Server.

- **Port for UEFI protection devices**

You can change the port number if the **Open port for UEFI protection devices** option is enabled. The default port number is 13294.

4. Click **OK** to save changes and return to the Quick Start Wizard.

You will have to configure authentication of the Administration Server by mobile devices and authentication of mobile devices by the Administration Server. If you want, you can configure authentication later, separately from the Quick Start Wizard.

► *To configure Administration Server authentication by mobile devices:*

1. Click the **Configure** button to the right of the **Mobile device connection** field.
2. In the drop-down list, select **Configure authentication**.

The Administration Server properties window opens, displaying the **Certificates** section.

3. Select the authentication option for mobile devices in the **Administration Server authentication by mobile devices** group of settings, and select the authentication option for UEFI protection devices in the **Administration Server authentication by UEFI protection devices** group of settings.

When Administration Server exchanges data with client devices, it is authenticated through the use of a certificate.

By default, Administration Server uses the certificate that was created during Administration Server installation. If you want, you can add a new certificate.

► *To add a new certificate (optional):*

1. Select **Other certificate**.
The **Browse** button appears.
2. Click the **Browse** button.
3. In the window that opens, specify the certificate settings:

- **Certificate type**

- Activation time:

- **Immediately**

The current certificate will be immediately replaced with the new one after you click **OK**.

Previously connected mobile devices will not be able to connect to Administration Server.

- **After this period expires, days**

If you select this option, a reserve certificate will be generated. The current certificate will

be replaced with the new one in the specified number of days. The effective date of the reserve certificate is displayed in the **Certificates** section.

It is recommended that you plan the reissue in advance. The reserve certificate must be downloaded to the mobile devices before the specified period expires. After the current certificate is replaced with the new one, previously connected mobile devices that do not have the reserve certificate will not be able to connect to Administration Server.

4. Click the **Properties** button to view the settings of the selected Administration Server certificate.

► To reissue a certificate issued through Administration Server:

1. Select **Certificate issued through Administration Server**.
2. Click the **Reissue** button.
3. In the window that opens, specify the following settings:

- Connection address:

- **Use old connection address**

The address of the Administration Server to which mobile devices connect remains unchanged.

This option is selected by default.

- **Change connection address to**

If you want mobile devices to connect to a different address, specify the relevant address in this field.

If the address for mobile device connection has changed, a new certificate must be issued. The old certificate becomes invalid on all mobile devices connected. Previously connected devices will not be able to connect to Administration Server so they will become unmanaged.

- Activation time:

- **Immediately**

The current certificate will be immediately replaced with the new one after you click **OK**.

Previously connected mobile devices will not be able to connect to Administration Server.

- **After this period expires, days**

If you select this option, a reserve certificate will be generated. The current certificate will be replaced with the new one in the specified number of days. The effective date of the reserve certificate is displayed in the **Certificates** section.

It is recommended that you plan the reissue in advance. The reserve certificate must be

downloaded to the mobile devices before the specified period expires. After the current certificate is replaced with the new one, previously connected mobile devices that do not have the reserve certificate will not be able to connect to Administration Server.

4. Click **OK** to save changes and return to the **Certificates** window.
5. Click **OK** to save changes and return to the Quick Start Wizard.

► *To set up issuance, automatic updating, and encryption of general-type certificates for identification of mobile devices by Administration Server:*

1. Click the **Configure** button on the right of the **Mobile device authentication** field.

The **Certificate issuance rules** window opens, displaying the **Issuance of mobile certificates** section.

2. If necessary, specify the following settings in the **Issuance settings** section:

- **Certificate lifetime, days**

Certificate lifetime period in days. The default lifetime of a certificate is 365 days. When this period expires, the mobile device will not be able to connect to the Administration Server.

- **Certificate source**

Select the source of general-type certificates for mobile devices: certificates are issued by Administration Server, or they are specified manually.

You can modify the certificate templates if integration with the public key infrastructure (PKI) has been configured in the **Integration with PKI** section. In this case, the following template selection fields are available:

- **Default template**

Use a certificate issued by an external certificate source – Certification Center – under the default template.

By default, this option is selected.

- **Other template**

Select a template used to issue certificates. You can specify certificate templates in the domain. The **Refresh list** button updates the list of certificate templates.

3. If necessary, specify the following settings for automatic issuance of certificates in the **Automatic Updates settings** section:

- **Renew when certificate is to expire in (days)**

The number of days remaining until the current certificate's expiration during which Administration Server should issue a new certificate. For example, if the value of the field

is 4, Administration Server issues a new certificate four days before the current certificate expires. The default value is 7.

- **Reissue certificate automatically if possible**

If possible, certificates will be reissued automatically. If a certificate was manually defined, automatic reissuance is not available. If this check box is cleared, certificates will not be reissued automatically. By default, this check box is cleared.

Certificates are automatically reissued by a Certification Authority.

4. If necessary, in the **Password protection** settings section, specify the settings for decrypting certificates during installation.

Select the **Prompt for password during certificate installation** check box to prompt the user for password when the certificate is installed on a mobile device. The password is used only once—during installation of the certificate on the mobile device.

The password will be automatically generated by Administration Server and sent to the email address that you specified. You can specify the user's email address, or your own email address if you want to use another method to forward the password to the user.

You can use the slider to specify the number of characters in the certificate decryption password.

The password prompting option is required, for example, to protect a shared certificate in a stand-alone Kaspersky Endpoint Security for Android installation package. Password protection will prevent an intruder from obtaining access to the shared certificate through theft of the stand-alone installation package from Kaspersky Security Center Web Server.

If this check box is cleared, the certificate is automatically decrypted during installation and the user will not be prompted for a password. By default, this check box is cleared.

5. Click **OK** to save changes and return to the Quick Start Wizard window.

Click the **Cancel** button to return to the Quick Start Wizard without saving any changes made.

► *To enable the function for moving mobile devices to an administration group that you choose,*

In the **Automatic moving of mobile devices** field, select the **Create a moving rule for mobile devices** check box.

If the **Create a moving rule for mobile devices** check box is selected, the application automatically creates a moving rule that moves devices running Android and iOS to the **Managed devices** group:

- With Android operating systems on which a Kaspersky Endpoint Security for Android and a mobile certificate are installed
- With iOS operating systems on which the iOS MDM profile with a shared certificate is installed

If such a rule already exists, the application does not create it again.

By default, this check box is cleared.

Kaspersky no longer supports Kaspersky Safe Browser.

Step 11. Creating an initial protection configuration

The **Configure initial protection** window displays a list of policies and tasks that are created automatically. The following policies and tasks are created:

- Kaspersky Security Center Network Agent policy
- Policies for managed Kaspersky applications
- Administration Server maintenance task
- Backup of Administration Server data task
- Download updates to the Administration Server repository task
- Find vulnerabilities and required updates task
- Install update task

Wait for the creation of policies and tasks to complete before proceeding to the next step of the Wizard.

If you have downloaded and installed the plug-in for Kaspersky Endpoint Security for Windows 10 Service Pack 1 and later till the 11.0.1, during the creation of policies and tasks, a window opens for initial configuration of the trusted zone of Kaspersky Endpoint Security for Windows. The application will prompt you to add vendors verified by Kaspersky to the trusted zone for the purposes of excluding their applications from scans to prevent them from being accidentally blocked. You can create recommended exclusions now or create a list of exclusions later by selecting the following in the console tree: **Policies** → Kaspersky Endpoint Security properties menu → **Advanced Threat Protection** → **Trusted zone** → **Settings** → **Add**. The list of scan exclusions is available for editing at any time when using the application.

Operations on the trusted zone are performed by using tools integrated into Kaspersky Endpoint Security for Windows. For detailed instructions on how to perform operations and a description of encryption features please refer to Kaspersky Endpoint Security for Windows Online Help <https://support.kaspersky.com/KESWin/11.6.0/en-US/127971.htm>.

To finish initial configuration of the trusted zone and return to the Wizard, click **OK**.

Click **Next**. This button becomes available after all necessary policies and tasks have been created.

Step 12. Downloading updates

Updates for anti-virus databases for Kaspersky Security Center and managed Kaspersky applications are downloaded automatically. The updates are downloaded from Kaspersky servers.

Step 13. Device discovery

The **Network poll** window displays information about the status of network polling performed by the Administration Server.

You can view network devices detected by Administration Server and receive help on working with the **Device discovery** window by clicking the links in the lower part of the window.

See also:

Scenario: Discovering networked devices[303](#)

Step 14. Closing the Quick Start Wizard

In the Quick Start Wizard completion window, select the **Run the Remote Installation Wizard** check box if you want to start automatic installation of anti-virus applications and/or Network Agent on devices on your network.

To complete the Wizard, click the **Finish** button.

Configuring the connection of Administration Console to Administration Server

In earlier versions of Kaspersky Security Center, Administration Console was connected to Administration Server through SSL port TCP 13291, as well as SSL port TCP 13000. Starting from Kaspersky Security Center 10 Service Pack 2, the SSL ports used by the application are strictly separated and misuse of ports is not possible:

- SSL port TCP 13291 can only be used by Administration Console and klakaut automation objects.
- SSL port TCP 13000 can only be used by Network Agent, a secondary Administration Server, and the primary Administration Server in the DMZ.

Port TCP 14000 can be used for connecting Administration Console, distribution points, secondary Administration Servers, and klakaut automation objects, as well as for receiving data from client devices.

In some cases, Administration Console may have to be connected through SSL port 13000:

- If a single SSL port is likely to be used both for Administration Console and for other activities (receiving data from client devices, connecting distribution points, connecting secondary Administration Servers).
- If a klakaut automation object is not connected to Administration Server directly but through a distribution point in the DMZ.

► *To allow the connection of Administration Console over port 13000:*

1. Open the system registry of the device on which Administration Server is installed (for example, locally, using the regedit command in the **Start** → **Run** menu).
2. Go to the following hive:
 - For a 64-bit system:
HKEY_LOCAL_MACHINE\SOFTWAREWow6432Node\KasperskyLab\Components\34\core\independent\KLLIM
 - For a 32-bit system:
HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\core\independent\KLLIM
3. For the LP_ConsoleMustUsePort13291 (DWORD) key, set 00000000 as the value.
The default value specified for this key is 1.
4. Restart the Administration Server service.

You will now be able to connect Administration Console to Administration Server over port 13000.

Requirements to custom certificates used in Kaspersky Security Center

The table below shows the requirements for custom certificates specified for different components of Kaspersky Security Center (see section "About Kaspersky Security Center certificates" on page [86](#)).

Table 44. *Requirements for Kaspersky Security Center certificates*

Certificate type	Requirements	Comments
Common certificate, Common reserve certificate ("C", "CR")	<p>Minimum key length: 2048.</p> <p>Basic constraints:</p> <ul style="list-style-type: none"> • CA: true • Path Length Constraint: None <p>Key Usage:</p> <ul style="list-style-type: none"> • Digital signature • Certificate signing • Key encipherment • CRL Signing <p>Extended Key Usage (optional): server authentication, client authentication.</p>	<p>Extended Key Usage parameter is optional.</p> <p>Path Length Constraint value may be an integer different from "None", but not less than 1.</p>
Mobile certificate, Mobile reserve certificate ("M", "MR")	<p>Minimum key length: 2048.</p> <p>Basic constraints:</p> <ul style="list-style-type: none"> • CA: true • Path Length Constraint: None <p>Key Usage:</p> <ul style="list-style-type: none"> • Digital signature • Certificate signing • Key encipherment • CRL Signing <p>Extended Key Usage (optional): server authentication.</p>	<p>Extended Key Usage parameter is optional.</p> <p>Path Length Constraint value may be an integer different from "None", if Common certificate has a Path Length Constraint value not less than 1.</p>
Certificate CA for auto-generated user certificates ("MCA")	<p>Minimum key length: 2048.</p> <p>Basic constraints:</p> <ul style="list-style-type: none"> • CA: true • Path Length Constraint: None <p>Key Usage:</p> <ul style="list-style-type: none"> • Digital signature • Certificate signing • Key encipherment • CRL Signing <p>Extended Key Usage (optional): server authentication, client authentication.</p>	<p>Extended Key Usage parameter is optional.</p> <p>Path Length Constraint value may be an integer different from "None," if Common certificate has a Path Length Constraint value not less than 1.</p>

Certificate type	Requirements	Comments
Web Server certificate	<p>Extended Key Usage: server authentication.</p> <p>The PKCS #12 / PEM container from which the certificate is specified includes the entire chain of public keys.</p> <p>The Subject Alternative Name (SAN) of the certificate is present; that is, the value of the <code>subjectAltName</code> field is valid.</p> <p>The certificate meets the effective requirements of browsers imposed on server certificates, as well as the current baseline requirements of the CA/Browser Forum.</p>	Not applicable.
Kaspersky Security Center Web Console certificate	<p>The PEM container from which the certificate is specified includes the entire chain of public keys.</p> <p>The Subject Alternative Name (SAN) of the certificate is present; that is, the value of the <code>subjectAltName</code> field is valid.</p> <p>The certificate meets the effective requirements of browsers to server certificates, as well as the current baseline requirements of the CA/Browser Forum.</p>	Encrypted certificates are not supported by Kaspersky Security Center Web Console (scheduled for version 13).

See also:

Administration Server certificate	604
Main installation scenario	59

Connecting out-of-office devices

This section describes how to connect out-of-office devices (that is, managed devices that are located outside of the main network) to Administration Server.

In this section

Scenario: Connecting out-of-office devices through a connection gateway.....	283
About connecting out-of-office devices.....	285
Connecting external desktop computers to Administration Server	286
About connection profiles for out-of-office users	287
Creating a connection profile for out-of-office users.....	288
About switching Network Agent to other Administration Servers	291
Creating a Network Agent switching rule by network location.....	292

Scenario: Connecting out-of-office devices through a connection gateway

This scenario describes how to connect managed devices that are located outside of the main network to Administration Server.

Prerequisites

The scenario has the following prerequisites:

- A demilitarized zone (DMZ) is organized in your organization's network.
- Kaspersky Security Center Administration Server is deployed on the corporate network.

Stages

This scenario proceeds in stages:

a. Selecting a client device in the DMZ

This device will be used as a connection gateway (on page [57](#)). The device that you select must meet the requirements for connection gateways.

b. Installing Network Agent in the connection gateway role

We recommend that you use a local installation (see section "Local installation of Network Agent" on page [178](#)) to install Network Agent on the selected device.

By default, the installation file is located at: \\<server name>\KLSHARE\PKgInst\NetAgent_<version number>

In the **Connection gateway** window of the Network Agent Setup Wizard, select **Use Network Agent as a connection gateway in DMZ**. This mode simultaneously activates the connection gateway role and tells Network Agent to wait for connections from Administration Server, rather than establish connections to Administration Server.

Alternatively, you can install Network Agent on a Linux device and configure Network Agent to work as a connection gateway (see section "Connecting a Linux device as a gateway in the demilitarized zone" on page [590](#)), but pay attention to the list of limitations of Network Agent running on Linux devices (see section "Usage of Network Agent for Windows, for macOS and for Linux: comparison" on page [942](#)).

c. Allowing connections in firewalls on the connection gateway

To make sure that Administration Server can actually connect to the connection gateway in the DMZ, allow connections to TCP port 13000 in all firewalls between Administration Server and the connection gateway.

If the connection gateway has no real IP address on the Internet, but instead is located behind Network Address Translation (NAT), configure a rule to forward connections through NAT.

d. Creating an administration group for external devices

Create a new group (see section "Creating administration groups" on page [631](#)) under the **Managed devices** group. This new group will contain external managed devices.

e. Connecting the connection gateway to Administration Server

The connection gateway that you have configured is waiting for a connection from Administration Server. However, Administration Server does not list the device with the connection gateway among managed devices. This is because the connection gateway has not tried to establish a connection to Administration Server. Therefore, you need a special procedure to ensure that Administration Server initiates a connection to the connection gateway.

Do the following:

Add the connection gateway as a distribution point (see section "Adding a connection gateway in the DMZ as a distribution point" on page [592](#)).

Move the connection gateway (see section "Moving devices to an administration group" on page [644](#)) from the **Unassigned devices** group to the group that you have created for external devices.

The connection gateway is connected and configured.

f. Connecting external desktop computers to Administration Server

Usually, external desktop computers are not moved inside the perimeter. Therefore, you need to configure them to connect (see section "Connecting external desktop computers to Administration Server" on page [286](#)) to Administration Server through the gateway when installing Network Agent.

g. Setting up updates for external desktop computers

If updates of security applications are configured to be downloaded from Administration Server, external computers download updates through the connection gateway. This has two disadvantages:

This is unnecessary traffic, which takes up bandwidth of the company's Internet communication channel.

This is not necessarily the quickest way to get updates. It is very likely that it would be cheaper and faster for external computers to receive updates from Kaspersky update servers.

Do the following:

Move all external computers to the separate administration group (see section "Moving devices to an administration group" on page [644](#)) that you created earlier.

Exclude the group with external devices from the update task (see section "Automatic installation of Kaspersky Endpoint Security updates on devices" on page [441](#)).

Create a separate update task for the group with external devices (see section "Automatic installation of Kaspersky Endpoint Security updates on devices" on page [441](#)).

h. Connecting traveling laptops to Administration Server

Traveling laptops are within the network sometimes and outside the network at other times. For effective management, you need them to connect to Administration Server differently depending on their location. For efficient use of traffic, they also need to receive updates from different sources, depending on their location.

You need to configure rules for out-of-office users (see section "About switching Network Agent to other Administration Servers" on page [291](#)): connection profiles (see section "Creating a connection profile for out-of-office users" on page [288](#)) and network location descriptions (see section "Creating a Network Agent switching rule by network location" on page [292](#)). Each rule defines the Administration Server instance to which traveling laptops must connect, depending on their location and the Administration Server instance from which they must receive updates.

See also:

Internet access: Network Agent as connection gateway in DMZ[132](#)

About connecting out-of-office devices

Some managed devices are always located outside of the main network (for example, computers in a company's regional branches; kiosks, ATMs, and terminals installed at various points of sale; computers in the home offices of employees). Some devices travel outside the perimeter from time to time (for example, laptops of users who visit regional branches or a customer's office).

You still need to monitor and manage the protection of out-of-office devices—receive actual information about their protection status and keep the security applications on them in the up-to-date state. This is necessary because, for example, if such a device is compromised while being away from the main network, it could become a platform for propagating threats as soon as it connects to the main network. To connect out-of-office devices to Administration Server, you can use two methods:

- Connection gateway in the demilitarized zone (DMZ)
See the data traffic scheme: Administration Server on LAN, managed devices on the Internet, connection gateway in use (see section "Administration Server on LAN, managed devices on Internet, connection gateway in use" on page [99](#))
- Administration Server in the DMZ
See the data traffic scheme: Administration Server in DMZ, managed devices on Internet (on page [104](#))

A connection gateway in the DMZ

A recommended method for connecting out-of-office devices to Administration Server is organizing a DMZ in the organization's network and installing a connection gateway (on page [57](#)) in the DMZ. External devices will connect to the connection gateway, and Administration Server inside the network will initiate a connection to the devices via the connection gateway.

As compared to the other method, this one is more secure:

- You do not need to open access to Administration Server from outside the network.
- A compromised connection gateway does not pose a high risk to the safety of the network devices. A connection gateway does not actually manage anything itself and does not establish any connections.

Also, a connection gateway does not require many hardware resources.

However, this method has a more complicated configuration process:

- To act a device as a connection gateway in the DMZ, you need to install Network Agent and connect it to Administration Server in a specific way.
- You will not be able to use the same address for connecting to Administration Server for all situations. From outside the perimeter, you will need to use not just a different address (connection gateway address), but also a different connection mode: through a connection gateway.
- You also need to define different connection settings for laptops in different locations.

The scenario in this section (see section "Scenario: Connecting out-of-office devices through a connection gateway" on page [283](#)) describes this method.

Administration Server in the DMZ

Another method is installing a single Administration Server in the DMZ.

This configuration is less secure than the other method. To manage external laptops in this case, Administration Server must accept connections from any address on the Internet. It will still manage all devices in the internal network, but from the DMZ. Therefore, a compromised Server could cause an enormous amount of damage, despite the low likelihood of such an event.

The risk gets significantly lower if Administration Server in the DMZ does not manage devices in the internal network. Such a configuration can be used, for example, by a service provider to manage the devices of customers.

You might want to use this method in the following cases:

- If you are familiar with installing and configuring Administration Server, and do not want to perform another procedure to install and configure a connection gateway.
- If you need to manage more devices. The maximum capacity of Administration Server is 100,000 devices, while a connection gateway can support up to 10,000 devices.

This solution also has possible difficulties:

- Administration Server requires more hardware resources and one more database.
- Information about devices will be stored in two unrelated databases (for Administration Server inside the network and another one in the DMZ), which complicates monitoring.
- To manage all devices, Administration Server needs to be joined into a hierarchy, which complicates not only monitoring but also management. A secondary Administration Server instance imposes limitations on the possible structures of administration groups. You have to decide how and which tasks and policies to distribute to a secondary Administration Server instance.
- Configuring external devices to use Administration Server in the DMZ from the outside and to use the primary Administration Server from the inside is not simpler than to just configure them to use a conditional connection through a gateway.
- High security risks. A compromised Administration Server instance makes it easier to compromise its managed laptops. If this happens, the hackers just need to wait for one of the laptops to return to the corporate network so that they can continue their attack on the local area network.

See also:

Administration Server and two devices in DMZ: a connection gateway and a client device.....	117
Internet access: Network Agent as connection gateway in DMZ	132
Administration Server in DMZ, managed devices on Internet	104
Internet access: Administration Server in DMZ	131

Connecting external desktop computers to Administration Server

Desktop computers that are always outside of the main network (for example, computers in the company's regional branches; kiosks, ATMs, and terminals installed at various points of sale; computers in the home offices of employees) cannot be connected to Administration Server directly. They must be connected to Administration Server via a connection gateway that is installed in the demilitarized zone (DMZ). This configuration is made when installing Network Agent on those computers.

► *To connect external desktop computers to Administration Server:*

1. Create a new installation package for Network Agent (see section "Creating an installation package" on page [344](#)).

When creating the installation package, select the nagent.kud file in the NetAgent folder of the Kaspersky Security Center distribution package.

2. Go to the properties of the created installation package, click the **Advanced** section, and then select the **Connect to Administration Server by using connection gateway** check box.

The **Connect to Administration Server by using connection gateway** setting is incompatible with the **Use Network Agent as a connection gateway in DMZ** setting. You cannot enable both of these settings at the same time.

3. In **Connection gateway address**, specify the public address of the connection gateway.

If the connection gateway is located behind Network Address Translation (NAT) and does not have its own public address, configure a NAT gateway rule for forwarding connections from the public address to the internal address of the connection gateway.

4. Create a stand-alone installation package (see section "Creating stand-alone installation packages" on page [346](#)) based on the created installation package.
5. Deliver the stand-alone installation package to the target computers, either electronically or on a removable drive.
6. Install Network Agent from the stand-alone package.

External desktop computers are connected to Administration Server.

About connection profiles for out-of-office users

Out-of-office users of laptops (hereinafter also referred to as "devices") may need to change the method of connecting to an Administration Server or switch between Administration Servers depending on the current location of the device on the enterprise network.

Connection profiles are supported only for devices running Windows.

Using different addresses of a single Administration Server

The following procedure is only applied to Kaspersky Security Center 10 Service Pack 1 and later.

Devices with Network Agent installed can connect to the Administration Server either from the organization's intranet or from the Internet. This situation may require Network Agent to use different addresses for connection to Administration Server: the external Administration Server address for the Internet connection and the internal Administration Server address for the internal network connection.

To do this, you must add a profile (for connection to Administration Server from the Internet) to the Network Agent policy. Add the profile in the policy properties (**Connectivity** section, **Connection profiles** subsection). In the profile creation window, you must clear the **Use to receive updates only** check box and select the **Synchronize**

connection settings with the Administration Server settings specified in this profile check box. If you use a connection gateway to access Administration Server (for example, in a Kaspersky Security Center configuration as that described in Internet access: Network Agent as connection gateway in DMZ (on page [132](#))), you must specify the address of the connection gateway in the corresponding field of the connection profile.

Switching between Administration Servers depending on the current network

The following procedure is only applied to Kaspersky Security Center 10 Service Pack 2 Maintenance Release 1 and any later versions.

If the organization has multiple offices with different Administration Servers and some of the devices with Network Agent installed move between them, you need Network Agent to connect to the Administration Server of the local network in the office where the device is currently located.

In this case, you must create a profile for connection to Administration Server in the properties of the policy of Network Agent for each of the offices, except for the home office where the original home Administration Server is located. You must specify the addresses of Administration Servers in connection profiles and select or clear the **Use to receive updates only** check box:

- Select the check box if you need Network Agent to be synchronized with the home Administration Server, while using the local Server for downloading updates only.
- Clear the check box if it is necessary for Network Agent to be managed completely by the local Administration Server.

After that, you must set up the conditions of switching to the newly created profiles: at least one condition for each of the offices, except for the home office. Every condition's purpose consists in detection of items that are specific for an office's network environment. If a condition is true, the corresponding profile gets activated. If none of the conditions is true, Network Agent switches to the home Administration Server.

See also:

Providing Internet access to the Administration Server.....	130
Internet access: Network Agent as connection gateway in DMZ	132
Creating a connection profile for out-of-office users.....	288

Creating a connection profile for out-of-office users

An Administration Server connection profile is available only on devices running Windows.

► *To create a profile for connecting Network Agent to Administration Server for out-of-office users:*

1. In the console tree, select the administration group containing the client devices for which you need to create a profile for connecting Network Agent to the Administration Server.
2. Do one of the following:

- If you want to create a connection profile for all devices in the group, select a Network Agent policy in the group workspace, on the **Policies** tab. Open the properties window of the selected policy.
 - If you want to create a connection profile for a device in a group, select that device in the group workspace, on the **Devices** tab, and perform the following actions:
 - a. Open the properties window of the selected device.
 - b. In the **Applications** section of the device properties window, select Network Agent.
 - c. Open the Network Agent properties window.
3. In the properties window, in the **Connectivity** section select the **Connection profiles** subsection.
 4. In the **Administration Server connection profiles** settings group, click the **Add** button.

By default, the list of connection profiles contains the <Offline mode> and <Home Administration Server> profiles. Profiles cannot be edited or removed.

The <Offline mode> profile does not specify any Server for connection. Therefore, Network Agent, when switched to that profile, does not attempt to connect to any Administration Server while applications installed on client devices run under out-of-office policies. The <Offline mode> profile can be used if devices are disconnected from the network.

The <Home Administration Server> profile specifies for connection the Administration Server that was selected during Network Agent installation. The <Home Administration Server> profile is applied when a device is reconnected to the home Administration Server after it was running on an external network for some time.

5. In the **New profile** window that opens, configure the connection profile:
 - **Profile name**

In the entry field you can view or change the connection profile name.
 - **Administration Server**

Address of the Administration Server to which the client device must connect during profile activation.
 - **Port**

Port number that is used for connection.
 - **SSL port**

Port number for connection if using the SSL protocol.
 - **Use SSL**

If this check box is selected, the connection is established through a secure port, by using SSL protocol.

By default, this check box is selected.
 - Click the **Configure connection through proxy server** link to configure connection through a proxy server:
 - **Use proxy server**

If this check box is selected, connection to the Administration Server is established through a proxy server.

If this check box is cleared, the entry fields for connection to the proxy server are not available.

By default, this check box is cleared.

- **Proxy server address**

Address of the proxy server used for Kaspersky Security Center connection to the Internet.
- **Port number**

Number of the port through which Kaspersky Security Center proxy connection will be established.
- **Proxy server authentication**

If this check box is selected, in the entry fields you can specify the credentials for proxy server authentication.

This entry field is available if the **Use proxy server** check box is selected.
- **User name** (this field is available if the **Proxy server authentication** check box is selected)

User account under which connection to the proxy server is established (this field is available if the **Proxy server authentication** check box is selected).
- **Password** (this field is available if the **Proxy server authentication** check box is selected)

Password set by the user under whose account the proxy server connection is established (this field is available if the **Proxy server authentication** check box is selected).

To see the entered password, click and hold the **Show** button for as long as you require.
- **Connection gateway settings**

Address of the gateway through which client devices connect to the Administration Server.
- **Enable out-of-office mode**

If this check box is selected, in case of connection through this profile, applications installed on the client device use policy profiles for devices in out-of-office mode, as well as out-of-office policies (see section "About switching Network Agent to other Administration Servers" on page [291](#)). If no out-of-office policy has been defined for the application, the active policy will be used.

If this check box is cleared, applications will use active policies.

By default, this check box is cleared.
- **Use to receive updates only**

If this check box is selected, the profile will only be used for downloading updates by applications installed on the client device. For other operations, connection to the Administration Server will be established with the initial connection settings defined during Network Agent installation.

By default, this check box is selected.
- **Synchronize connection settings with the Administration Server settings specified in this profile**

If this check box is selected, Network Agent connects to Administration Server using the settings specified in the profile properties.

If this check box is cleared, Network Agent connects to Administration Server using the

original settings that have been specified during installation.

This check box is available if the **Use to receive updates only** check box is cleared.

By default, this check box is cleared.

6. Select the **Enable out-of-office mode when Administration Server is not available** check box to allow the applications installed on a client device to use policy profiles for devices in out-of-office mode, as well as out-of-office policies (see section "About switching Network Agent to other Administration Servers" on page [291](#)), at any connection attempt if the Administration Server is not available. If no out-of-office policy has been defined for the application, the active policy will be used.

A profile for connecting Network Agent to Administration Server is created for out-of-office users. When Network Agent connects to Administration Server using this profile, applications installed on the client device will use policies for devices in out-of-office mode, or out-of-office policies.

See also:

| About connection profiles for out-of-office users.....[287](#)

About switching Network Agent to other Administration Servers

Kaspersky Security Center provides the option of switching Network Agent on a client device to other Administration Servers if the following settings of the network have been changed:

- Default gateway address—The address of the main network gateway has changed.
- DHCP server address—The IP address of the network DHCP server has changed.
- DNS domain—The DNS suffix of the subnet has changed.
- DNS server address—The IP address of the network DNS server has changed.
- Windows domain accessibility—The status of the Windows domain to which the client device is connected has changed.
- Subnet—The subnet address and mask have changed.
- WINS server address—The IP address of the network WINS server has changed.
- Name resolvability—The DNS or NetBIOS name of the client device has changed.
- SSL connection address accessibility—The client device can or cannot (depending on the option that you select) establish an SSL connection with Administration Server (name:port).

This feature is supported only for Network Agents installed on devices running Windows (see section "Hardware and software requirements" on page [31](#)).

The initial settings of the Network Agent connection to Administration Server are defined when installing the Network Agent. Afterwards, if rules for switching the Network Agent to other Administration Servers have been created, the Network Agent responds to changes in the network settings as follows:

- If the network settings comply with one of the rules created, Network Agent connects to the Administration Server specified in this rule. Applications installed on client devices switch to out-of-office policies, provided such behavior is enabled by a rule.
- If none of the rules apply, Network Agent reverts to the default settings of connection to the Administration Server specified during the installation. Applications installed on client devices switch back to active policies.

- If the Administration Server is not accessible, Network Agent uses out-of-office policies.

Network Agent switches to the out-of-office policy only if the **Enable out-of-office mode when Administration Server is not available** (see section "**Creating a connection profile for out-of-office users**" on page 288) option is enabled in the Network Agent policy settings.

The settings of Network Agent connection to Administration Server are saved in a connection profile. In the connection profile, you can create rules for switching client devices to out-of-office policies, and you can configure the profile so that it could only be used for downloading updates.

Creating a Network Agent switching rule by network location

Network Agent-switching by network location is available only on devices running Windows.

- ▶ *To create a rule for Network Agent switching from one Administration Server to another if network settings change:*
 1. In the console tree, select the administration group containing the devices for which you need to create a Network Agent switching rule by the network location description.
 2. Do one of the following:
 - If you want to create a rule for all devices in the group, go to the group workspace and select a Network Agent policy on the **Policies** tab. Open the properties window of the selected policy.
 - If you want to create a rule for a device selected from a group, go to the group workspace, select the device on the **Devices** tab, and perform the following actions:
 - a. Open the properties window of the selected device.
 - b. In the **Applications** section of the device properties window, select Network Agent.
 - c. Open the Network Agent properties window.
 3. In the properties window that opens, in the **Connectivity** section, select the **Connection profiles** subsection.
 4. In the **Network location settings** section, click the **Add** button.
 5. In the **New description** window that opens, configure the network location description and switching rule. Specify the following network location description settings:
 - **Network location description name**

The name of a network location description cannot be longer than 255 characters nor contain special symbols, such as ("*<>?V:|).
 - **Use connection profile**

In the drop-down list you can specify the connection profile that Network Agent uses to connect to the Administration Server. This profile will be used when the network location description conditions are met. The connection profile contains the settings for Network Agent connection to the Administration Server; it also defines when client devices must switch to out-of-office policies. The profile is used only for downloading updates.

6. In the **Switch conditions** section, click the **Add** button to create a list of network location description conditions.

The conditions in a rule are combined by using the logical AND operator. To trigger a switching rule by the network location description, all of the rule switching conditions must be met.

7. In the drop-down list, select the value that corresponds to the change in characteristics of the network to which the client device is connected:
 - **Default connection gateway address**—The address of the main network gateway has changed.
 - **DHCP server address**—The IP address of the network Dynamic Host Configuration Protocol (DHCP) server has changed.
 - **DNS domain**—The DNS suffix of the subnet has changed.
 - **DNS server address**—The IP address of the network DNS server has changed.
 - **Windows domain accessibility**—Changes the status of the Windows domain to which the client device is connected.
 - **Subnet**—Changes the subnet address and mask.
 - **WINS server address**—The IP address of the network WINS server has changed.
 - **Name resolvability**—The DNS or NetBIOS name of the client device has changed.
 - **SSL connection address accessibility**—The client device can or cannot (depending on the option that you select) establish an SSL connection with a specified Server (name:port). For each server, you can additionally specify an SSL certificate. In this case, the Network Agent verifies the Server certificate in addition to checking the capability of an SSL connection. If the certificate does not match, the connection fails.
8. In the window that opens, specify the condition for Network Agent to be switched to another Administration Server. The name of the window depends on the value selected during the previous step. Specify the following settings of the switching condition:

- **Value**

In the field, you can add one or several values for the condition being created.

- **Matches at least one value from the list**

If this option is selected, the condition will be met regardless of any value specified in the **Value** list.

By default, this option is selected.

- **Does not match any of the values in the list**

If this option is selected, the condition is met if its value is not in the **Value** list.

9. In the **New description** window, select the **Description enabled** check box to enable the use of the new network location description.

A new switching rule by the network location description is created; any time its conditions are met, the Network Agent uses the connection profile specified in the rule to connect to the Administration Server.

The network location descriptions are checked for a match to the network layout in the order of their appearance in the list. If a network matches several descriptions, the first one will be used.

You can change the order of rules on the list using the **Up** button () and **Down** button ()

Encrypt communication with SSL/TLS

To fix vulnerabilities on your organization's corporate network, you can enable traffic encryption using SSL/TLS. You can enable SSL/TLS on Administration Server and iOS MDM Server. Kaspersky Security Center supports SSL v3 as well as Transport Layer Security (TLS v1.0, 1.1, and 1.2). You can select encryption protocol and cipher suites. Kaspersky Security Center uses a self-signed certificates. Additional configuration of the iOS devices is not required. You can also use your own certificates. Kaspersky specialists recommend to use certificates issued by trusted certificate authorities.

Administration Server

► *To configure allowed encryption protocols and cipher suites on the Administration Server:*

1. Open the system registry of the client device that has Administration Server installed (for example, locally, using the `regedit` command in the Start → Run menu).

2. Go to the following hive:

- For a 64-bit system:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.  
core\independent\Transport
```

- For a 32-bit system:

```
HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.  
core\independent\Transport
```

3. Create a key with the `SrvUseStrictSslSettings` name.

4. Specify `DWORD` as the key type.

5. Set the key value:

- 0—All of the supported encryption protocols and cipher suites are enabled
- 1—SSL v2 is disabled

Cipher suites:

- AES256-GCM-SHA384
- AES256-SHA256
- AES256-SHA
- CAMELLIA256-SHA
- AES128-GCM-SHA256
- AES128-SHA256
- AES128-SHA
- SEED-SHA
- CAMELLIA128-SHA
- IDEA-CBC-SHA
- RC4-SHA

- RC4-MD5
- DES-CBC3-SHA
- 2—SSL v2 and SSL v3 are disabled (default value)

Cipher suites:

- AES256-GCM-SHA384
- AES256-SHA256
- AES256-SHA
- CAMELLIA256-SHA
- AES128-GCM-SHA256
- AES128-SHA256
- AES128-SHA
- SEED-SHA
- CAMELLIA128-SHA
- IDEA-CBC-SHA
- RC4-SHA
- RC4-MD5
- DES-CBC3-SHA
- 3—only TLS v1.2.

Cipher suites:

- AES256-GCM-SHA384
- AES256-SHA256
- AES256-SHA
- CAMELLIA256-SHA
- AES128-GCM-SHA256
- AES128-SHA256
- AES128-SHA
- CAMELLIA128-SHA

6. Restart the Kaspersky Security Center 13 Administration Server service.

iOS MDM Server

The connection between the iOS devices and the iOS MDM Server is encrypted default.

► *To configure allowed encryption protocols and cipher suites on the iOS MDM Server:*

1. Open the system registry of the client device that has iOS MDM Server installed (for example, locally, using the regedit command in the Start → Run menu).
2. Go to the following hive:

- For a 64-bit system:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0\Conset
```

- For a 32-bit system:

```
HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0\Conset
```

3. Create a key with the `StrictSslSettings` name.
4. Specify `DWORD` as the key type.
5. Set the key value:
 - 2—SSL v3 is disabled (TLS 1.0, TLS 1.1, TLS 1.2 are allowed)
 - 3—only TLS 1.2 (default value)
6. Restart the Kaspersky Security Center 13 iOS MDM Server service.

Notifications of events

This section describes how to select a method for delivering administrator notifications about events on client devices, and how to configure event notification settings.

It also describes how to test the distribution of event notifications by using the Eicar test virus.

In this chapter

Configuring event notification	297
Testing notifications	299
Event notifications displayed by running an executable file	300

Configuring event notification

Kaspersky Security Center allows you to select a method of notifying the administrator of events on client devices and to configure notification.

- **Email.** When an event occurs, the application sends a notification to email addresses specified. You can edit the text of the notification.
- **SMS.** When an event occurs, the application sends a notification to the phone numbers specified. You can configure SMS notifications to be sent through the mail gateway.
- **Executable file.** When an event occurs on a device, the executable file is started on the administrator's workstation. Using the executable file, the administrator can receive the parameters of any event that has occurred (see section "Event notifications displayed by running an executable file" on page [300](#)).

► *To configure notification of events occurring on client devices:*

1. In the console tree, select the node with the name of the required Administration Server.
2. In the workspace of the node, select the **Events** tab.
3. Click the **Configure notifications and event export** link and select the **Configure notifications** value in the drop-down list.

This opens the **Properties: Events** window.

4. In the **Notification** section, select a notification method (by email, by SMS, or by running an executable file) and define the notification settings:
 - **Email**

The **Email** tab allows you to configure event notification by email.

In the **Recipients (email addresses)** field, specify the email addresses to which the application will send notifications. You can specify multiple addresses in this field, separating them with semicolons.

In the **SMTP servers** field, specify mail server addresses, separating them with semicolons. You can use the IP address or the Windows network name (NetBIOS name) of the device as the address.

In the **SMTP server port** field, specify the number of an SMTP server communication

port. The default port number is 25.

Click the **Settings** link to define additional notification settings (for example, specify a message subject).

The **Notification message** field contains standard text with information about the event that the application sends when an event occurs. This text includes substitute parameters, such as event name, device name, and domain name. You can edit the message text by adding some other substitute parameters with more relevant details of the event. The list of substitute parameters is available by clicking the button to the right of the field.

If the notification text contains a percent sign (%), you have to type it twice in a row to allow message sending. For example, "CPU load is 100%%".

Clicking the **Configure numeric limit of notifications** link allows you to specify the maximum number of notifications that the application can send over the specified time interval.

Clicking the **Send test message** button allows you to check if you have configured notifications properly: the application sends a test notification to the email addresses that you have specified.

- **SMS**

The **SMS** tab allows you to configure the transmission of SMS notifications of various events to a cell phone. SMS messages will be sent through a mail gateway.

In the **Recipients (email addresses)** field, specify the email addresses to which the application will send notifications. You can specify multiple addresses in this field, separating them with semicolons. The notifications will be delivered to the phone numbers associated with the specified email addresses.

In the **SMTP servers** field, specify mail server addresses, separating them with semicolons. You can use the IP address or the Windows network name (NetBIOS name) of the device as the address.

In the **SMTP server port** field, specify the number of an SMTP server communication port. The default port number is 25.

Click the **Settings** link to define additional notification settings (for example, specify a message subject).

The **Notification message** field contains standard text with information about the event that the application sends when an event occurs. This text includes substitute parameters, such as event name, device name, and domain name. You can edit the message text by adding some other substitute parameters with more relevant details of the event. The list of substitute parameters is available by clicking the button to the right of the field.

If the notification text contains a percent sign (%), you have to type it twice in a row to allow message sending. For example, "CPU load is 100%%".

Clicking the **Configure numeric limit of notifications** link allows you to specify the maximum number of notifications that the application can send during the specified time interval.

Clicking the **Send test message** allows you to check whether you configured notifications properly: the application sends a test notification to the recipient that you specified.

- **Executable file to be run**

If this notification method is selected, in the entry field you can specify the application that will start when an event occurs.

Clicking the **Configure numeric limit of notifications** link allows you to specify the maximum number of notifications that the application can send during the specified time interval.

Clicking the **Send test message** button allows you to check whether you configured notifications properly: the application sends a test notification to the email addresses that you specified.

1. In the **Notification message** field, enter the text that the application will send when an event occurs. You can use the drop-down list to the right of the text field to add substitution settings with event details (for example, event description, or time of occurrence).

If the notification text contains a percent (%), you must specify it twice in succession to allow message sending. For example, "CPU load is 100%%".

2. Click the **Send test message** button to check whether notification has been configured correctly. The application sends a test notification to the specified user.
3. Click **OK** to save the changes.

The re-adjusted notification settings are applied to all events that occur on client devices.

You can override notification settings for certain events in the **Event configuration** section of the Administration Server settings, of a policy settings (see section "General policy settings" on page [663](#)), or of an application settings (see section "Selecting events for an application" on page [798](#)).

See also:

Event processing and storage on the Administration Server[610](#)

Testing notifications

To check whether event notifications are sent, the application uses the notification of the EICAR test "virus" detection on client devices.

► *To verify sending of event notifications:*

1. Stop the real-time file system protection task on a client device and copy the EICAR test "virus" to that client device. Now re-enable real-time protection of the file system.
2. Run a scan task for client devices in an administration group or for specific devices, including one with the EICAR "virus".

If the scan task is configured correctly, the test "virus" will be detected. If notifications are configured correctly, you are notified that a virus has been detected.

In the workspace of the **Administration Server** node, on the **Events** tab, the **Recent events** selection displays a record of detection of a "virus".

The EICAR test "virus" contains no code that can do harm to your device. However, most manufacturers' security applications identify this file as virus. You can download the test "virus" from the official EICAR website <https://www.eicar.org>.

Event notifications displayed by running an executable file

Kaspersky Security Center can notify the administrator about events on client devices by running an executable file. The executable file must contain another executable file with placeholders of the event to be relayed to the administrator.

Table 45. Placeholders for describing an event

Placeholder	Placeholder description
%SEVERITY%	Event importance level
%COMPUTER%	Name of the device where the event occurred
%DOMAIN%	Domain
%EVENT%	Event
%DESCR%	Event description
%RISE_TIME%	Time created
%KLCSAK_EVENT_TASK_DISPLAY_NAME%	Task name
%KL_PRODUCT%	Kaspersky Security Center Network Agent
%KL_VERSION%	Network Agent version number
%HOST_IP%	IP address
%HOST_CONN_IP%	Connection IP address

Example

Event notifications are sent by an executable file (such as *script1.bat*) inside which another executable file (such as *script2.bat*) with the %COMPUTER% placeholder is launched. When an event occurs, the *script1.bat* file is run on the administrator's device, which, in turn, runs the *script2.bat* file with the %COMPUTER% placeholder. The administrator then receives the name of the device where the event occurred.

Configuring the interface

You can configure the Kaspersky Security Center interface:

- Show and hide objects in the console tree, workspace, and properties windows of objects (folders, sections), depending on the features being used.

- Show and hide elements of the main window (for example, console tree or standard menus such as **Actions** and **View**).
- *To configure the Kaspersky Security Center interface in accordance with the currently used set of features:*
1. In the console tree, select the **Administration Server** node.
 2. On the menu bar of the main application window, select **View** → **Configure interface**.
 3. In the **Configure interface** window that opens, configure the display of interface elements using the following check boxes:
 - **Display Vulnerability and Patch Management**

If this check box is selected, the **Remote installation** folder displays the **Deploy device images** subfolder, and the **Repositories** folder displays the **Hardware** subfolder.

This check box is cleared by default if the Quick Start Wizard has not finished. This check box is selected by default after the Quick Start Wizard has finished.
 - **Display data encryption and protection**

If this check box is selected, the console tree displays the **Data encryption and protection** folder.

By default, this check box is selected.
 - **Display endpoint control settings**

If this check box is selected, the following subsections are displayed in the **Security Controls** section of the properties window of the Kaspersky Endpoint Security for Windows policy:
 - **Application Control**
 - **Vulnerability Monitor**
 - **Device Control**
 - **Web Control**

If this check box is cleared, the above-specified subsections are not displayed in the **Security Controls** section.

By default, this check box is selected.
 - **Display Mobile Device Management**

If this check box is selected, the **Mobile Device Management** feature is available. After you restart the application, the console tree displays the **Mobile devices** folder.

By default, this check box is selected.
 - **Display secondary Administration Servers**

If the check box is selected, the console tree displays the nodes of secondary and virtual Administration Servers within administration groups. The features connected with secondary and virtual Administration Servers—for example, creation of tasks for remote installation of applications on secondary Administration Servers—are available at that.

By default, this check box is cleared.
 - **Display security settings sections**

If this check box is selected, the **Security** section is displayed in the properties window of Administration Server, administration groups and other objects. This check box allows

you to give users and user groups custom permissions for working with objects.

By default, this check box is cleared.

4. Click **OK**.

To apply some of the changes, you have to close the main application window and then open it again.

► *To configure the display of elements in the main application window:*

1. On the menu bar of the main application window, select **View** → **Configure**.
2. In the **Configure view** window that opens, configure the display of main window elements by using check boxes.
3. Click **OK**.

Discovering networked devices

This section describes steps you must take after the Kaspersky Security Center installation.

In this chapter

Scenario: Discovering networked devices	303
Unassigned devices.....	304
Equipment inventory	315

Scenario: Discovering networked devices

You must perform device discovery before installation of the security applications. When all networked devices are discovered, you can receive information about them and manage them through policies. Regular network polls are needed to discover if there are any new devices and whether previously discovered devices are still on the network.

Discovery of networked devices proceeds in stages:

a. Initial device discovery

The Quick Start Wizard guides you through initial device discovery (see section "Step 13. Device discovery" on page [277](#)), and helps you find networked devices such as computers, tablets, and mobile phones. You can also perform device discovery manually (see section "Device discovery" on page [304](#)).

b. Configuring future polls

Decide which type(s) of discovery (see section "Device discovery" on page [304](#)) you want to use regularly. Make sure that this type is enabled and that the poll schedule meets the needs of your organization. When configuring the poll schedule, use the recommendations for network polling frequency.

c. Setting up rules for adding discovered devices to administration groups (optional)

If new devices appear on your network, they are discovered during regular polls and are automatically included in the **Unassigned devices** group. If you want, you can set up the rules for automatically moving these devices (see section "Device moving rules" on page [401](#)) to the **Managed devices** group. You can also establish retention rules (see section "Configuring retention rules for unassigned devices" on page [311](#)).

If you skip this rule-setting stage, all the newly discovered devices go to the **Unassigned devices** group and stay there. If you want, you can move these devices to the **Managed devices** group manually. If you move the devices to the **Managed devices** group manually, you can analyze information about each device and decide whether you want to move it to an administration group, and, if so, to which group.

Results

Completion of the scenario yields the following:

- Kaspersky Security Center Administration Server discovers the devices that are on the network and provides you with information about them.
- Future polls are set up and are conducted according to the specified schedule.
- The newly discovered devices are arranged according to the configured rules. (Or, if no rules are configured, the devices stay in the **Unassigned devices** group).

See also:

Ports used by Kaspersky Security Center	65
Interaction of Kaspersky Security Center components and security applications: more information	108
Basic concepts.....	44
Architecture.....	58
Scenario: Installation and initial setup of Kaspersky Security Center 13 Web Console	962

Unassigned devices

This section provides information about how to manage devices on an enterprise network if they are not included in an administration group.

In this section

Device discovery.....	304
Working with Windows domains. Viewing and changing the domain settings	311
Configuring retention rules for unassigned devices	311
Working with IP ranges.....	312
Working with the Active Directory groups. Viewing and modifying group settings.....	313
Creating rules for moving devices to administration groups automatically	313
Using VDI dynamic mode on client devices	313

Device discovery

This section describes the types of device discovery available in Kaspersky Security Center and provides information using each type.

The Administration Server receives information about the structure of the network and devices on this network through regular polling. The information is recorded to the Administration Server database. Administration Server can use the following types of polling:

- **Windows network polling.** The Administration Server can perform two kinds of Windows network poll: quick and full. During a quick poll, the Administration Server only retrieves information from the list of the NetBIOS names of devices in all network domains and workgroups. During a full poll, more information is requested from each client device, such as operating system name, IP address, DNS name, and NetBIOS name. By default, both quick poll and full poll are enabled. Windows network polling may fail to discover devices, for example, if the ports UDP 137, UDP 138, TCP 139 are closed on the router or by the firewall.
- **Active Directory polling.** The Administration Server retrieves information about the Active Directory unit structure and about DNS names of the devices from Active Directory groups. By default, this type of polling is enabled. We recommend that you use Active Directory polling if you use Active directory; otherwise, the Administration Server does not discover any devices. If you use Active Directory but some of the networked devices are not listed as members, these devices cannot be discovered by Active Directory polling.
- **IP range polling.** The Administration Server polls the specified IP ranges using ICMP packets and compiles a complete set of data on devices within those IP ranges. By default, this type of polling is disabled. It is not recommended to use this type of polling if you use Windows network polling and/or Active Directory polling.

If you set up and enabled device moving rules (on page [401](#)), the newly discovered devices are automatically included in the **Managed devices** group. If no moving rules have been enabled, the newly discovered devices are automatically included in the **Unassigned devices** group.

You can modify device discovery settings for each type. For example, you may want to modify the polling schedule or to set whether to poll the entire Active Directory forest or only a specific domain.

See also:

Scenario: Discovering networked devices	303
Windows network polling.....	305
Active Directory polling.....	308
IP range polling	310

Windows network polling

About Windows network polling

During a quick poll, the Administration Server only retrieves information from the list of the NetBIOS names of devices in all network domains and workgroups. During a full poll, the following information is requested from each client device:

- Operating system name
- IP address
- DNS name
- NetBIOS name

Both quick polls and full polls require the following:

- Ports UDP 137/138, TCP 139, UDP 445, TCP 445 must be available in the network.
- The Microsoft Computer Browser service must be used, and the master browser computer must be enabled on the Administration Server.
- The Microsoft Computer Browser service must be used, and the master browser computer must be enabled on the client devices:
 - On at least one device, if the number of networked devices does not exceed 32.
 - On at least one device for each 32 networked devices.

The full poll can run only if the quick poll has run at least once.

Viewing and modifying the settings for Windows network polling

► *To modify the settings for the Windows network polling:*

1. In the console tree, in the **Device discovery** folder, select the **Domains** subfolder.

You can proceed from the **Unassigned devices** folder to the **Device discovery** folder by clicking the **Poll now** button.

In the workspace of the **Domains** subfolder, the list of the devices is displayed.

2. Click **Poll now**.

The domain properties window opens. If you want, modify the settings of Windows network polling:

- **Enable Windows network polling**

This option is selected by default. If you do not want to perform Windows network poll (for example, if you think that Active Directory polling is enough), you can unselect this option.

- **Set quick polling schedule**

The default period is 15 minutes.

During a quick poll, Kaspersky Security Center only retrieves information from the list of the NetBIOS names of devices in all network domains and work groups.

The data received at the next polling completely replaces the old data.

The following polling schedule options are available:

- **Every N days**

The polling runs regularly, with the specified interval in days, starting from the specified date and time.

By default, the polling runs every day, starting from the current system date and time.

- **Every N minutes**

The polling runs regularly, with the specified interval in minutes, starting from the specified time.

By default, the polling runs every five minutes, starting from the current system time.

- **By days of week**

The polling runs regularly, on the specified days of week, and at the specified time.

By default, the polling runs every Friday at 6:00:00 P.M.

- **Every month on specified days of selected weeks**

The polling runs regularly, on the specified days of each month, and at the specified time.

By default, no days of month are selected; the default start time is 6:00:00 P.M.

- **Run missed tasks**

If the Administration Server is switched off or unavailable during the time for which the poll is scheduled, the Administration Server can either start the poll immediately after it is switched on, or wait for the next time for which the poll scheduled.

If this option is enabled, the Administration Server starts polling immediately after it is switched on.

If this option is disabled, the Administration Server waits for the next time for which the polling is scheduled.

By default, this option is enabled.

- **Set full polling schedule**

The default period is one hour. The data received at the next polling completely replaces the old data.

The following polling schedule options are available:

- **Every N days**

The polling runs regularly, with the specified interval in days, starting from the specified date and time.

By default, the polling runs every day, starting from the current system date and time.

- **Every N minutes**

The polling runs regularly, with the specified interval in minutes, starting from the specified time.

By default, the polling runs every five minutes, starting from the current system time.

- **By days of week**

The polling runs regularly, on the specified days of week, and at the specified time.

By default, the polling runs every Friday at 6:00:00 P.M.

- **Every month on specified days of selected weeks**

The polling runs regularly, on the specified days of each month, and at the specified time.

By default, no days of month are selected; the default start time is 6:00:00 P.M.

- **Run missed tasks**

If the Administration Server is switched off or unavailable during the time for which the poll is scheduled, the Administration Server can either start the poll immediately after it is switched on, or wait for the next time for which the poll scheduled.

If this option is enabled, the Administration Server starts polling immediately after it is switched on.

If this option is disabled, the Administration Server waits for the next time for which the polling is scheduled.

By default, this option is enabled.

If you want to perform the poll immediately, click **Poll now**. Both types of polls will start.

On the virtual Administration Server you can view and edit the polling settings of the Windows network in the properties window of the distribution point, in the **Device discovery** section.

See also:

Working with Windows domains. Viewing and changing the domain settings[311](#)

Active Directory polling



Use Active Directory polling if you use Active Directory; otherwise, it is recommended to use other poll types. If you use Active Directory but some of the networked devices are not listed as members, these devices cannot be discovered by Active Directory polling.

Viewing and modifying the settings for Active Directory polling

► *To view and modify the settings for polling Active Directory groups:*

1. In the console tree, in the **Device discovery** folder, select the **Active Directory** subfolder.

Alternatively, you can proceed from the **Unassigned devices** folder to the **Device discovery** folder by clicking the **Poll now** button.

2. Click **Configure polling**.

The Active Directory properties window opens. If you want, modify the settings of Active Directory group polling:

- **Enable Active Directory polling**

This option is selected by default. However, if you do not use Active Directory, the poll does not retrieve any results. In this case, you can unselect this option.

- **Set polling schedule**

The default period is one hour. The data received at the next polling completely replaces the old data.

The following polling schedule options are available:

- **Every N days**

The polling runs regularly, with the specified interval in days, starting from the specified date and time.

By default, the polling runs every day, starting from the current system date and time.

- **Every N minutes**

The polling runs regularly, with the specified interval in minutes, starting from the specified time.

By default, the polling runs every five minutes, starting from the current system time.

- **By days of week**

The polling runs regularly, on the specified days of week, and at the specified time.

By default, the polling runs every Friday at 6:00:00 P.M.

- **Every month on specified days of selected weeks**

The polling runs regularly, on the specified days of each month, and at the specified time.

By default, no days of month are selected; the default start time is 6:00:00 P.M.

- **Run missed tasks**

If the Administration Server is switched off or unavailable during the time for which the poll is scheduled, the Administration Server can either start the poll immediately after it is switched on, or wait for the next time for which the poll scheduled.

If this option is enabled, the Administration Server starts polling immediately after it is switched on.

If this option is disabled, the Administration Server waits for the next time for which the polling is scheduled.

By default, this option is enabled.

- **Advanced**

You can select which Active Directory domains to poll:

- Active Directory domain to which the Kaspersky Security Center belongs.
- Domain forest to which the Kaspersky Security Center belongs.
- Specified list of Active Directory domains.

If you select this option, you can add domains to the polling scope:

- Click the **Add** button.
- In the corresponding fields, specify the address of the domain controller, the name and password of the account for accessing it.
- Click **OK** to save changes.

You can select the domain controller address on the list and click the **Modify** or **Remove** buttons to modify or remove it.

- Click **OK** to save changes.

If you want to perform the poll immediately, click the **Poll now** button.

On the virtual Administration Server, you can view and edit the polling settings of Active Directory groups in the properties window (see section "Network Agent policy settings" on page [665](#)) of the distribution point, in the **Device discovery** section.

IP range polling

The Administration Server polls the specified IP ranges using ICMP packets and compiles a complete set of data on devices within those IP ranges. By default, this type of polling is disabled. It is not recommended to use this type of polling if you use Windows network polling and/or Active Directory polling.

Viewing and modifying the settings for IP range polling

► *To view and modify the settings for polling IP range groups:*

1. In the console tree, in the **Device discovery** folder, select the **IP ranges** subfolder.

You can proceed from the **Unassigned devices** folder to the **Device discovery** folder by clicking **Poll now**.

2. If you want, in the **IP ranges** subfolder click **Add subnet** to add an IP range (see section "Working with IP ranges" on page [312](#)) for polling, and then click **OK**.
3. Click **Configure polling**.

The IP ranges properties window opens. If you want, you can modify the settings of IP range polling:

- **Enable IP range polling**

This option is not selected by default. It is not recommended to use this type of polling if you use Windows network polling and / or Active Directory polling.

- **Set polling schedule**

The default period is 420 minutes. The data received at the next polling completely replaces the old data.

The following polling schedule options are available:

- **Every N days**

The polling runs regularly, with the specified interval in days, starting from the specified date and time.

By default, the polling runs every day, starting from the current system date and time.

- **Every N minutes**

The polling runs regularly, with the specified interval in minutes, starting from the specified time.

By default, the polling runs every five minutes, starting from the current system time.

- **By days of week**

The polling runs regularly, on the specified days of week, and at the specified time.

By default, the polling runs every Friday at 6:00:00 P.M.

- **Every month on specified days of selected weeks**

The polling runs regularly, on the specified days of each month, and at the specified time.

By default, no days of month are selected; the default start time is 6:00:00 P.M.

- **Run missed tasks**

If the Administration Server is switched off or unavailable during the time for which the poll is scheduled, the Administration Server can either start the poll immediately after it is switched on, or wait for the next time for which the poll scheduled.

If this option is enabled, the Administration Server starts polling immediately after it is switched on.

If this option is disabled, the Administration Server waits for the next time for which the polling is scheduled.

By default, this option is enabled.

If you want to perform the poll immediately, click **Poll now**. This button is only available if you selected **Enable IP range polling**.

On the virtual Administration Server, you can view and edit the settings for IP range polling in the distribution point properties window (see section "Network Agent policy settings" on page 665), in the **Device discovery** section. Client devices discovered during the poll of IP ranges are displayed in the **Domains** folder of the virtual Administration Server.

Working with Windows domains. Viewing and changing the domain settings

► *To modify the domain settings:*

1. In the console tree, in the **Device discovery** folder, select the **Domains** subfolder.
2. Select a domain and open its properties window in one of the following ways:
 - By selecting **Properties** in the context menu of the domain.
 - By clicking the **Show group properties** link.

The **Properties: <Domain name>** window opens where you can configure the selected domain.

Configuring retention rules for unassigned devices

After Windows network polling is complete, the found devices are placed into subgroups of the Unassigned devices administration group. This administration group can be found at **Advanced** → **Device discovery** → **Domains**. The **Domains** folder is the parent group. It contains child groups named after the corresponding domains and workgroups that have been found during the network polling. The parent group may also contain the administration group of mobile devices. You can configure the retention rules of the unassigned devices for the parent group and for each of the child groups. The retention rules do not depend on the network polling settings and work even if the network polling is disabled.

► *To configure retention rules for unassigned devices:*

1. In the console tree, in the **Device discovery** folder, do one of the following:
 - To configure settings of the parent group, right-click the **Domains** subfolder and select **Properties**. The parent group properties window opens.
 - To configure settings of a child group, right-click its name and select **Properties**. The child group properties window opens.
2. In the **Devices** section, specify the following settings:

- **Remove the device from the group if it has been inactive for longer than (days)**

If this option is enabled, you can specify the time interval after which the device is automatically removed from the group. By default, this option is also distributed to the child groups. The default time interval is 7 days.

By default, this option is enabled.
- **Inherit from parent group**

If this option is enabled, the retention period for the devices in the current group is inherited from the parent group and cannot be changed.

This option is available only for child groups.

By default, this option is enabled.
- **Force inheritance in child groups**

The setting values will be distributed to child groups but in the properties of the child groups these settings are locked.

By default, this option is disabled.

Your changes are saved and applied.

See also:

Scenario: Discovering networked devices	303
---	---------------------

Working with IP ranges

You can customize existing IP ranges and create new ones.

In this section

Creating an IP range.....	312
Viewing and changing the IP range settings	313

Creating an IP range

► *To create an IP range:*

1. In the console tree, in the **Device discovery** folder, select the **IP ranges** subfolder.
2. In the context menu of the folder, select **New** → **IP range**.
3. In the **New IP range** window that opens, set up the new IP range.

The new IP range appears in the **IP ranges** folder.

Viewing and changing the IP range settings

► *To modify the IP range settings:*

1. In the console tree, in the **Device discovery** folder select the **IP ranges** subfolder.
2. Select an IP range and open its properties window in one of the following ways:
 - By selecting **Properties** in the context menu of the IP range.
 - By clicking the **Show group properties** link.

The **Properties: <IP range name>** window opens where you can configure the properties of the selected IP range.

Working with the Active Directory groups. Viewing and modifying group settings

► *To modify the settings for the Active Director group:*

1. In the console tree, in the **Device discovery** folder, select the **Active Directory** subfolder.
2. Select an Active Directory group and open its properties window in one of the following ways:
 - By selecting **Properties** in the context menu of the IP range.
 - By clicking the **Show group properties** link.

The **Properties: <Active Directory group name>** window opens where you can configure the selected Active Directory group.

Creating rules for moving devices to administration groups automatically

You can configure devices to be moved automatically to administration groups after they are discovered during a poll on an enterprise network.

► *To configure rules for moving devices to administration groups automatically:*

1. In the console tree, select the **Unassigned devices** folder.
2. In the workspace of this folder, click **Configure rules**.

This opens the **Properties: Unassigned devices**. In the **Move devices** section, configure the rules to move devices to administration groups automatically.

See also:

Scenario: Deployment for cloud environment.....	821
Synchronization with cloud.....	873

Using VDI dynamic mode on client devices

A virtual infrastructure can be deployed on a corporate network using temporary virtual machines. Kaspersky Security Center detects temporary virtual machines and adds information about them to the Administration Server

database. After a user finishes using a temporary virtual machine, the machine is removed from the virtual infrastructure. However, a record about the removed virtual machine can be saved in the database of the Administration Server. Also, nonexistent virtual machines can be displayed in Administration Console.

To prevent information about nonexistent virtual machines from being saved, Kaspersky Security Center supports dynamic mode for Virtual Desktop Infrastructure (VDI). The administrator can enable support of dynamic mode for VDI (see section "Enabling VDI dynamic mode in the properties of an installation package for Network Agent" on page [314](#)) in the properties of the installation package of Network Agent (see section "Network Agent installation package settings" on page [183](#)) to be installed on the temporary virtual machine (only Windows).

When a temporary virtual machine is disabled, Network Agent notifies the Administration Server that the machine has been disabled. If the virtual machine has been disabled successfully, it is removed from the list of devices connected to the Administration Server. If the virtual machine is disabled with errors and Network Agent does not send a notification about the disabled virtual machine to the Administration Server, a backup scenario is used. In this scenario, the virtual machine is removed from the list of devices connected to the Administration Server after three unsuccessful attempts to synchronize with the Administration Server.

In this section

Enabling VDI dynamic mode in the properties of an installation package for Network Agent	314
Searching for devices that are part of VDI.....	314
Moving devices from VDI to an administration group	315

Enabling VDI dynamic mode in the properties of an installation package for Network Agent

Using dynamic mode for Virtual Desktop Infrastructure (VDI) is available only for devices running Windows.

► To enable VDI dynamic mode:

1. In the **Remote installation** folder of the console tree, select the **Installation packages** subfolder.
2. In the context menu of the Network Agent installation package, select **Properties**.
The **Properties: Kaspersky Security Center Network Agent** window opens.
3. In the **Properties: Kaspersky Security Center Network Agent** window, select the **Advanced** section.
4. In the **Advanced** section, select the **Enable dynamic mode for VDI** check box.

The device on which Network Agent is to be installed will be a part of VDI.

Searching for devices that are part of VDI

► To find devices that make up part of VDI:

1. Select **Search** from the context menu of the **Unassigned devices** folder.
2. In the **Find devices** window, on the **Virtual machines** tab, in the **This is a virtual machine** drop-down list, select **Yes**.
3. Click the **Find now** button.

The application search for devices that make up part of Virtual Desktop Infrastructure.

Moving devices from VDI to an administration group

► *To move devices that are part of VDI to an administration group:*

1. In the workspace of the **Unassigned devices** folder, click **Configure rules**.
This opens the properties window of the **Unassigned devices** folder.
 2. In the properties window of the **Unassigned devices** folder, in the **Move devices** section, click the **Add** button.
The **New rule** window opens.
 3. In the **New rule** window, select the **Virtual machines** section.
 4. In the **This is a virtual machine** drop-down list, select **Yes**.
- A rule will be created for device relocation to an administration group.

Equipment inventory

The hardware list (**Repositories** → **Hardware**) that you use to inventory equipment is populated in two ways: automatically and manually. After each network polling, all detected computers are added to the list automatically; however, you can also add computers manually if you do not want to poll the network. You can add other devices to the list manually, for example, routers, printers, or computer hardware.

In the properties of a device, you can view and edit detailed information about that device.

The hardware list may contain the following types of devices:

- Computers
- Mobile devices
- Network devices
- Virtual devices
- OEM components
- Computer peripherals
- Connected devices
- VoIP phones
- Network repositories

The administrator can assign the "Enterprise equipment" attribute to detected devices. This attribute can be assigned manually in the properties of a device, or the administrator can specify criteria for the attribute to be assigned automatically. In this case, the "Enterprise equipment" attribute is assigned by device type.

Kaspersky Security Center allows writing off equipment. To do this, select the **Device is written off** check box in the properties of a device. The device is not displayed on the equipment list.

An administrator can manage the list of programmable logic controllers (PLC) in the **Hardware** folder. Detailed information on managing the PLC list is provided in the *Kaspersky Industrial CyberSecurity for Nodes User Guide*.

In this section

Adding information about new devices	316
Configuring criteria used to define enterprise devices	316
Configuring custom fields	317

Adding information about new devices

► *To add information about new devices on the network:*

1. In the **Repositories** folder of the console tree, select the **Hardware** subfolder.
2. In the workspace of the **Hardware** folder, click the **Add device** button to open the **New device** window.
The **New device** window opens.
3. In the **New device** window, in the **Type** drop-down list select a device type that you want to add.
4. Click **OK**.
The device properties window opens on the **General** section.
5. In the **General** section, fill in the entry fields with data on the device. The **General** section lists the following settings:
 - **Enterprise device.** Select the check box if you want to assign the "Enterprise" attribute to the device. Using this attribute, you can search for devices in the **Hardware** folder.
 - **Device is written off.** Select the check box if you do not want the device to be displayed in the list of devices in the **Hardware** folder.
6. Click **Apply**.
The new device will be displayed in the workspace of the **Hardware** folder.

Configuring criteria used to define enterprise devices

► *To configure criteria of detection for enterprise devices:*

1. In the **Repositories** folder of the console tree, select the **Hardware** subfolder.
2. In the workspace of the **Hardware** folder, click the **Additional actions** button and select **Set up rule for Enterprise devices** in the drop-down list.
The hardware properties window opens.
3. In the hardware properties window, in the **Enterprise devices** section, select a method for assigning the "Enterprise" attribute to the device:
 - **Set the Enterprise device attribute manually for the device.** The "Enterprise hardware" attribute is assigned to the device manually in the device properties window, in the **General** section.
 - **Set the Enterprise device attribute automatically for the device.** In the **By device type** block of settings, specify device types to which the application will automatically assign the "Enterprise" attribute.
4. Click **OK**.

Configuring custom fields

► *To configure custom fields of devices:*

1. In the **Repositories** folder of the console tree, select the **Hardware** subfolder.
2. In the workspace of the **Hardware** folder, click the **Additional actions** button and select **Configure custom data fields** in the drop-down list.

The hardware properties window opens.

3. In the hardware properties window, select the **Custom fields** section and click the **Add** button.

The **Add field** window opens.

4. In the **Add field** window, specify the name of the custom field that will be displayed in the hardware properties.

You can create multiple custom fields with unique names.

5. Click **OK**.

The custom fields that have been added are displayed in the **Custom fields** section of the hardware properties. You can use custom fields to provide specific information about devices. For example, this could be the internal order number for a hardware purchase.

Licensing

This section provides information about general concepts related to Kaspersky Security Center 13 licensing.

See also:

Kaspersky applications: licensing and activation	357
Step 3. Selecting the application activation method	267
About the End User License Agreement	318
About the license	319
About the license certificate.....	319
About the license key.....	320
Kaspersky Security Center licensing options	320
About restrictions on the main functionality	322
About the activation code	323
About the key file	323
About data provision	324
About the subscription	328
Events of the licensing limit exceeded.....	329
Licensing features of Kaspersky Security Center and managed applications	329
Revoking consent with End User License Agreement	331

About the End User License Agreement

The *End User License Agreement* (License Agreement or EULA) is a binding agreement between you and AO Kaspersky Lab stipulating the terms under which you may use the application.

Carefully read the License Agreement before you start using the application.

Kaspersky Security Center and its components, for example, Network Agent, have their own EULA.

You can view the terms of the End User License Agreement for Kaspersky Security Center using the following methods:

- During installation of Kaspersky Security Center.
- By reading the license.txt document included in the Kaspersky Security Center distribution kit.
- By reading the license.txt document in the Kaspersky Security Center installation folder.

You can view the terms of the End User License Agreement for Network Agent for Windows, Network Agent for Mac, Network Agent for Linux using the following methods:

- During downloading of Network Agent distribution package from the Kaspersky web servers.
- During installation of Network Agent for Windows, Network Agent for Mac, Network Agent for Linux.

- By reading the license.txt document included in the Network Agent for Windows, Network Agent for Mac, Network Agent for Linux distribution package.
- By reading the license.txt document in the Network Agent for Windows, Network Agent for Mac, Network Agent for Linux installation folder.

You accept the terms of the End User License Agreement by confirming that you agree with the End User License Agreement when installing the application. If you do not accept the terms of the License Agreement, cancel the application installation and do not use the application.

About the license

A *license* is a time-limited right to use the application, granted under the terms of the End User License Agreement.

A license entitles you to the following kinds of services:

- Use of the application in accordance with the terms of the End User License Agreement
- Getting technical support

The scope of services and validity period depend on the type of license under which the application was activated.

The following license types are provided:

- *Trial* – a free license intended for trying out the application.

A trial license usually has a short term. When the trial license expires, all Kaspersky Security Center features become disabled. To continue using the application, you need to purchase the commercial license.

You can activate the application under the trial license only once.

- *Commercial* – a paid license granted upon purchase of the application.

When the commercial license expires, the application continues running with limited functionality (for example, Kaspersky Security Center database updates are not available). To continue using all the features of Kaspersky Security Center, you must renew your commercial license.

We recommend renewing the license before its expiration to ensure maximum protection against all security threats.

About the license certificate

A *license certificate* is a document that you receive along with a key file or an activation code.

A license certificate contains the following information about the license provided:

- License key or order number
- Information about the user who has been granted the license
- Information about the application that can be activated under the license provided
- Limit of the number of licensing units (e.g., devices on which the application can be used under the license provided)
- License validity start date
- License expiration date or license term

- License type

About the license key

A *license key* is a sequence of bits that you can apply to activate and then use the application in accordance with the terms of the End User License Agreement. License keys are generated by Kaspersky specialists.

You can add a license key to the application using one of the following methods: by applying a *key file* or by entering an *activation code*. The license key is displayed in the application interface as a unique alphanumeric sequence after you add it to the application.

The license key may be blocked by Kaspersky in case the terms of the License Agreement have been violated. If the license key has been blocked, you need to add another one if you want to use the application.

A license key may be active or additional (or reserve).

An *active license key* is a license key that is currently used by the application. An active license key can be added for a trial or commercial license. The application cannot have more than one active license key.

An *additional (or reserve) license key* is a license key that entitles the user to use the application, but is not currently in use. The additional license key automatically becomes active when the license associated with the current active license key expires. An additional license key can be added only if an active license key has already been added.

A license key for a trial license can be added as an active license key. A license key for a trial license cannot be added as an additional license key.

Kaspersky Security Center licensing options

In Kaspersky Security Center, the license can apply to different groups of functionality.

When adding a license key in the Administration Server properties window, ensure that you add a license key that lets you use Kaspersky Security Center. You can find this information at the Kaspersky website. Each solution webpage contains the list of applications included in this solution. Administration Server may accept unsupported license keys, for example a license key for Kaspersky Endpoint Security Cloud, but the functionality of Kaspersky Security Center in such cases is not supported.

Basic functionality of Administration Console

The following functions are available:

- Creation of virtual Administration Servers that are used to administer a network of remote offices or client organizations.
- Creation of a hierarchy of administration groups to manage specific devices as a single entity.
- Control of the anti-virus security status of an organization.
- Remote installation of applications.
- Viewing the list of operating system images available for remote installation.
- Centralized configuration of applications installed on client devices.
- Viewing and editing existing licensed applications groups.
- Statistics and reports on the application's operation, as well as notifications about critical events.

- Encryption and data protection management.
- Viewing and manual editing of the list of hardware components detected by polling the network.
- Centralized operations with files that were moved to Quarantine or Backup and files whose processing was postponed.
- Management of user roles.

Kaspersky Security Center with support of the basic functionality of Administration Console is delivered as a part of Kaspersky applications for protection of corporate networks. You can also download it from Kaspersky website.

Before the application is activated or after the commercial license expires, Kaspersky Security Center provides only the basic functionality of Administration Console (see section "About restrictions on the main functionality" on page [322](#)).

Vulnerability and Patch Management feature

The following functions are available:

- Remote installation of operating systems.
- Remote installation of software updates, scanning and fixing of vulnerabilities.
- Hardware inventory.
- Licensed applications group management.
- Remote permission of connection to client devices through a component of Microsoft® Windows® named Remote Desktop Connection.
- Remote connection to client devices through Windows Desktop Sharing.

The management unit for Vulnerability and Patch Management is a client device in the Managed devices group.

Detailed information about devices' hardware is available during the inventory process as part of Vulnerability and Patch Management.

For a proper functioning of Vulnerability and Patch Management, at least 100 GB free disk space must be available.

Mobile Device Management feature

The Mobile Device Management feature is used to manage Exchange ActiveSync (EAS) and iOS MDM mobile devices.

The following functions are available for Exchange ActiveSync mobile devices:

- Creation and editing of mobile device management profiles, assignment of profiles to users' mailboxes.
- Configuration of mobile devices (email synchronization, apps usage, user password, data encryption, connection of removable drives).
- Installation of certificates on mobile devices.

The following functions are available for iOS MDM devices:

- Creating and editing configuration profiles, and installing configuration profiles on mobile devices.
- Installing applications on mobile devices through App Store® or using manifest files (.plist).
- Locking mobile devices, resetting the mobile device password, and deleting all data from the mobile device.

In addition, Mobile Devices Management allows executing commands provided by relevant protocols.

The management unit for Mobile Devices Management is a mobile device. A mobile device is considered to be managed after it is connected to the Mobile Devices Server.

See also:

Scenario: Installation and initial setup of Kaspersky Security Center 13 Web Console[962](#)

About restrictions on the main functionality

Before the application is activated or after the commercial license expires, Kaspersky Security Center provides only the basic functionality of Administration Console. The limitations of this basic application operation are described below.

Mobile Device Management

You cannot create a new profile and assign it to a mobile device (iOS MDM) or to a mailbox (Exchange ActiveSync). Changes to existing profiles and assignment of profiles to mailboxes are always available.

Managing applications

You cannot run the update installation task and the update removal task. All tasks that started before the license expired will be completed, but the latest updates will not be installed. For example, if the critical update installation task was started before the license expired, only critical updates found before the license expiration will be installed.

Launch and editing of the synchronization, vulnerability scan, and vulnerabilities database update tasks are always available. Also, there are no limitations on viewing, searching, or sorting of entries in the list of vulnerabilities and updates.

Remote installation of operating systems and applications

Tasks for capturing and installing an operating system image cannot be run. Tasks that were started before the license expired will be completed.

Hardware inventory

Information about new devices cannot be retrieved through Mobile Device Server. Information about computers and connected devices is kept updated.

Notifications are not sent about changes in the configuration of devices.

The equipment list is available for viewing and editing manually.

Licensed applications group management

You cannot add a new license key.

Notifications are not sent about violations of license key usage restrictions.

Remote connection to client devices

Remote connection to client devices is not available.

Anti-virus security

Anti-Virus uses databases that were installed before the license expired.

Integration with cloud environments

When working in a cloud environment, you cannot use AWS, Azure, or Google API tools for cloud segment polling and installation of applications on devices. Interface elements that display functions specific for working in a cloud environment are also not available.

About the activation code

Activation code is a unique sequence of 20 alphanumeric characters. You enter an activation code to add a license key that activates Kaspersky Security Center. You receive the activation code through the email address that you specified after purchasing Kaspersky Security Center or after ordering the trial version of Kaspersky Security Center.

To activate the application with an activation code, you need Internet access to establish connection with Kaspersky activation servers.

If the application was activated with an activation code, the application in some cases sends regular requests to Kaspersky activation servers in order to check the current status of the license key. You must provide the application Internet access to make it possible to send requests.

If you lost your activation code after you activated the application, it can be restored. You may need your activation code, for example, to register with Kaspersky CompanyAccount. To restore the activation code, you must contact the Kaspersky Technical Support (see section "How to get technical support" on page [1401](#)).

You cannot use key files for activating managed applications; only activation codes are accepted.

About the key file

A *key file* is a file with the .key extension provided to you by Kaspersky. Key files are designed to activate the application by adding a license key.

You receive a key file at the email address that you provided when you bought Kaspersky Security Center or ordered the trial version of Kaspersky Security Center.

You do not need to connect to Kaspersky activation servers in order to activate the application with a key file.

You can restore a key file if it has been accidentally deleted. You may need a key file to register a Kaspersky CompanyAccount, for example.

To restore your key file, perform any of the following actions:

- Contact the license seller.

- Receive a key file through Kaspersky website (<https://keyfile.kaspersky.com/en/>) by using your available activation code.

About data provision

Data transferred to third parties

When using the mobile device management functionality of the Software, for the purpose of timely delivery of commands to devices running the Android operating system through the push notification mechanism the Google Firebase Cloud Messaging service is used. If the User has configured the usage of the Google Firebase Cloud Messaging service, the User accepts to provide the following information to the Google Firebase Cloud Messaging service in automatic mode: installation IDs of the Kaspersky Endpoint Security for Android applications to which push notifications must be sent.

To block exchange of information with the Google Firebase Cloud Messaging service, the User must roll back the usage settings of the Google Firebase Cloud Messaging service to their factory values.

When using the mobile device management functionality of the Software, for the purpose of timely delivery of commands to devices running the iOS operating system through the push notification mechanism the Apple Push Notification Service (APNs) is used. If the User has installed an APNs certificate on an iOS MDM Server, created an iOS MDM profile with a collection of settings for connection of iOS mobile devices to the Software, and installed this profile on mobile devices, the User agrees to provide the following information to APNs in automatic mode:

- Token—Push token of the device. The server uses this token when sending push notifications to the device.
- PushMagic—String that must be included in the push notification. The string value is generated by the device.

Data processed locally

Kaspersky Security Center is designed for centralized execution of basic administration and maintenance tasks on an organization's network. Kaspersky Security Center provides the administrator with access to detailed information about the organization's network security level; Kaspersky Security Center lets the administrator configure all the components of protection based on Kaspersky applications. Kaspersky Security Center performs the following main functions:

- Detecting devices and their users on the organization's network
- Creating a hierarchy of administration groups for device management
- Installing Kaspersky applications on devices
- Managing the settings and tasks of installed applications
- Managing the updates for Kaspersky and third-party applications, and finding and fixing vulnerabilities
- Activating Kaspersky applications on devices
- Managing user accounts
- Viewing information about the operation of Kaspersky applications on devices
- Viewing reports

To perform its main functions Kaspersky Security Center can receive, store, and process the following information:

- Information about the devices on the organization's network received as a result of device discovery on the Active Directory network or Windows network, or through scanning of IP intervals. Administration Server gets data independently or receives data from Network Agent.

- Information about the Active Directory organizational units, domains, users, and groups received as a result of device discovery on the Active Directory network. Administration Server gets data independently or receives data from Network Agent.
- Details of managed devices. Network Agent transfers the data listed below from the device to Administration Server. The user enters the display name and description of the device in the Administration Console interface or Kaspersky Security Center 13 Web Console interface:
 - Technical specifications of the managed device and its components required for device identification: device display name and description, Windows domain name and type, device name in Windows environment, DNS domain and DNS name, IP address, network location, MAC address, operating system type, whether the device is a virtual machine together with hypervisor type, and whether the device is a dynamic virtual machine as part of VDI.
 - Other specifications of managed devices and their components required for audit of managed devices and for making decisions about whether specific patches and updates are applicable: Windows Update Agent (WUA) status, operating system architecture, operating system vendor, operating system build number, operating system release ID, operating system location folder, if the device is a virtual machine—the virtual machine type.
 - Details of actions on managed devices: date and time of the last update, time the device was last visible on the network, restart waiting status, and time the device was turned on.
 - Details of device user accounts and their work sessions.
- Distribution point operation statistics if the device is a distribution point. Network Agent transfers data from the device to Administration Server.
- Details of mobile devices transferred by using the Exchange ActiveSync protocol. The data listed below are transferred from the mobile device to Administration Server:
 - Technical specifications of the mobile device and its components required for device identification: device name, model, operating system name, IMEI number, and phone number.
 - Specifications of the mobile device and its components: device management status, support of SMS, permission to send SMS messages, support of FCM, support of user commands, operating system storage folder, and device name.
 - Details of actions on mobile devices: device location (through the Locate command), time of last synchronization, time of last connection to the Administration Server, and synchronization support details.
- Details of mobile devices transferred by using the iOS MDM protocol. The data listed below are transferred from the mobile device to Administration Server:
 - Technical specifications of the mobile device and its components required for device identification: device name, model, operating system name and build number, device model number, IMEI number, UDID, MEID, serial number, amount of memory, modem firmware version, Bluetooth MAC address, Wi-Fi MAC address, and SIM card details (ICCID as part of the SIM card ID).
 - Details of the mobile network used by the managed device: mobile network type, name of the currently used mobile network, name of the home mobile network, version of the mobile network operator settings, voice roaming and data roaming status, country code of the home network, residence country code, country code of the currently used network, and encryption level.
 - Security settings of the mobile device: use of a password and its compliance with the policy settings, list of configuration profiles and provisioning profiles used for installation of third-party applications.
 - Date of last synchronization with Administration Server and device management status.

- Details of Kaspersky applications installed on the device. The managed application transfers data from the device to Administration Server through Network Agent:
 - Settings of Kaspersky applications installed on the managed device: Kaspersky application name and version, status, real-time protection status, last device scan date and time, number of threats detected, number of objects that failed to be disinfected, availability and status of the application components, time of last update and version of anti-virus databases, details of Kaspersky application settings and tasks, information about the active and reserve license key, application installation date and ID.
 - Application operation statistics: events related to the changes in the status of Kaspersky application components on the managed device and to the performance of tasks initiated by the application components.
 - Device status defined by the Kaspersky application.
 - Tags assigned by the Kaspersky application.
 - Set of installed and applicable updates for the Kaspersky application.
- Data contained in events from Kaspersky Security Center components and Kaspersky managed applications. Network Agent transfers data from the device to Administration Server.
- Settings of Kaspersky Security Center components and Kaspersky managed applications presented in policies and policy profiles. The User enters data in the Administration Console or Kaspersky Security Center 13 Web Console interface.
- Task settings of Kaspersky Security Center components and Kaspersky managed applications. The User enters data in the Administration Console or Kaspersky Security Center 13 Web Console interface.
- Data processed by the Vulnerability and Patch Management feature. Network Agent transfers the data listed below from the device to Administration Server:
 - Details of applications and patches installed on managed devices (Applications registry).
 - Information about the hardware detected on managed devices (Hardware registry).
 - Details of vulnerabilities in third-party software detected on managed devices.
 - Details of updates available for third-party applications installed on managed devices.
 - Details of Microsoft updates found by the WSUS feature.
 - List of Microsoft updates found by the WSUS feature that must be installed on the device.
- User categories of applications. The User enters data in the Administration Console or Kaspersky Security Center 13 Web Console interface.
- Details of executable files detected on managed devices by the Application Control feature. The User enters data in the Administration Console or Kaspersky Security Center 13 Web Console interface. A complete list of data is provided in the Help files of the corresponding application.
- Details of files placed in Backup. The managed application transfers data from the device to Administration Server through Network Agent. A complete list of data is provided in the Help files of the corresponding application.
- Details of files placed in Quarantine. The managed application transfers data from the device to Administration Server through Network Agent. A complete list of data is provided in the Help files of the corresponding application.
- Details of files requested by Kaspersky specialists for detailed analysis. The managed application transfers data from the device to Administration Server through Network Agent. A complete list of data is provided in the Help files of the corresponding application.

- Details of the status and triggering of Adaptive Anomaly Control rules. The managed application transfers data from the device to Administration Server through Network Agent. A complete list of data is provided in the Help files of the corresponding application.
- Details of external devices (memory units, information transfer tools, information hardcopy tools, and connection buses) installed or connected to the managed device and detected by the Device Control feature. The managed application transfers data from the device to Administration Server through Network Agent. A complete list of data is provided in the Help files of the corresponding application.
- Information about encrypted devices and the encryption status. The managed application transfers data from the device to Administration Server through Network Agent.
- Details of data encryption errors on devices performed using the Data encryption feature of Kaspersky applications. The managed application transfers data from the device to Administration Server through Network Agent. A complete list of data is provided in the Help files of the corresponding application.
- List of managed programmable logic controllers (PLCs). The managed application transfers data from the device to Administration Server through Network Agent. A complete list of data is provided in the Help files of the corresponding application.
- Data required for creation of a threat development chain. The managed application transfers data from the device to Administration Server through Network Agent. A complete list of data is provided in the Help files of the corresponding application.
- Data required for Kaspersky Security Center integration with the Kaspersky Managed Detection and Response service (the dedicated plug-in must be installed for Kaspersky Security Center 13 Web Console): integration initiation token, integration token, and user session token. The User enters the integration initiation token in the Kaspersky Security Center 13 Web Console interface. The Kaspersky MDR service transfers the integration token and the user session token through the dedicated plug-in.
- Details of the entered activation codes or specified key files. The User enters data in the Administration Console or Kaspersky Security Center 13 Web Console interface.
- User accounts: name, description, full name, email address, main phone number, password, secret key generated by Administration Server, and one-time password for two-step verification. The User enters data in the Administration Console or Kaspersky Security Center 13 Web Console interface.
- Revision history of management objects. The User enters data in the Administration Console or Kaspersky Security Center 13 Web Console interface.
- Registry of deleted management objects. The User enters data in the Administration Console or Kaspersky Security Center 13 Web Console interface.
- Installation packages created from the file, as well as installation settings. The User enters data in the Administration Console or Kaspersky Security Center 13 Web Console interface.
- Data required for the display of announcements from Kaspersky in Kaspersky Security Center 13 Web Console. The User enters data in the Administration Console or Kaspersky Security Center 13 Web Console interface.
- Data required for the functioning of plug-ins of managed applications in Kaspersky Security Center 13 Web Console and saved by the plug-ins in the Administration Server database during their routine operation. The description and ways of providing the data are provided in the Help files of the corresponding application.
- Kaspersky Security Center 13 Web Console user settings: localization language and theme of the interface, Monitoring panel display settings, information about the status of notifications (Already read / Not yet read), status of columns in spreadsheets (Show / Hide), Training mode progress. The User enters data in the Kaspersky Security Center 13 Web Console interface.

- Kaspersky Event Log for Kaspersky Security Center components and Kaspersky managed applications. Kaspersky Event Log is stored on each device and is never transferred to Administration Server.
- Certificate for secure connection of managed devices to the Kaspersky Security Center components. The User enters data in the Administration Console or Kaspersky Security Center 13 Web Console interface.
- Data required for the Kaspersky Security Center operation in cloud environments, such as Amazon Web Services (AWS), Microsoft Azure, Google Cloud, and Yandex.Cloud. Administration Server receives the data from the virtual machine on which it runs.
- Information about the User's acceptance of the terms and conditions of legal agreements with Kaspersky.
- Any data that the User enters in the Administration Console or Kaspersky Security Center 13 Web Console interface.

The data listed above can be present in Kaspersky Security Center if one of the following methods is applied:

- The User enters data in the Administration Console or Kaspersky Security Center 13 Web Console interface.
- Network Agent automatically receives data from the device and transfers it to Administration Server.
- Network Agent receives data retrieved by the Kaspersky managed application and transfers it to Administration Server. The lists of data processed by Kaspersky managed applications are provided in the Help files for the corresponding applications.
- Administration Server and Network Agent assigned a distribution point receive information about the networked devices.
- Data is transferred from the mobile device to Administration Server by using the Exchange ActiveSync or iOS MDM protocol.

The listed data is stored in the Administration Server database. User names and passwords are stored in encrypted form.

All data listed above can be transferred to Kaspersky only through dump files, trace files, or log files of Kaspersky Security Center components, including log files created by installers and utilities.

Dump files, trace files, and log files of Kaspersky Security Center components contain random data of Administration Server, Network Agent, Administration Console, iOS MDM Server, Exchange Mobile Device Server, and Kaspersky Security Center 13 Web Console. These files can contain personal details and sensitive data. Dump files, trace files, and log files are stored on the device in non-encrypted form. Dump files, trace files, and log files are not transferred to Kaspersky automatically; however, the administrator can transfer data to Kaspersky manually upon request by Technical Support to resolve issues in the Kaspersky Security Center operation.

Kaspersky uses the received data in anonymized form and for general statistics only. Summary statistics are generated automatically from the originally received information and do not contain any personal or confidential data. As soon as new data is accumulated, the previous data is wiped (once a year). Summary statistics are stored indefinitely.

Kaspersky protects any information received in accordance with law and applicable Kaspersky rules. Data is transmitted over a secure channel.

About the subscription

Subscription to Kaspersky Security Center is an order for use of the application under the selected settings (subscription expiration date, number of protected devices). You can register your subscription to Kaspersky

Security Center with your service provider (for example, your Internet provider). A subscription can be renewed manually or in automatic mode; also, you can cancel it.

A subscription can be limited (for example, one-year) or unlimited (with no expiration date). To continue using Kaspersky Security Center after a limited subscription expires, you must renew it. An unlimited subscription is renewed automatically if it has been prepaid to the service provider in due dates.

When a limited subscription expires, you may be provided a grace period for renewal during which the application continues to function. The availability and duration of the grace period is defined by the service provider.

To use Kaspersky Security Center under subscription, you must apply the activation code received from the service provider.

You can apply a different activation code for Kaspersky Security Center only after your subscription expires or when you cancel it.

Depending on the service provider, the set of possible actions for subscription management may vary. The service provider might not provide a grace period for subscription renewal and so the application loses its functionality.

Activation codes purchased under subscription cannot be used for activating earlier versions of Kaspersky Security Center.

When the application is used under subscription, Kaspersky Security Center automatically attempts to access the activation server at specified time intervals until the subscription expires. You can renew your subscription on the service provider's website.

Events of the licensing limit exceeded

Kaspersky Security Center allows you to get information about events when some licensing limits are exceeded by Kaspersky applications installed on client devices.

The importance level of such events when a licensing restriction is exceeded is defined according to the following rules:

- If the currently used units covered by a single license constitute 90% to 100% of the total number of units covered by the license, the event is published with the **Info** importance level.
- If the currently used units covered by a single license constitute 100% to 110% of the total number of units covered by the license, the event is published with the **Warning** importance level.
- If the number of currently used units covered by a single license exceeds 110% of the total number of units covered by the license, the event is published with the **Critical event** importance level.

See also:

| Adjusting the general settings of Administration Server[609](#)

Licensing features of Kaspersky Security Center and managed applications

Licensing of Administration Server and managed applications involves the following:

- You can add license key or valid activation code (see section "Kaspersky applications: licensing and activation" on page [357](#)) to an Administration Server to activate Vulnerability and Patch Management, Mobile Device Management, or Integration with the SIEM systems. Some features of Kaspersky Security Center are only accessible depending on active key files or valid activation codes added to the Administration Server.
- You can add multiple activation codes and key files for managed applications (see section "Adding a license key to the Administration Server repository" on page [360](#)) to the Administration Server repository.

About Kaspersky Security Center licensing

If you activated one of the licensed features (for example, Mobile Device Management) using a key file, but you also want to use another licensed feature (for example, Vulnerability and Patch Management), you must purchase from your service provider a key file that activates both these features and you must activate Administration Server by using this key file.

Licensing features of managed applications

For licensing of managed applications, an activation code or key file can be deployed automatically or in any other convenient way. The following methods can be applied to deploy an activation code or key file:

- Automatic deployment

If you use different managed applications and you have to deploy a specific key file or activation code to devices, opt for other ways of deploying that activation code or key file.

Kaspersky Security Center allows you to automatically deploy available license keys to devices. For example, three license keys are stored in the Administration Server repository. You have selected the **Automatically distribute license key to managed devices** check box for all three license keys. A Kaspersky security application—for example, Kaspersky Endpoint Security for Windows—is installed on the organization's devices. A new device is discovered to which a license key must be deployed. The application determines, for instance, that two of the license keys from the repository can be applied to the device: license key named *Key_1* and license key named *Key_2*. One of these license keys is deployed to the device. In this case, it cannot be predicted which of the two license keys will be deployed to the device because automatic deployment of license keys does not provide for any administrator activity.

When a license key is deployed, the devices are recounted for that license key. You must make sure that the number of devices to which the license key was deployed does not exceed the license limit. If the number of devices exceeds the license limit, all devices that were not covered by the license will be assigned *Critical* status.

- Adding a key file or activation code to the installation package of a managed application

If you install a managed application using an installation package, you can specify an activation code or key file in this installation package or in the policy of the application. The license key will be deployed to managed devices at the next synchronization of the device with the Administration Server.

- Deployment through the add license key task for a managed application

If you opt for using the add license key task for a managed application, you can select the license key that must be deployed to devices and select the devices in any convenient way—for example, by selecting an administration group or a device selection.

- Adding an activation code or a key file manually to the devices

Revoking consent with End User License Agreement

If you decide to stop protection of your client devices, you can uninstall managed Kaspersky applications and revoke your End User License Agreement (EULA) for these applications.

► *To revoke a EULA for managed Kaspersky applications:*

1. In the console tree, select **Administration Server** → **Advanced** → **Accepted EULAs**.

A list of EULAs—accepted upon creation of installation packages, at the seamless installation of updates, or upon deployment of Kaspersky Security for Mobile—is displayed.

2. In the list, select the EULA which agreement you want to revoke.

You can view the following properties of the EULA:

- Date when the EULA was accepted.
- The name of the user who accepted the EULA.
- Link to the terms of the EULA.
- List of the objects that are connected to the EULA: names of installation packages, names of seamless updates, names of mobile apps.

3. Click the **Revoke EULA** button.

In the window that opens, you are informed that you must uninstall Kaspersky application corresponding to the EULA.

4. Click the button to confirm the revoke.

Kaspersky Security Center checks whether the installation packages (corresponding to the managed Kaspersky application whose EULA you want to revoke) are deleted.

You can revoke only the EULA for a managed Kaspersky application, whose installation packages are deleted.

The EULA is revoked. It is not displayed in the list of EULAs in the **Administration Server** → **Advanced** → **Accepted EULAs** section. You cannot protect client devices using a Kaspersky application whose EULA you have revoked.

Kaspersky applications. Centralized deployment

This section describes the methods for remote installation of Kaspersky applications and their removal from networked devices.

Before deploying applications on client devices, make sure that the hardware and software of client devices meets the applicable requirements.

Network Agent is a component that provides for Administration Server connection with client devices. Therefore, it must be installed on each client device to be connected to the remote centralized control system. The device on which the Administration Server is installed can only use the server version of Network Agent. This version is included in Administration Server as a part that is installed and removed together with it. There is no need to install Network Agent on that device.

Network Agent can be installed remotely or locally like any application. During centralized deployment of security applications through Administration Console, you can install Network Agent jointly with security applications.

Network Agents can differ depending upon the Kaspersky applications with which they work. In some cases, Network Agent can be installed locally only (for details please refer to the documentation for the corresponding applications). You only have to install Network Agent on a client device once.

Kaspersky applications (see section "List of supported Kaspersky applications" on page [41](#)) are managed through Administration Console by using management plug-ins. Therefore, to access the application management interface through Kaspersky Security Center, the corresponding management plug-in must be installed on the administrator's workstation.

You can perform remote installation of applications from the administrator's workstation in the Kaspersky Security Center main window.

To install software remotely, you must create a remote installation task.

The created task for remote installation will start according to its schedule. You can interrupt the installation procedure by stopping the task manually.

If remote installation of an application returns an error, you can find the cause of this error and fix it using the remote installation preparation utility (see section "Preparing a device for remote installation. Utility tool riprep.exe" on page [353](#)).

You can track the progress of remote installation of Kaspersky applications on a network using the deployment report.

For details about management of the listed applications in Kaspersky Security Center, please refer to the documentation for the corresponding applications.

In this chapter

Replacing third-party security applications	333
Installing applications using a remote installation task.....	334
Installing applications using Remote Installation Wizard.....	338
Viewing a protection deployment report	342
Remote removal of applications	342
Working with installation packages.....	344
Receiving up-to-date versions of applications	351
Preparing a device for remote installation. Utility tool riprep.exe	353
Preparing a Linux device for remote installation of Network Agent.....	355
Preparing a macOS device for remote installation of Network Agent	356

Replacing third-party security applications

Installation of Kaspersky security applications through Kaspersky Security Center may require removal of third-party software incompatible with the application being installed. Kaspersky Security Center provides several ways of removing the third-party applications.

Removing incompatible applications by using the installer

This option is available in Microsoft Management Console-based Administration Console only.

The installer method of removing incompatible applications is supported by various types of installation. Before the security application installation, all incompatible applications are removed automatically if the properties window of the installation package of this security application (**Incompatible applications** section) has the **Uninstall incompatible applications automatically** check box selected.

Removing incompatible applications when configuring remote installation of an application

You can enable the **Uninstall incompatible applications automatically** option when you configure remote installation of a security application. In Microsoft Management Console (MMC) based Administration Console, this option is available in the Remote Installation Wizard. In Kaspersky Security Center 13 Web Console, you can find this option in the Protection Deployment Wizard. When this option is enabled, Kaspersky Security Center removes incompatible applications before installing a security application on a managed device.

How-to instructions:

- Administration Console: Installing applications using Remote Installation Wizard (on page [338](#))
or
- Kaspersky Security Center 13 Web Console: Removing incompatible applications before installation (see section "Step 7. Removing incompatible applications before installation" on page [1005](#))

Removing incompatible applications through a dedicated task

To remove incompatible applications, use the **Uninstall application remotely** task. This task should be run on devices before the security application installation task. For example, in the installation task you can select **On completing another task** as the schedule type where the other task is **Uninstall application remotely**.

This method of uninstallation is useful when the security application installer cannot properly remove an incompatible application.

How-to instructions:

- Administration Console: Creating a task (on page [374](#))

Installing applications using a remote installation task

Kaspersky Security Center allows you to install applications on devices remotely, using remote installation tasks. Those tasks are created and assigned to devices through a dedicated Wizard. To assign a task to devices more quickly and easily, you can specify devices in the Wizard window in one of the following ways:

- **Select networked devices detected by Administration Server.** In this case, the task is assigned to specific devices. The specific devices can include devices in administration groups as well as unassigned devices.
- **Specify device addresses manually or import addresses from a list.** You can specify NetBIOS names, DNS names, IP addresses, and IP subnets of devices to which you want to assign the task.
- **Assign task to a device selection.** In this case, the task is assigned to devices included in a selection created earlier. You can specify the default selection or a custom one that you created.
- **Assign task to an administration group.** In this case, the task is assigned to devices included in an administration group created earlier.

For correct remote installation on a device with no Network Agent installed, the following ports must be opened: a) TCP 139 and 445; b) UDP 137 and 138. By default, these ports are opened on all devices included in the domain. They are opened automatically using the remote installation preparation utility (see section "Preparing a device for remote installation. Utility tool riprep.exe" on page [353](#)).

In this section

Installing an application on selected devices.....	335
Installing an application on client devices in an administration group	335
Installing an application through Active Directory group policies	335
Installing applications on secondary Administration Servers	337

Installing an application on selected devices

► *To install an application on selected devices:*

1. Establish connection with the Administration Server that controls the relevant devices.
2. In the console tree, select the **Tasks** folder.
3. Run the task creation by clicking the **Create a task** button.

The New Task Wizard starts. Follow the instructions of the Wizard.

In the **Select the task type** window of the New Task Wizard, in the **Kaspersky Security Center 13 Administration Server** node select **Install application remotely** as the task type.

The New Task Wizard creates a task of remote installation of the selected application for specific devices. The newly created task is displayed in the workspace of the **Tasks** folder.

4. Run the task manually or wait for it to launch according to the schedule specified by you in the task settings.

On completion of the remote installation task, the selected application will be installed on the selected devices.

Installing an application on client devices in an administration group

► *To install an application on client devices in an administration group:*

1. Establish a connection with the Administration Server that controls the relevant administration group.
2. Select an administration group in the console tree.
3. In the group workspace, select the **Tasks** tab.
4. Run the task creation by clicking the **Create a task** button.

The New Task Wizard starts. Follow the instructions of the Wizard.

In the **Select the task type** window of the New Task Wizard, in the **Kaspersky Security Center 13 Administration Server** node select **Install application remotely** as the task type.

The New Task Wizard creates a group task of remote installation of the selected application. The new task appears in the workspace of the administration group on the **Tasks** tab.

5. Run the task manually or wait for it to launch according to the schedule specified by you in the task settings.

On completion of the remote installation task, the selected application will be installed on client devices in the administration group.

Installing an application through Active Directory group policies

Kaspersky Security Center allows you to install Kaspersky applications on managed devices by using Active Directory group policies.

You can install applications by using Active Directory group policies only from installation packages that include Network Agent.

► *To install an application using Active Directory group policies:*

1. Start configuring the application installation by using Remote Installation Wizard (see section "Installing applications using Remote Installation Wizard" on page [338](#)).
2. In the **Defining remote installation task settings** window of the Remote Installation Wizard, select the **Assign package installation in Active Directory group policies** check box.
3. In the **Select accounts to access devices** window of the Remote Installation Wizard, select the **Account required (Network Agent is not used)** option.
4. Add the account with administrator privileges on the device where Kaspersky Security Center is installed or the account included in the Group Policy Creator Owners domain group.
5. Grant the permissions to the selected account:
 - a. Go to **Control Panel** → **Administrative Tools** and open **Group Policy Management**.
 - b. Click the node with the required domain.
 - c. Click the **Delegation** section.
 - d. In the **Permission** drop-down list, select **Link GPOs**.
 - e. Click **Add**.
 - f. In the **Select User, Computer, or Group** window that opens, select the necessary account.
 - g. Click **OK** to close the **Select User, Computer, or Group** window.
 - h. In the **Groups and users** list, select the account that you have just added, and then click **Advanced** → **Advanced**.
 - i. In the **Permission entries** list, double-click the account that you have just added.
 - j. Grant the following permissions:
 - **Create Group objects**
 - **Delete Group objects**
 - **Create group Policy Container objects**
 - **Delete group Policy Container objects**
 - k. Click **OK** to save the changes.
6. Define other settings by following the instructions of the Wizard.
7. Run the created remote installation task manually or wait for its scheduled start.

The following remote installation sequence starts:

1. When the task is running, the following objects are created in each domain that includes any client devices from the specified set:
 - Group policy object (GPO) under the name **Kaspersky_AK{GUID}**.
 - A security group that corresponds to the GPO. This security group includes client devices covered by the task. The content of the security group defines the scope of the GPO.
2. Kaspersky Security Center installs the selected Kaspersky applications on client devices directly from Share, that is, the shared network folder of the application. In the Kaspersky Security Center installation folder, an auxiliary nested folder will be created that contains the .msi file for the application to be installed.

3. When new devices are added to the task scope, they are added to the security group after the next start of the task. If the **Run missed tasks** check box is selected in the task schedule, devices are added to the security group immediately.
4. When devices are deleted from the task scope, they are deleted from the security group after the next start of the task.
5. When a task is deleted from Active Directory, the GPO, the link to the GPO, and the corresponding security group is deleted, too.

If you want to apply another installation schema using Active Directory, you can configure the required settings manually. For example, this may be required in the following cases:

- When the anti-virus protection administrator does not have rights to make changes to the Active Directory of certain domains
- When the original installation package has to be stored on a separate network resource
- When it is necessary to link a GPO to specific Active Directory units

The following options for using an alternative installation scheme through Active Directory are available:

- If installation is to be performed directly from the Kaspersky Security Center shared folder, in the GPO properties you must specify the .msi file located in the exec subfolder of the installation package folder for the required application.
- If the installation package has to be located on another network resource, you must copy the whole exec folder content to it, because in addition to the file with .msi extension the folder contains configuration files generated when the package was created. To install the license key with the application, copy the key file to this folder as well.

See also:

Deployment using group policies of Microsoft Windows[156](#)

Installing applications on secondary Administration Servers

► *To install an application on secondary Administration Servers:*

1. Establish a connection with the Administration Server that controls the relevant secondary Administration Servers.
2. Make sure that the installation package corresponding to the application being installed is available on each of the selected secondary Administration Servers. If the installation package cannot be found on any of the secondary Servers, distribute it by using the installation package distribution task (see section "Distributing installation packages to secondary Administration Servers" on page [349](#)).
3. Create the task of application installation on secondary Administration Servers in one of the following ways:
 - If you want to create a task for secondary Administration Servers in the selected administration group, create a group task of remote installation for this group (see section "Installing an application on client devices in an administration group" on page [335](#)).
 - If you want to create a task for specific secondary Administration Servers, create a task of remote installation for specific devices (see section "Installing an application on selected devices" on page [335](#)).

The Deployment Task Creation Wizard starts to guide you through creation of the remote installation task. Follow the instructions of the Wizard.

In the **Select the task type** window of the New Task Wizard, in the **Kaspersky Security Center 13 Administration Server** section open the **Advanced** folder and select **Install application on secondary Administration Servers remotely** as the task type.

The New Task Wizard will create the task of remote installation of the selected application on specific secondary Administration Servers.

4. Run the task manually or wait for it to launch according to the schedule specified by you in the task settings.

On completion of the remote installation task, the selected application will be installed on secondary Administration Servers.

Installing applications using Remote Installation Wizard

To install Kaspersky applications, you can use the Remote Installation Wizard. The Remote Installation Wizard allows remote installation of applications either through specially created installation packages or directly from a distribution package.

For proper operation of the Remote installation task on a client device that does not have Network Agent installed, the following ports must be open: TCP 139 and 445; UDP 137 and 138. By default, these ports are open for all devices included in the domain. They are opened automatically by the remote installation preparation utility (see section "Preparing a device for remote installation. Utility tool riprep.exe" on page [353](#)).

► *To install the application on selected devices by using the Remote Installation Wizard:*

1. In the console tree, locate the **Remote installation** folder and select the **Installation packages** subfolder.
2. In the workspace of the folder, select the installation package of the application that you have to install.
3. In the context menu of the installation package, select **Install application**.

The Remote Installation Wizard starts.

4. In the **Select devices for installation** window, you can create a list of devices on which the application will be installed:

- **Install on a group of managed devices**

If this option is selected, the remote installation task is created for a group of devices.

- **Select devices for installation**

If this option is selected, the remote installation task is created for specific devices. Those specific devices can include both managed and unassigned ones.

5. In the **Defining remote installation task settings** window, specify the settings for remote installation of the application.

In the **Force installation package download** settings group, specify how files that are required for the application installation are distributed to client devices:

- **Using Network Agent**

If this option is enabled, installation packages are delivered to client devices by Network

Agent installed on those client devices.

If this option is disabled, installation packages are delivered using Microsoft Windows tools.

We recommend that you enable this option if the task has been assigned to devices with Network Agents installed.

By default, this option is enabled.

- **Using operating system resources through Administration Server**

If this option is enabled, files will be transmitted to client devices by using Microsoft Windows tools through the Administration Server. You can enable this option if no Network Agent is installed on the client device, but the client device is in the same network as the Administration Server.

By default, this option is enabled.

- **Using operating system resources through distribution points**

If this option is enabled, installation packages are transmitted to client devices using operating system tools through distribution points. You can select this option if there is at least one distribution point on the network.

If the **Using Network Agent** option is enabled, the files are delivered using operating system tools only if Network Agent tools are unavailable.

By default, this option is enabled for remote installation tasks that have been created on a virtual Administration Server.

- **Number of attempts to install**

If, when running the Remote installation task, Kaspersky Security Center fails to install an application on a managed device within the number of installer runs specified by the parameter, Kaspersky Security Center stops delivering the installation package to this managed device and does not start the installer on the device anymore.

The `Number of attempts to install` parameter allows you to save the resources of the managed device, as well as reduce traffic (uninstallation, MSI file run, and error messages).

Recurring task start attempts may indicate a problem on the device that prevents installation. The administrator should resolve the problem within the specified number of installation attempts (for example, by allocating sufficient disk space, removing incompatible applications, or modifying the settings of other applications that prevent installation) and to restart the task (manually or by a schedule).

If installation is not achieved eventually, the problem is considered unresolvable and any further task starts are seen as costly in terms of unnecessary consumption of resources and traffic.

When the task is created, the counter of attempts is set to 0. Each run of the installer that returns an error on the device increments the counter reading.

If the number of attempts specified in the parameter has been exceeded and the device is ready for application installation, you can increase the value of the `Number of attempts to install` parameter and start the task to install the application. Alternatively, you can create a new Remote installation task.

Define what to do with client devices managed by another Administration Server:

- **Install on all devices**

The application will be installed even on devices managed by other Administration Servers.

This option is selected by default; you do not have to change this setting if you have only one Administration Server in your network.

- **Install only on devices managed through this Administration Server**

The application will be installed only on devices managed by this Administration Server. Select this option if you have more than one Administration Server in your network and want to avoid conflicts (see section "Avoiding conflicts between multiple Administration Servers" on page [623](#)) between them.

Define the additional settings:

- **Do not re-install application if it is already installed**

If this option is enabled, the selected application will not be re-installed if it has already been installed on this client device.

If this option is disabled, the application will be installed anyway.

By default, this option is enabled.

- **Assign package installation in Active Directory group policies**

If this option is enabled, an installation package is installed by using the Active Directory group policies.

This option is available if the Network Agent installation package is selected.

By default, this option is disabled.

1. In the **Selecting a license key** window, select a license key and a method for its distribution:

- **Do not place license key in installation package (recommended)**

The key is automatically distributed to all devices with which it is compatible:

- If automatic distribution (see section "Automatic distribution of a license key" on page [361](#)) has been enabled in the key properties.
- If the **Add key** task has been created.

- **Place license key in installation package**

The key is distributed to devices together with the installation package.

We do not recommend that you distribute the key using this method because shared read access is enabled to the packages repository.

The **Selecting a license key** window is displayed if the installation package does not include a license key.

If the installation package includes a license key, the **License key properties** window is displayed, containing the license key details.

1. In the **Selecting an operating system restart option** window, specify whether the devices must be restarted if the operating system has to be restarted during installation of applications on them:

- **Do not restart the device**

If this option is selected, the device will not be restarted after the security application installation.

- **Restart the device**

If this option is selected, the device will be restarted after the security application installation.

- **Prompt user for action**

If this option is selected, after the security application installation, a notification is displayed to the user, informing that the device needs to be restarted. By using the **Modify** link you can modify message text, the period of message display, and the time of automatic restart.

By default, this option is selected.

- **Force closure of applications in blocked sessions**

If this check box is selected, applications on blocked devices are forced to close before the restart.

By default, this check box is cleared.

2. In the **Select accounts to access devices** window, you can add the accounts that will be used to start the Remote installation task:

- **No account required (Network Agent installed)**

If this option is selected, you do not have to specify the account under which the application installer will be run. The task will run under the account under which the Administration Server service is running.

If Network Agent has not been installed on client devices, this option is not available.

- **Account required (Network Agent is not used)**

If this option is selected, you can specify the account under which the application installer will be run. You can specify the user account if Network Agent has not been installed on the devices for which the task is assigned.

You can specify multiple user accounts if, for example, none of them have all the required rights on all devices for which this task is assigned. In this case, all accounts that have been added are used for running the task, in consecutive order, top-down.

If no accounts have been added, the task will be run under the account under which the Administration Server service is running.

3. In the **Starting installation** window, click the **Next** button to create and start a Remote installation task on the selected devices.

If the **Starting installation** window has the **Do not run the task after the Remote Installation Wizard finishes** check box selected, the remote installation task will not start. You can start this task manually later. The task name corresponds to the name of the installation package for the application: **Installation of <Installation package name>**.

► *To install the application on devices in an administration group by using the Remote Installation Wizard:*

1. Establish a connection with the Administration Server that controls the relevant administration group.
2. Select an administration group in the console tree.
3. In the workspace of the group, click the **Perform action** button and select **Install application** in the drop-down list.

This will start the Remote Installation Wizard. Follow the instructions of the Wizard.

4. At the final step of the Wizard, click **Next** to create and run a remote installation task on the selected devices.

When the Remote Installation Wizard finishes, Kaspersky Security Center performs the following actions:

- Creates an installation package for application installation (if it was not created earlier). The installation package is located in the **Remote installation** folder, in the **Installation packages** subfolder, under a name that corresponds to the application name and version. You can use this installation package for the application installation in the future.
- Creates and runs a remote installation task for specific devices or for an administration group. The newly created remote installation task is stored in the **Tasks** folder or added to the tasks of the administration group for which it has been created. You can later launch this task manually. The task name corresponds to the name of the installation package for the application: **Installation of <Installation package name>**.

Viewing a protection deployment report

You can use the protection deployment report to monitor the progress of network protection deployment.

► *To view a protection deployment report:*

1. In the console tree, select the node with the name of the required Administration Server.
2. In the workspace of the node, select the **Reports** tab.
3. In the workspace of the **Reports** folder, select the report template named **Report on protection deployment**.

The workspace displays a report containing information about protection deployment on all networked devices.

You can generate a new protection deployment report and specify the type of data that it should include (see section "Working with reports" on page [504](#)):

- For an administration group
- For specific devices
- For a device selection
- For all devices

Kaspersky Security Center assumes that protection is deployed on a device if a security application is installed and real-time protection enabled.

Remote removal of applications

Kaspersky Security Center allows you to uninstall applications from devices remotely through remote uninstallation tasks. Those tasks are created and assigned to devices through a dedicated Wizard. To assign a task to devices more quickly and easily, you can specify devices in the Wizard window in one of the following ways:

- **Select networked devices detected by Administration Server.** In this case, the task is assigned to specific devices. The specific devices can include devices in administration groups as well as unassigned devices.
- **Specify device addresses manually or import addresses from a list.** You can specify NetBIOS names, DNS names, IP addresses, and IP subnets of devices to which you want to assign the task.
- **Assign task to a device selection.** In this case, the task is assigned to devices included in a selection created earlier. You can specify the default selection or a custom one that you created.
- **Assign task to an administration group.** In this case, the task is assigned to devices included in an administration group created earlier.

In this section

Remote removal of an application from client devices of the administration group	343
Remote removal of an application from selected devices	343

Remote removal of an application from client devices of the administration group

► *To remove an application remotely from client devices of the administration group:*

1. Establish a connection with the Administration Server that controls the relevant administration group.
2. Select an administration group in the console tree.
3. In the group workspace, select the **Tasks** tab.
4. Run the task creation by clicking the **Create a task** button.

The New Task Wizard starts. Follow the instructions of the Wizard.

In the **Select the task type** window of the New Task Wizard, in the **Kaspersky Security Center 13 Administration Server** node, in the **Advanced** folder select **Uninstall application remotely** as the task type.

The New Task Wizard creates a group task of remote removal of the selected application. The new task appears in the workspace of the administration group on the **Tasks** tab.

5. Run the task manually or wait for it to launch according to the schedule specified by you in the task settings.

On completion of the remote removal task, the selected application will be removed from client devices in the administration group.

Remote removal of an application from selected devices

► *To remove an application remotely from selected devices:*

1. Establish connection with the Administration Server that controls the relevant devices.
2. In the console tree, select the **Tasks** folder.
3. Run task creation by clicking **New task**.

The New Task Wizard starts. Follow the instructions of the Wizard.

In the **Select the task type** window of the New Task Wizard, in the **Kaspersky Security Center 13 Administration Server** node, in the **Advanced** folder select **Uninstall application remotely** as the task type.

The New Task Wizard creates a task of remote removal of the selected application from specific devices. The newly created task is displayed in the workspace of the **Tasks** folder.

4. Run the task manually or wait for it to launch according to the schedule specified by you in the task settings.

Upon completion of the remote removal task, the selected application will be removed from the selected devices.

Working with installation packages

When creating remote installation tasks, the system uses installation packages containing sets of parameters necessary for software installation.

Installation packages can contain a key file. It is recommended that you avoid sharing access to installation packages that contain a key file.

You can use a single installation package several times.

Installation packages created for Administration Server are moved to the console tree and located in the **Remote installation** folder, in the **Installation packages** subfolder. Installation packages are stored on the Administration Server, in a service subfolder named Packages, within the specified shared folder.

In this section

Creating an installation package	344
Creating stand-alone installation packages.....	346
Creating custom installation packages	347
Viewing and editing properties of custom installation packages	348
Distributing installation packages to secondary Administration Servers	349
Distributing installation packages through distribution points.....	350
Transferring application installation results to Kaspersky Security Center	350

Creating an installation package

► *To create an installation package, do the following:*

1. Connect to the necessary Administration Server.
2. In the console tree, in the **Remote installation** folder select the **Installation packages** subfolder.
3. Start creation of an installation package in one of the following ways:
 - By selecting **New** → **Installation package** in the context menu of the **Installation packages** folder.

- By selecting **Create** → **Installation package** in the context menu of the list of installation packages.
- By clicking the **Create installation package** link in the installation packages list management section.

This will start the New Package Wizard. Follow the instructions of the Wizard.

When creating an installation package for the Kaspersky application, you may be prompted to view the License Agreement and the Privacy Policy for this application. Please carefully read the License Agreement and Privacy Policy. If you agree with all the terms of the License Agreement and the Privacy Policy, select the following check boxes in the **I confirm that I have fully read, understand, and accept the terms and conditions of the following** section:

- **The terms and conditions of this EULA**
- **Privacy Policy describing the handling of data**

Installation of the application on your device will continue after you select both check boxes. Creation of the installation package then resumes. The path to the License Agreement and Privacy Policy file is specified in a KUD or KPD file included in the distribution kit of the application for which the installation package is to be created.

When you create an installation package for Kaspersky Endpoint Security for Mac, you can select the language of the License Agreement and Privacy Policy.

During creation of an installation package for an application from the Kaspersky database of applications, you can enable automatic installation of system components (prerequisites) required for installation of the application. The New Package Wizard displays a list of all available system components for the selected application. If a patch installation package is created (incomplete distribution package), the list contains all system prerequisites for deployment of the patch, up to the full distribution package. You can find this list at any time in the installation package properties.

Updates of managed applications may require a specific minimum version of Kaspersky Security Center to be installed. If this version is later than your current version, these updates are displayed but cannot be approved. Also, no installation packages can be created from such updates until you upgrade Kaspersky Security Center. You are prompted to upgrade your Kaspersky Security Center instance to the required minimum version.

After the New Package Wizard finishes, the new installation package appears in the workspace of the **Installation packages** folder, in the console tree.

You do not have to manually create an installation package for remote installation of Network Agent. It is created automatically during Kaspersky Security Center installation and is stored in the **Installation packages** folder. If the package for remote installation of the Network Agent has been deleted, to re-create it you select the nagent.kud file in the NetAgent folder of the Kaspersky Security Center distribution package.

Do not specify any details of privileged accounts in the parameters of installation packages.

When an installation package for Administration Server is created, select the sc.kud file in the root folder of the Kaspersky Security Center distribution package as the description file.

Creating stand-alone installation packages

You and device users in your organization can use stand-alone installation packages to install applications on devices manually.

A stand-alone installation package is an executable file (installer.exe) that you can store on Web Server, in a shared folder, or transfer to a client device by another method. You can also send a link to the stand-alone installation package by email. On the client device, the user can run the received file locally to install an application, without involving Kaspersky Security Center.

Be sure that the stand-alone installation package is not available for unauthorized persons.

You can create stand-alone installation packages for Kaspersky applications and for third-party applications for Windows, macOS, and Linux platforms. To create a stand-alone installation package for a third-party application, you must create a custom installation package (see section "Creating custom installation packages" on page [347](#)) first.

The source to create stand-alone installation packages are installation packages in the list of created on the Administration Server.

► *To create a stand-alone installation package:*

1. In the console tree, select the **Administration Server** → **Advanced** → **Remote installation** → **Installation packages**.

A list of installation packages available on Administration Server is displayed.

2. In the list of installation packages, select an installation package for which you want to create a stand-alone package.
3. In the context menu, select **Create stand-alone installation package**.

Stand-alone Installation Package Creation Wizard starts. Proceed through the Wizard by using the **Next** button.

4. On the first page of the Wizard, if you have selected an installation package for the Kaspersky application and you want to install Network Agent together with the selected application, make sure that the **Install Network Agent together with this application** option is enabled.

By default, the option is enabled. We recommend enabling this option if you are not sure whether Network Agent is installed on the device. If Network Agent is already installed on the device, after the stand-alone installation package with Network Agent is installed, Network Agent will be updated to the newer version.

If you disable this option, Network Agent will not be installed on the device and the device will be unmanaged.

If a stand-alone installation package for the selected application already exists on Administration Server, the Wizard informs you about this fact. In this case, you must select one of the following actions:

- **Create stand-alone installation package.** Select this option if, for example, you want to create a stand-alone installation package for a new application version and also want to retain a stand-alone installation package that you created for a previous application version. The new stand-alone installation package is placed in another folder.
- **Use existing stand-alone installation package.** Select this option if you want to use an existing stand-alone installation package. The process of package creation will not be started.

- **Rebuild existing stand-alone installation package.** Select this option if you want to create a stand-alone installation package for the same application again. The stand-alone installation package is placed in the same folder.
5. On the next page of the Wizard, select the **Move unassigned devices to this group** option and specify an administration group to which you want to move the client device after Network Agent installation.
By default, the device is moved to the **Managed devices** group.
If you do not want to move the client device to an administration group after Network Agent installation, select the **Do not move devices** option.
 6. On the next page of the Wizard, when the process of the stand-alone installation package creation is finished, a result of the stand-alone package creation and a path to the stand-alone package are displayed.
You can click the links and do any of the following:
 - Open the folder with the stand-alone installation package.
 - Email the link to the created stand-alone installation package. To perform this action, you must have an email application launched.
 - Sample HTML code for publishing the link on a website. A TXT file is created and opened in an application that is associated with a TXT format. In the file, the `<a>` HTML tag with attributes is displayed.
 7. On the next page of the Wizard, if you want to open the list of stand-alone installation packages, enable the **Open the list of stand-alone packages** option.
 8. Click the **FINISH** button.

The Stand-alone Installation Package Creation Wizard closes.

The stand-alone installation package is created and placed in the PkgInst subfolder of the Administration Server shared folder (see section "Defining a shared folder" on page [224](#)). You can view the list of stand-alone packages by clicking the **View the list of stand-alone packages** button above the list of installation packages.

Creating custom installation packages

You can use custom installation packages to do the following:

- To install any application (for example, a text editor) on a client device, for example, by means of a task (see section "Tasks" on page [1078](#)).
- To create a stand-alone installation package (see section "Creating stand-alone installation packages" on page [346](#)).

A custom installation package is a folder with a set of files. The source to create a custom installation package is an *archive file*. The archive file contains a file or files that must be included in the custom installation package. Creating a custom installation package, you can specify command-line parameters, for example, to install the application in a silent mode.

► *To create a custom installation package:*

1. In the console tree, select the **Administration Server** → **Advanced** → **Remote installation** → **Installation packages**.

A list of installation packages available on Administration Server is displayed.

2. Above the list of installation packages, click the **Create installation package** button.
The New Package Wizard starts. Proceed through the Wizard by using the **Next** button.
3. On the first page of the Wizard, select **Create an installation package for the specified executable file**.
4. On the next page of the Wizard, specify the custom installation package name.
5. On the next page of the Wizard, click the **Browse** button and, in a standard Windows **Open** window, choose an archive file located on the available disks to create a custom installation package.

You can choose one of the following file types: ZIP, CAB, TAR, or TAR.GZ.

It is not possible to create an installation package from an SFX (self-extracting archive) file.

Files are downloaded to the Kaspersky Security Center Administration Server.

6. On the next page of the Wizard, specify the command-line parameters of an executable file.
You can specify command-line parameters to install the application from the installation package in a silent mode. Specifying command-line parameters is optional.

If you want, configure the following options:

- **Copy entire folder to the installation package**
- **Convert settings to recommended values for applications recognized by Kaspersky Security Center 13**

The process to create the custom installation package starts.

The Wizard informs you when the process is finished.

If the custom installation package is not created, an appropriate message is displayed.

7. Click the **Finish** button to close the Wizard.

The installation package that you created is downloaded to the Packages subfolder of the Administration Server shared folder (see section "Defining a shared folder" on page [224](#)). After downloading, the custom installation package appears in the list of installation packages.

In the list of installation packages on Administration Server, you can view and edit custom installation package properties (see section "Viewing and editing properties of custom installation packages" on page [348](#)).

Viewing and editing properties of custom installation packages

After you created a custom installation package, you can view general information about the installation package and specify the installation settings in the properties window.

► *To view and edit properties of a custom installation package:*

1. In the console tree, select the **Administration Server** → **Advanced** → **Remote installation** → **Installation packages**.

A list of installation packages available on Administration Server is displayed.

2. In the context menu of an installation package, select **Properties**.

The properties window of the selected installation package opens.

3. View the following information:

- Installation package name
 - Application name packed into the custom installation package
 - Application version
 - Installation package creation date
 - Path to the custom installation package on the Administration Server
 - Executable file command line
4. Specify the following settings:
- Installation package name
 - **Install required general system components**

If this option is enabled, before installing an update the application automatically installs all general system components (prerequisites) that are required to install the update. For example, these prerequisites can be operating system updates

If this option is disabled, you may have to install the prerequisites manually.

By default, this option is disabled.

This option is only available when the application added to the installation package is recognized by Kaspersky Security Center.

- **Executable file command line**

If the application requires additional parameters for a silent installation, specify them in this field. Refer to the vendor's documentation for details.

You can also enter other parameters.

This option is only available for packages that are not created on the basis of Kaspersky applications.

1. Click the **OK** or **Apply** button to save the changes, if any.

The new settings are saved.

See also:

| Creating custom installation packages [347](#)

Distributing installation packages to secondary Administration Servers

► *To distribute installation packages to secondary Administration Servers:*

1. Establish a connection with the Administration Server that controls the relevant secondary Administration Servers.

2. Create a task of installation package distribution to secondary Administration Servers in one of the following ways:
 - If you want to create a task for secondary Administration Servers in the selected administration group, launch the creation of a group task for this group.
 - If you want to create a task for specific secondary Administration Servers, launch the creation of a task for specific devices.

The New Task Wizard starts. Follow the instructions of the Wizard.

In the **Select the task type** window of the New Task Wizard, in the **Kaspersky Security Center 13 Administration Server** node, in the **Advanced** folder select **Distribute installation package** as the task type.

The New Task Wizard will create the task of distributing the selected installation packages to specific secondary Administration Servers.

3. Run the task manually or wait for it to launch according to the schedule specified by you in the task settings.

The selected installation packages will be copied to the specific secondary Administration Servers.

Distributing installation packages through distribution points

You can use distribution points to distribute installation packages within an administration group.

After the installation packages are received from the Administration Server, distribution points automatically distribute them to client devices through IP multicasting. IP multicasting of new installation packages within an administration group occurs once. If a client device has been disconnected from the corporate network at the time of distribution, Network Agent (on the client device) automatically downloads the necessary installation package from a distribution point when the installation task is started.

Transferring application installation results to Kaspersky Security Center

After you have created the application installation package, you can configure it so that all diagnostic information about the results of the application installation is transferred to Kaspersky Security Center. For installation packages of Kaspersky applications, transfer of diagnostic information about the application installation results is configured by default, and no additional configuration is required.

► *To configure the transfer of diagnostic information about the results of application installation to Kaspersky Security Center:*

1. Navigate to the folder of the installation package created by using Kaspersky Security Center for the selected application. The folder can be found in the shared folder specified during Kaspersky Security Center installation.
2. Open the file with the .kpd or .kud extension for editing (for example, in the Microsoft Windows Notepad editor).

The file has the format of a regular configuration .ini file.

3. Add the following lines to the file:

```
[SetupProcessResult]
Wait=1
```

This command configures Kaspersky Security Center to wait for setup completion for the application, for which the installation package is created, and to analyze the installer return code. If you have to disable the transfer of diagnostic data, set the value of the Wait key to 0.

4. Add the description of return codes for a successful installation. To do this, add the following lines to the file:

```
[SetupProcessResult_SuccessCodes]
<return code>=[<description>]
<return code 1>=[<description>]
...
```

Square brackets contain optional keys.

Syntax for the lines:

- `<return code>`. Any number corresponding to the installer return code. The number of return codes can be arbitrary.
 - `<description>`. Text description of the installation result. The description can be omitted.
5. Add the description of return codes for a failed installation. To do this, add the following lines to the file:

```
[SetupProcessResult_ErrorCodes]
<return code>=[<description>]
<return code 1>=[<description>]
...
```

The syntax of these lines is identical to the syntax for the lines containing successful setup return codes.

6. Close the .kpd or .kud file by saving all changes.

Finally, the results of installation of the user-defined application will be registered in the logs of Kaspersky Security Center and then shown in the list of events, in reports, and in task run logs.

Receiving up-to-date versions of applications

Kaspersky Security Center allows you to receive up-to-date versions of corporate applications stored on Kaspersky servers.

► *To receive up-to-date versions of Kaspersky corporate applications:*

1. Do one of the following:
 - In the console tree select the node with the name of the required Administration Server, make sure the **Monitoring** tab is selected, and in the **Deployment** section click the **There are new versions of Kaspersky applications available** link.

The **There are new versions of Kaspersky applications available** link becomes visible when Administration Server finds a new version of a corporate application on a Kaspersky server.

- In the console tree, select **Advanced** → **Remote installation** → **Installation packages**, and in the workspace click **Additional actions** and from the drop-down list select View current version of Kaspersky application.

The list of the current version of Kaspersky applications is displayed.

2. Select the required application from the list.
3. Download the application distribution package by clicking the link in the **Distribution package web address** string.

Updates of managed applications may require a specific minimum version of Kaspersky Security Center to be installed. If this version is later than your current version, these updates are displayed but cannot be approved. Also, no installation packages can be created from such updates until you upgrade Kaspersky Security Center. You are prompted to upgrade your Kaspersky Security Center instance to the required minimum version.

If the **Download applications and create installation packages** button is displayed for the application selected, you can click this button to download the application distribution package and create an installation package automatically. Kaspersky Security Center downloads the application distribution package to Administration Server, to the shared folder specified during installation of Kaspersky Security Center. The automatically created installation package is displayed in the **Remote installation** folder in the console tree, in the **Installation packages** subfolder.

After the **Current application versions** window is closed, the **There are new versions of Kaspersky applications available** link disappears from the **Deployment** section.

You can create installation packages for new versions of applications and manage newly created installation packages in the **Remote installation** folder in the console tree, in the **Installation packages** subfolder.

You can also open the **Current application versions** window by clicking the **View current versions of Kaspersky applications** link in the workspace of the **Installation packages** folder.

See also:

Replacing third-party security applications	333
Installing applications using a remote installation task	334
Installing applications using Remote Installation Wizard	338
Viewing a protection deployment report	342
Remote removal of applications	342
Working with installation packages	344
Preparing a device for remote installation. Utility tool riprep.exe	353
Preparing a Linux device for remote installation of Network Agent	355
Preparing a macOS device for remote installation of Network Agent	356
Creating an installation package	344

Preparing a device for remote installation. Utility tool riprep.exe

Remote installation of the application on the client device may return an error for the following reasons:

- The task has already been successfully performed on this device. In this case, the task does not have to be performed again.
- When a task was started, the device was shut down. In this case, turn on the device and restart the task.
- There is no connection between the Administration Server and the Network Agent installed on the client device. To determine the cause of the problem, use the utility designed for remote diagnostics of client devices (klactgui).
- If Network Agent is not installed on the device, the following problems may occur during remote installation:
 - The client device has **Disable simple file sharing** enabled.
 - The Server service is not running on the client device.
 - The required ports are closed on the client device.
 - The account that is used to perform the task has insufficient privileges.

To solve problems that occur during installation of the application on a client device without Network Agent installed, you can use the utility designed to prepare devices for remote installation (riprep).

This section contains a description of the utility that allows you to prepare a device for remote installation (riprep). The utility is located in the Kaspersky Security Center installation folder on the device on which Administration Server is installed.

The utility used to prepare a device for remote installation does not run on Microsoft Windows XP Home Edition.

In this section

Preparing a device for remote installation in interactive mode.....	353
Preparing a device for remote installation in non-interactive mode	354

Preparing a device for remote installation in interactive mode

► *To prepare a device for remote installation in interactive mode:*

1. Run the riprep.exe file on a client device.
2. In the main window of the remote installation preparation utility, select the following check boxes:
 - **Disable simple file sharing.**
 - **Start the Administration Server service.**
 - **Open ports.**
 - **Add an account.**

- **Disable User Account Control (UAC).** This setting is only available for devices running Microsoft Windows Vista, Microsoft Windows 7, or Microsoft Windows Server 2008.

3. Click the **Start** button.

The stages of device preparation for remote installation are shown in the lower part of the utility's main window.

If you selected the **Add an account** check box, when an account is created you will be prompted to enter the account name and password. This will create a local account belonging to the local administrators' group.

If you selected the **Disable User Account Control (UAC)** check box, an attempt to disable User Account Control will be made even if UAC was disabled before the utility was started. After UAC is disabled, you will be prompted to restart the device.

Preparing a device for remote installation in non-interactive mode

► *To prepare a device for remote installation in non-interactive mode:*

Run the `riprep.exe` file on the client device from the command line with the requisite set of keys.

Utility command line syntax:

```
riprep.exe [-silent] [-cfg CONFIG_FILE] [-tl traceLevel]
```

Descriptions of the keys:

- `-silent`—Starts the utility in the non-interactive mode.
- `-cfg CONFIG_FILE`—Defines the utility configuration, where `CONFIG_FILE` is the path to the configuration file (a file with the `.ini` extension).
- `-tl traceLevel`—Defines the trace level, where `traceLevel` is a number from 0 to 5. If no key is specified, the value 0 is used.

You can perform the following tasks by starting the utility in silent mode:

- Disabling the simple sharing of files
- Starting the Server service on the client device
- Opening the ports
- Creating a local account
- Disabling User Account Control (UAC)

You can specify the parameters for device preparation for remote installation in the configuration file specified in the `-cfg` key. To define these parameters, add the following information to the configuration file:

- In the `Common` section, specify the tasks to be performed:
 - `DisableSFS`—Disable the simple sharing of files (0 —the task is disabled; 1 —the task is enabled).
 - `StartServer`—Start the Server service (0 —the task is disabled; 1 —the task is enabled).
 - `OpenFirewallPorts`—Open the necessary ports (0 —the task is disabled; 1 —the task is enabled).
 - `DisableUAC`—Disable User Account Control (UAC) (0 —the task is disabled; 1 —the task is enabled).

- `RebootType`—Define behavior if restart of device is required when UAC is disabled. You can use the following values:
 - 0—Never restart the device.
 - 1—Restart the device, if UAC was enabled before starting the utility.
 - 2—Force restart, if UAC was enabled before starting the utility.
 - 4—Always restart the device.
 - 5—Always restart the device with force.
- In the `UserAccount` section, specify the account name (`user`) and its password (`Pwd`).

Sample context of the configuration file:

```
[Common]
DisableSFS=0
StartServer=1
OpenFirewallPorts=1

[UserAccount]
user=Admin
Pwd=Pass123
```

After the utility completes, the following files will be created in the utility start folder:

- `riprep.txt`—Operation report, in which phases of the utility operation are listed with reasons for these operations.
- `riprep.log`—Trace file (created if the tracing level is set above 0).

Preparing a Linux device for remote installation of Network Agent

► *To prepare a device running Linux for remote installation of Network Agent:*

1. Make sure that `sudo` is installed on the target Linux device.
2. Test the device configuration:
 - a. Check whether you can connect to the device through an SSH client (such as PuTTY).

If you cannot connect to the device, open the `/etc/ssh/sshd_config` file and make sure that the following settings have the respective values listed below:

```
PasswordAuthentication no
ChallengeResponseAuthentication yes
```

Save the file (if necessary) and restart the SSH service by using the `sudo service ssh restart` command.

- b. Disable the `sudo` password for the user account under which the device is to be connected.

Use the `visudo` command in `sudo` to open the `sudoers` configuration file. In the file you have opened, specify the following: `username ALL = (ALL) NOPASSWD: ALL`. In this case, `username` is the user account, which is to be used for the device connection using SSH.

- c. Save the `sudoers` file and then close it.

- d. Connect to the device again through SSH and make sure that the Sudo service does not prompt you to enter a password; you can do this using the `sudo whoami` command.
3. Download and create an installation package:
 - a. Before installing the package on the device, make sure that it already has all the dependencies (programs and libraries) installed for this package.

You can view the dependencies for each package on your own, using utilities that are specific for the Linux distribution on which the package is to be installed. For more details about utilities, refer to your operating system documentation.
 - b. Download the Network Agent installation package.
 - c. To create a remote installation package, use the following files:
 - `knagent.kpd`
 - `akinstall.sh`
 - `.deb` or `.rpm` package of Network Agent
 4. Create a remote installation task with the following settings:
 - On the **Settings** page of the New Task Wizard, select the **Using operating system resources through Administration Server** check box. Clear all other check boxes.
 - On the **Selecting an account to run the task** page, to run the task specify the settings of the user account that is used for device connection through SSH.
 5. Run the remote installation task.

An error may be returned if you install Network Agent with SSH on devices running Fedora versions earlier than version 20. In this case, for successful installation of Network Agent, comment out the Defaults requiretty option (enclose it in comment syntax to remove it from parsed code) in the `/etc/sudoers` file. For a detailed description of the condition of the Defaults requiretty option that may cause problems during SSH connection, please refer to the Bugzilla bugtracker website (https://bugzilla.redhat.com/show_bug.cgi?id=1020147).

Preparing a macOS device for remote installation of Network Agent

► *To prepare a device running macOS for remote installation of Network Agent:*

1. Make sure that sudo is installed on the target macOS device.
2. Test the device configuration:
 - a. Make sure port 22 is open on the client device: in the **System Preferences**, open the **Sharing** pane and make sure the **Remote Login** check box is selected. You can use the `ssh <device_name>` command to log in to the macOS device remotely.

In the **Sharing** pane, you can use the **Allow access for** option to set the scope of users who are allowed access to the macOS device.
 - b. Disable the sudo password for the user account under which the device is to be connected.

Use the `sudo visudo` command in the Terminal to open the sudoers configuration file. In the file that you have opened, in the `User privilege specification` entry specify the following:
`username ALL = (ALL) NOPASSWD: ALL`. In this case, `username` stands for the user account, which is to be used for the device connection using Secure Shell (SSH).
 - c. Save the sudoers file and then close it.

- d. Connect to the device again through SSH and make sure that the Sudo service does not prompt you to enter a password; you can do this using the `sudo whoami` command.
3. Download and create an installation package:
 - a. Download the Network Agent installation package using one of the following methods:
 - In the console tree, by opening the context menu on **Remote installation** → **Installation packages** and selecting **Show current application versions** to choose from available packages
 - By downloading the relevant version of Network Agent from Technical Support website at <https://support.kaspersky.com/> <https://support.kaspersky.com>
 - By requesting the installation package from Technical Support specialists
 - b. To create a remote installation package, use the following files:
 - `klnagent.kud`
 - `install.sh`
 - `klnagentmac.dmg`
 4. Create a remote installation task with the following settings:
 - On the **Settings** page of the New Task Wizard, select the **Using operating system resources through Administration Server** check box. Clear all other check boxes.
 - On the **Selecting an account to run the task** page, to run the task specify the settings of the user account that is used for device connection through SSH.

The client device is ready for remote installation of Network Agent through the corresponding task that you have created.

Kaspersky applications: licensing and activation

This section describes the features of Kaspersky Security Center related to working with the license keys of managed Kaspersky applications.

Kaspersky Security Center allows you to perform centralized distribution of license keys for Kaspersky applications on client devices, monitor their use, and renew licenses.

When adding a license key using Kaspersky Security Center, the settings of the license key are saved on the Administration Server. Based on this information, the application generates a license key usage report and notifies the administrator of license expirations and violation of license restrictions that are set in the properties of license keys. You can configure notifications of the use of license keys within the Administration Server settings.

See also:

Scenario: Installation and initial setup of Kaspersky Security Center 13 Web Console	962
Licensing of managed applications	358
Viewing information about license keys in use	360
Adding a license key to the Administration Server repository	360
Deleting an Administration Server license key	361
Deploying a license key to client devices	361
Automatic distribution of a license key	361
Creating and viewing a license key usage report	362

Licensing of managed applications

The Kaspersky applications installed on managed devices must be licensed by applying a key file or activation code to each of the applications. A key file or activation code can be deployed in the following ways:

- Automatic deployment
- The installation package of a managed application
- The Add license key task for a managed application
- Manual activation of a managed application

Automatic deployment

If you use different managed applications and you have to deploy a specific key file or activation code to devices, opt for other ways of deploying that activation code or key file.

Kaspersky Security Center allows you to automatically deploy available license keys to devices. For example, three license keys are stored in the Administration Server repository. You have enabled the **Automatically distributed license key** option for all three license keys. A Kaspersky security application—for example, Kaspersky Endpoint Security for Windows—is installed on the organization's devices. A new device is discovered to which a license key must be deployed. The application determines, for instance, that two of the license keys from the repository can be deployed to the device: license key named *Key_1* and license key named *Key_2*. One of these license keys is deployed to the device. In this case, it cannot be predicted which of the two license keys will be deployed to the device because automatic deployment of license keys does not provide for any administrator activity.

When a license key is deployed, the devices are recounted for that license key. You must make sure that the number of devices to which the license key was deployed does not exceed the license limit. If the number of devices exceeds the license limit (see section "Events of the licensing limit exceeded" on page [329](#)), all devices that were not covered by the license will be assigned *Critical* status.

Before deployment, the key file or activation code must be added to the Administration Server repository.

How-to instructions:

- Administration Console:
 - Adding a license key to the Administration Server repository (on page [360](#))
 - Automatic distribution of a license key (on page [361](#))or
- Kaspersky Security Center 13 Web Console:
 - Adding a license key to the Administration Server repository (on page [1056](#))
 - Automatic distribution of a license key (on page [1057](#))

Adding a key file or activation code to the installation package of a managed application

For security reasons, this option is not recommended. A key file or activation code added to an installation package may be compromised.

If you install a managed application using an installation package, you can specify an activation code or key file in this installation package or in the policy of the application. The license key will be deployed to managed devices at the next synchronization of the device with the Administration Server.

How-to instructions:

- Administration Console:
 - Creating an installation package (on page [344](#))
 - Installing applications on client devices (on page [719](#))or
- Kaspersky Security Center 13 Web Console: Adding a license key to an installation package (see section "Step 2. Selecting a method for distribution of key file or activation code" on page [1002](#))

Deployment through the Add license key task for a managed application

If you opt for using the Add license key task for a managed application, you can select the license key that must be deployed to devices and select the devices in any convenient way—for example, by selecting an administration group or a device selection.

Before deployment, the key file or activation code must be added to the Administration Server repository.

How-to instructions:

- Administration Console:
 - Adding a license key to the Administration Server repository (on page [360](#))
 - Deploying a license key to client devices (on page [361](#))or
- Kaspersky Security Center 13 Web Console:
 - Adding a license key to the Administration Server repository (on page [1056](#))
 - Deploying a license key to client devices (on page [1057](#))

Adding an activation code or a key file manually to the devices

You can activate the installed Kaspersky application locally, by using the tools provided in the application interface. Please refer to the documentation of the installed application.




Viewing information about license keys in use

► *To view information about license keys in use,*

In the console tree, select the **Kaspersky Licenses** folder.

The workspace of the folder displays a list of license keys used on client devices.

Next to each of the license keys an icon is displayed, corresponding to the type of use:

-  —Information about the currently used license key is received from a client device connected to the Administration Server. The file of this license key is stored outside of the Administration Server.
-  —The license key is stored in the Administration Server repository. Automatic distribution is disabled for this license key.
-  —The license key is stored in the Administration Server repository. Automatic distribution is enabled for this license key.

You can view information about which license keys are used for activation of the application on a client device by opening the **Applications** section of the client device (see section "Viewing and editing local application settings" on page [404](#)) properties window.

To define the up-to-date settings of virtual Administration Server license keys, the Administration Server sends a request to Kaspersky activation servers at least once per day.

Adding a license key to the Administration Server repository

► *To add a license key to the Administration Server repository:*

1. In the console tree, select the **Kaspersky Licenses** folder.
2. Start the license key adding task in one of the following ways:
 - By selecting **Add activation code or key file** in the context menu of the list of license keys.
 - By clicking the **Add activation code or key file** link in the workspace of the list of license keys.

This will start the Add License Key Wizard. Follow the instructions of the Wizard.

Deleting an Administration Server license key

► *To delete an Administration Server license key:*

1. In the context menu of the Administration Server, select **Properties**.
2. In the Administration Server properties window that opens, select the **License keys** section.
3. Delete the active or reserve license key by clicking the **Remove** button.

This deletes the license key.

If a reserve license key has been added, the reserve license key automatically becomes the active license key after the former active license key is deleted.

After the active license key of Administration Server is deleted, Vulnerability and Patch Management (see section "Kaspersky Security Center licensing options" on page [320](#)) and Mobile Device Management (see section "Kaspersky Security Center licensing options" on page [320](#)) become unavailable. You can add (see section "Adding a license key to the Administration Server repository" on page [360](#)) a deleted license key again or add a new license key.

Deploying a license key to client devices

Kaspersky Security Center allows you to distribute a license key to client devices through the license key distribution task.

► *To distribute a license key to client devices:*

1. In the console tree, select the **Kaspersky Licenses** folder.
2. In the workspace of the list of license keys, click the **Deploy license key to managed devices** button.

The Application Activation Task Creation Wizard starts. Follow the instructions of the Wizard.

Tasks created through the Application Activation Task Creation Wizard are tasks for specific devices stored in the **Tasks** folder of the console tree.

You can also create a group or local license key distribution task through the Task Creation Wizard for an administration group and for a client device.

Automatic distribution of a license key

Kaspersky Security Center allows automatic distribution of license keys to managed devices if they are located in the license keys repository on the Administration Server.

► *To distribute a license key to managed devices automatically:*

1. In the console tree, select the **Kaspersky Licenses** folder.
2. In the workspace of the folder, select the license key that you want to distribute to devices automatically.
3. Open the properties window of the selected license key in one of the following ways:
 - By selecting **Properties** in the context menu of the license key.
 - By clicking the **View license key properties** link in the information box for the selected license key.

4. In the license key properties window that opens, select the **Automatically distributed license key** check box. Close the license key properties window.

The license key will be automatically distributed as the active or reserve license key to all compatible devices.

License key distribution is performed by means of Network Agent. No reserve license key distribution tasks are created for the application.

During automatic distribution of a license key as the active or reserve license key, the licensing limit on the number of devices is taken into account. (The licensing limit is set in the properties of the license key.) If the licensing limit is reached, distribution of this license key on devices ceases automatically.

Creating and viewing a license key usage report

► *To create a report on usage of license keys on client devices:*

1. In the console tree, select the node with the name of the required Administration Server.
2. In the workspace of the node, select the **Reports** tab.
3. Select the report template named **License key usage report**, or create a new report template of the same type.

The workspace of the license key usage report displays information about active and reserve license keys used on the client devices. The report also contains information about devices on which the license keys are used, and about restrictions specified in the properties of those license keys.

Configuring network protection

This section contains information about manual configuration of policies, tasks, and other settings of Administration Server, and information about the distribution point, building an administration group structure and hierarchy of tasks, and other settings.

In this chapter

Scenario: Configuring network protection.....	364
Policy setup and propagation: Device-centric approach	365
About device-centric and user-centric security management approaches.....	367
Manual setup of Kaspersky Endpoint Security.....	368
Manual setup of the group update task for Kaspersky Endpoint Security.....	371
Manual setup of the group task for scanning a device with Kaspersky Endpoint Security	371
Scheduling the Find vulnerabilities and required updates task	372
Manual setup of the group task for updates installation and vulnerabilities fix	372
Setting the maximum number of events in the event repository	372
Managing tasks.....	373
Creating a hierarchy of administration groups subordinate to a virtual Administration Server	384
Hierarchy of policies, using policy profiles	385
Managing policies	387
Device moving rules	401
Cloning device moving rules.....	402
Software categorization	403
Prerequisites for installing applications on devices of a client organization.....	403
Viewing and editing local application settings	404

Scenario: Configuring network protection

The Quick Start Wizard creates policies and tasks with the default settings. These settings may turn out to be sub-optimal or even disallowed by the organization. Therefore, we recommend that you fine-tune these policies and tasks and create other policies and tasks, if they are necessary for your network.

Prerequisites

Before you start, make sure that you have done the following:

- Installed Kaspersky Security Center 13 Administration Server (see section "Installing Kaspersky Security Center (Standard installation)" on page [966](#))
- Installed Kaspersky Security Center 13 Web Console (see section "Installing Kaspersky Security Center 13 Web Console" on page [967](#)) (optional)
- Completed the Kaspersky Security Center main installation scenario (see section "Main installation scenario" on page [59](#))
- Completed the Quick Start Wizard (see section "Quick Start Wizard (Kaspersky Security Center 13 Web Console)" on page [993](#)) or manually created the following policies and tasks in the **Managed devices** administration group:
 - Policy of Kaspersky Endpoint Security
 - Group task for updating Kaspersky Endpoint Security
 - Policy of Network Agent
 - *Find vulnerabilities and required updates* task

Configuring network protection proceeds in stages:

a. Setup and propagation of Kaspersky application policies and policy profiles

To configure and propagate settings for Kaspersky applications installed on the managed devices, you can use two different security management approaches (see section "About device-centric and user-centric security management approaches" on page [367](#))—device-centric or user-centric. These two approaches can also be combined. To implement device-centric security management (see section "Policy setup and propagation: Device-centric approach" on page [365](#)), you can use tools provided in Microsoft Management Console-based Administration Console or Kaspersky Security Center 13 Web Console. User-centric security management (see section "Policy setup and propagation: User-centric approach" on page [1066](#)) can be implemented through Kaspersky Security Center 13 Web Console only.

b. Configuring tasks for remote management of Kaspersky applications

Check the tasks created with the Quick Start Wizard and fine-tune them, if necessary.

How-to instructions:

- Administration Console:
 - Setting up the group task for updating Kaspersky Endpoint Security (see section "Manual setup of the group update task for Kaspersky Endpoint Security" on page [371](#))
 - Scheduling the Find vulnerabilities and required updates task (on page [372](#))

or

- Kaspersky Security Center 13 Web Console:

- Setting up the group task for updating Kaspersky Endpoint Security (see section "Manual setup of the group update task for Kaspersky Endpoint Security" on page [1073](#))
- Find vulnerabilities and required updates task settings (on page [1219](#))

If necessary, create additional tasks (see section "Managing tasks" on page [373](#)) to manage the Kaspersky applications installed on the client devices.

c. Evaluating and limiting the event load on the database

Information about events during the operation of managed applications is transferred from a client device and registered in the Administration Server database. To reduce the load on the Administration Server, evaluate and limit the maximum number of events that can be stored in the database.

How-to instructions:

- Administration Console: Setting the maximum number of events (see section "Setting the maximum number of events in the event repository" on page [372](#))

or

- Kaspersky Security Center 13 Web Console: Setting the maximum number of events (see section "Setting the maximum number of events in the event repository" on page [1008](#))

Results

Upon completion of this scenario, your network will be protected by configuration of Kaspersky applications, tasks, and events received by the Administration Server:

- The Kaspersky applications are configured according to the policies and policy profiles.
- The applications are managed through a set of tasks.
- The maximum number of events that can be stored in the database is set.

When the network protection configuration is complete, you can proceed to configuring regular updates to Kaspersky databases and applications (see section "Scenario: Regular updating Kaspersky databases and applications" on page [1174](#)).

See also:

Scenario: Installation and initial setup of Kaspersky Security Center 13 Web Console	962
Scenario: Regular updating Kaspersky databases and applications	1174

Policy setup and propagation: Device-centric approach

When you complete this scenario, the applications will be configured on all of the managed devices in accordance with the application policies and policy profiles that you define.

Prerequisites

Before you start, make sure that you have successfully installed Kaspersky Security Center Administration Server (see section "Installing Kaspersky Security Center (Standard installation)" on page [966](#)) and Kaspersky Security Center 13 Web Console (see section "Installing Kaspersky Security Center 13 Web Console" on page [967](#)) (optional). If you installed Kaspersky Security Center 13 Web Console, you might also want to consider user-centric (see section "Policy setup and propagation: User-centric approach" on page [1066](#)) security management as an alternative or additional option to the device-centric approach.

Stages

The scenario of device-centric management of Kaspersky applications consists of the following steps:

a. Configuring application policies

Configure settings for Kaspersky applications installed on the managed devices by creating a policy (see section "Creating a policy" on page [1118](#)) for each application. The set of policies will be propagated to the client devices.

When you configure the protection of your network in Quick Start Wizard, Kaspersky Security Center creates the default policy for Kaspersky Endpoint Security for Windows. If you completed the configuration process by using this Wizard, you do not have to create a new policy for this application. Proceed to the manual setup of Kaspersky Endpoint Security policy (on page [368](#)).

If you have a hierarchical structure of several Administration Servers and/or administration groups, the secondary Administration Servers and child administration groups inherit the policies from the primary Administration Server by default. You can force the inheritance by the child groups and secondary Administration Servers to prohibit any modifications of the settings configured in the upstream policy. If you want only part of the settings to be forcibly inherited, you can lock them in the upstream policy. The rest unlocked settings will be available for modification in the downstream policies. The created hierarchy of policies (on page [385](#)) will allow you to effectively manage devices in the administration groups.

How-to instructions:

- Administration Console: Creating a policy (on page [388](#))

or

- Kaspersky Security Center 13 Web Console: Creating a policy (on page [1118](#))

b. Creating policy profiles (optional)

If you want devices within a single administration group to run under different policy settings, create policy profiles (see section "Policy profiles in a hierarchy of policies" on page [1113](#)) for those devices. A policy profile is a named subset of policy settings. This subset is distributed on target devices together with the policy, supplementing it under a specific condition called the *profile activation condition*. Profiles only contain settings that differ from the "basic" policy, which is active on the managed device.

By using profile activation conditions, you can apply different policy profiles, for example, to the devices located in a specific unit or security group of Active Directory, having a specific hardware configuration, or marked with specific tags (see section "About device tags" on page [1046](#)). Use tags to filter devices that meet specific criteria. For example, you can create a tag called *Windows*, mark all devices running Windows operating system with this tag, and then specify this tag as an activation condition for a policy profile. As a result, Kaspersky applications installed on all devices running Windows will be managed by their own policy profile.

How-to instructions:

- Administration Console:
 - Creating a policy profile (on page [395](#))
 - Creating a policy profile activation rule (on page [397](#))

or

- Kaspersky Security Center 13 Web Console:
 - Creating a policy profile (on page [1128](#))
 - Creating a policy profile activation rule (on page [1129](#))

c. Propagating policies and policy profiles to the managed devices

By default, the Administration Server automatically synchronizes with managed devices every 15 minutes. During the synchronization, the new or changed policies and policy profiles are propagated to the managed devices. You can circumvent auto-synchronization and run the synchronization manually by using the Force synchronization (see section "Forced synchronization" on page [646](#)) command. When synchronization is complete, the policies and policy profiles are delivered and applied to the installed Kaspersky applications.

If you use Kaspersky Security Center 13 Web Console, you can check whether the policies and policy profiles were delivered to a device. Kaspersky Security Center specifies the delivery date and time in the properties of the device.

How-to instructions:

- Administration Console: Forced synchronization (on page [646](#))
- or
- Kaspersky Security Center 13 Web Console: Forced synchronization (on page [1123](#))

Results

When the device-centric scenario is complete, the Kaspersky applications are configured according to the settings specified and propagated through the hierarchy of policies.

The configured application policies and policy profiles will be applied automatically to the new devices added to the administration groups.

See also:

Main installation scenario	59
Hierarchy of Administration Servers	45
Administration groups	49
Policies.....	51
Policy profiles.....	52
Hierarchy of policies	385
About user roles.....	1137
Scenario: Configuring network protection.....	364

About device-centric and user-centric security management approaches

You can manage security settings from the standpoint of device features and from the standpoint of user roles. The first approach is called *device-centric security management* and the second is called *user-centric security management*. To apply different application settings to different devices you can use either or both types of management in combination. To implement device-centric security management, you can use tools provided in Microsoft Management Console-based Administration Console or Kaspersky Security Center 13 Web Console. User-centric security management can be implemented through Kaspersky Security Center 13 Web Console only.

Device-centric security management (see section "Policy setup and propagation: Device-centric approach" on page [365](#)) enables you to apply different security application settings to managed devices depending on device-specific

features. For example, you can apply different settings to devices allocated in different administration groups. You can also differentiate the devices by usage of those devices in Active Directory, or their hardware specifications.

User-centric security management (see section "Policy setup and propagation: User-centric approach" on page [1066](#)) enables you to apply different security application settings to different user roles. You can create several user roles, assign an appropriate user role to each user, and define different application settings to the devices owned by users with different roles. For example, you may want to apply different application settings to devices of accountants and human resources (HR) specialists. As a result, when user-centric security management is implemented, each department—accounts department and HR department—has its own settings configuration for Kaspersky applications. A settings configuration defines which application settings can be changed by users and which are forcibly set and locked by the administrator.

By using user-centric security management you can apply specific application settings to individual users. This may be required when an employee has a unique role in the company or when you want to monitor security incidents related to devices of a specific person. Depending on the role of this employee in the company, you can expand or limit the rights of this person to change application settings. For example, you might want to expand the rights of a system administrator who manages client devices in a local office.

You can also combine the device-centric and user-centric security management approaches. For example, you can configure a specific application policy (see section "Policies" on page [51](#)) for each administration group and then create policy profiles (on page [52](#)) for one or several user roles of your enterprise. In this case, the policies and policy profiles are applied in the following order:

1. The policies created for device-centric security management are applied.
2. They are modified by the policy profiles according to the policy profile priorities.
3. The policies are modified by the policy profiles associated with user roles (see section "Associating policy profiles with roles" on page [1167](#)).

See also:

Scenario: Installation and initial setup of Kaspersky Security Center 13 Web Console	962
Scenario: Configuring network protection	364

Manual setup of Kaspersky Endpoint Security policy

This section provides recommendations on how to configure the Kaspersky Endpoint Security policy, which is created by the Quick Start Wizard of Kaspersky Security Center. Setup is performed in the policy properties window.

When editing a setting, please keep in mind that you must click the lock icon above the relevant setting in order to allow using its value on a workstation.

In this section

Configuring the policy in the Advanced Threat Protection section	369
Configuring the policy in the Essential Threat Protection section	369
Configuring the policy in the General Settings section	370
Configuring the policy in the Event configuration section	370

Configuring the policy in the Advanced Threat Protection section

For a full description of the settings in this section please refer to the [Kaspersky Endpoint Security for Windows documentation](#).

In the **Advanced Threat Protection** section, you can configure the use of Kaspersky Security Network for Kaspersky Endpoint Security for Windows. You can also configure Kaspersky Endpoint Security for Windows modules, such as Behavior Detection, Exploit Prevention, Host Intrusion Prevention, and Remediation Engine.

In the **Kaspersky Security Network** subsection, we recommend that you enable the **Use KSN Proxy** option. This will significantly increase the reliability of malware detection. You can also enable use of KSN servers if the KSN Proxy service is not available. KSN servers may be located either on the side of Kaspersky (when Global KSN is used) or on the side of third parties (when Private KSN is used).

Configuring the policy in the Essential Threat Protection section

For a full description of the settings in this section please refer to the [Kaspersky Endpoint Security for Windows documentation](#).

Described below are additional setup actions, which we recommend that you perform in the policy properties window of Kaspersky Endpoint Security for Windows, in the **Essential Threat Protection** section.

Essential Threat Protection section, Firewall subsection

Check the list of networks in the policy properties. The list may not contain all networks.

► *To check the list of networks:*

1. In the policy properties, in the **Essential Threat Protection** section select the **Firewall** subsection.
2. In the **Available networks** section, click the **Settings** button.

This opens the **Firewall** window. This window displays the list of networks on the **Networks** tab.

Essential Threat Protection section, File Threat Protection subsection

Enabling the scanning of network drives can place a significant load on network drives. It is more convenient to perform indirect scanning, on file servers.

► *To disable scanning of network drives:*

1. In the policy properties, in the **Essential Threat Protection** section select the **File Threat Protection** subsection.
2. In the **Security level** section, click the **Settings** button.
3. In the **File Threat Protection** window that opens, on the **General** tab clear the **All network drives** check box.

Configuring the policy in the General Settings section

For a full description of the settings in this section please refer to the Kaspersky Endpoint Security for Windows documentation.

Described below are advanced setup actions, which we recommend that you perform in the policy properties window of Kaspersky Endpoint Security for Windows, in the **General Settings** section.

General Settings section, Reports and Storage subsection

In the **Data transfer to Administration Server** section, please note the following setting:

About started applications check box: if this check box is selected, the Administration Server database saves information about all versions of all software modules on the networked devices. This information may require a significant amount of disk space in the Kaspersky Security Center database (dozens of gigabytes). Therefore, if the **About started applications** check box is still selected in the top-level policy, it must be cleared.

General Settings section, Interface subsection

If the Anti-Virus protection on the organization's network must be managed in centralized mode through Administration Console, you must disable the display of the Kaspersky Endpoint Security for Windows user interface on workstations (by clearing the **Display application interface** check box in the **Interaction with user** section), and enable password protection on them (by selecting the **Enable password protection** check box in the **Password protection** section).

Configuring the policy in the Event configuration section

In the **Event configuration** section, you should disable the saving of any events on Administration Server, except for the following ones:

- On the **Critical event** tab:
 - Application autorun is disabled
 - Access denied
 - Application startup prohibited
 - Disinfection not possible
 - License Agreement violated
 - Could not load encryption module
 - Cannot start two tasks at the same time
 - Active threat detected. Start Advanced Disinfection
 - Network attack detected
 - Not all components were updated
 - Activation error
 - Error enabling portable mode
 - Error in interaction with Kaspersky Security Center
 - Error disabling portable mode

- Application content modification error
- Error applying file encryption / decryption rules
- Policy cannot be applied
- Process terminated
- Network activity blocked
- On the **Functional failure** tab:
 - Invalid task settings. Settings not applied
- On the **Warning** tab:
 - Self-Defense is disabled
 - Incorrect reserve activation code
 - User has opted out of the encryption policy
- On the **Info** tab:
 - Application startup prohibited in test mode

Manual setup of the group update task for Kaspersky Endpoint Security

Information from this subsection is only applicable to Kaspersky Security Center 10 Maintenance Release 1 and later versions.

The optimal and recommended schedule option for Kaspersky Endpoint Security versions 10 and later is **When new updates are downloaded to the repository** when the **Use automatically randomized delay for task starts** check box is selected.

For a group update task in Kaspersky Endpoint Security version 8 you must explicitly specify the launch delay (1 hour or longer) and select the **Use automatically randomized delay for task starts** check box.

Manual setup of the group task for scanning a device with Kaspersky Endpoint Security

The Quick Start Wizard creates a group task for scanning a device. By default, the task is assigned a **Run on Fridays at 7:00 PM** schedule with automatic randomization, and the **Run missed tasks** check box is cleared.

This means that if devices in an organization are shut down on Fridays, for example, at 6:30 PM, the device scan task will never run. You must set up the most convenient schedule for this task based on the workplace rules adopted in the organization.

Scheduling the Find vulnerabilities and required updates task

The Quick Start Wizard creates the *Find vulnerabilities and required updates* task for Network Agent. By default, the task is assigned a **Run on Tuesdays at 7:00 PM** schedule with automatic randomization, and the **Run missed tasks** check box is selected.

If the organization's workplace rules provide for shutting down all devices at this time, the *Find vulnerabilities and required updates* task will run after the devices are turned on again, that is, on Wednesday morning. Such activity may be undesirable because a vulnerability scan may increase the load on CPUs and disk subsystems. You must set up the most convenient schedule for the task based on the workplace rules adopted in the organization.

See also:

Scenario: Finding and fixing vulnerabilities in third-party software	459
Scenario: Updating third-party software	1208

Manual setup of the group task for updates installation and vulnerabilities fix

The Quick Start Wizard creates a group task for updates installation and vulnerabilities fix for Network Agent. By default, the task is set up to run every day at 01:00 AM, with automatic randomization, and the **Run missed tasks** check box is cleared.

If the organization's workplace rules provide for shutting down devices overnight, the update installation will never run. You must set up the most convenient schedule for the vulnerability scan task based on the workplace rules adopted in the organization. It is also important to keep in mind that installation of updates may require restarting the device.

Setting the maximum number of events in the event repository

In the **Events repository** section of the Administration Server properties window, you can edit the settings of events storage in the Administration Server database by limiting the number of event records and record storage term. When you specify the maximum number of events, the application calculates an approximate amount of storage space required for the specified number. You can use this approximate calculation to evaluate whether you have enough free space on the disk to avoid database overflow. The default capacity of the Administration Server database is 400,000 events. The maximum recommended capacity of the database is 45 million events.

If the number of events in the database reaches the maximum value specified by the administrator, the application deletes the oldest events and rewrites them with new ones. When the Administration Server deletes old events, it cannot save new events to the database. During this period of time, information about events that were rejected is written to the Kaspersky Event Log. The new events are queued and then saved to the database after the deletion operation is complete.

► *To limit the number of events that can be stored in the events repository on the Administration Server:*

1. Right-click the Administration Server, and then select **Properties**.

The Administration Server properties window opens.

2. In the workspace of the **Events repository** section, specify the maximum number of events stored in the database.
3. Click **OK**.

The number of events that can be stored to the database is limited to the specified value.

Managing tasks

Kaspersky Security Center manages applications installed on devices, by creating and running various tasks. Tasks are required for installing, launching, and stopping applications, scanning files, updating databases and software modules, and taking other actions on applications.

Tasks are subdivided into the following types:

- *Group tasks*. Tasks that are performed on the devices of the selected administration group.
- *Administration Server tasks*. Tasks that are performed on the Administration Server.
- *Tasks for specific devices*. Tasks that are performed on selected devices, regardless of whether they are included in any administration groups.
- *Local tasks*. Tasks that are performed on a specific device.

An application task can only be created if the management plug-in for that application is installed on the administrator's workstation.

You can compile a list of devices for which a task will be created by in one of the following ways:

- By selecting networked devices discovered by Administration Server.
- By specifying a list of devices manually. You can use an IP address (or IP range), NetBIOS name, or DNS name as the device address.
- Import a list of devices from a .txt file containing the addresses of devices to be added (each address must be placed in an individual line).

If you import a list of devices from a file or create one manually, and devices are identified by their names, the list can only contain devices for which information has already been entered into the Administration Server database when those devices were connected or during device discovery.

For each application, you can create any number of group tasks, tasks for specific devices, or local tasks.

The exchange of task information between an application installed on a device and the Kaspersky Security Center database is carried out when Network Agent is connected to Administration Server.

You can make changes to the settings of tasks, view task progress, and copy, export, import, and delete tasks.

Tasks are started on a device only if the application for which the task was created is running. When the application is not running, all running tasks are canceled.

Results of completed tasks are saved in the event logs of Microsoft Windows and Kaspersky Security Center, both centrally on the Administration Server and locally on each device.

Do not include private data in task settings. For example, avoid specifying the domain administrator password.

Details of managing tasks for applications with multitenancy support

A group task for an application with multitenancy support is applied to the application depending on the hierarchy of Administration Servers and client devices. The virtual Administration Server from which the task is created must be in the same or a lower-level administration group than the client device on which the application is installed.

In events that correspond to task execution results, a service provider administrator is shown the information about the device on which the task executed. By contrast, a tenant administration is shown **Multi-tenant node**.

See also:

Scenario: Configuring network protection.....	364
Creating a task.....	374
Creating an Administration Server task.....	375
Creating a task for specific devices.....	376
Creating a local task.....	376
Displaying an inherited group task in the workspace of a nested group.....	377
Automatically turning on devices before starting a task.....	377
Automatically turning off a device after a task is completed.....	377
Limiting task run time.....	378
Exporting a task.....	378
Importing a task.....	378
Converting tasks.....	379
Starting and stopping a task manually.....	379
Pausing and resuming a task manually.....	380
Monitoring task execution.....	380
Viewing task run results stored on the Administration Server.....	380
Configuring filtering of information about task run results.....	380
Modifying a task. Rolling back changes.....	381
Comparing tasks.....	381
Accounts to start tasks.....	382
Change Tasks Password Wizard.....	383

Creating a task

In Administration Console, you can create tasks directly in the folder of the administration group for which a group task is to be created, or in the workspace of the **Tasks** folder.

► *To create a group task in the folder of an administration group:*

1. In the console tree, select the administration group for which you want to create a task.
2. In the group workspace, select the **Tasks** tab.
3. Run the task creation by clicking the **Create a task** button.

The New Task Wizard starts. Follow the instructions of the Wizard.

► *To create a task in the workspace of the **Tasks** folder:*

1. In the console tree, select the **Tasks** folder.
2. Run the task creation by clicking the **Finish** button.

The New Task Wizard starts. Follow the instructions of the Wizard.

Do not include private data in task settings. For example, avoid specifying the domain administrator password.

Creating an Administration Server task

The Administration Server performs the following tasks:

- Automatic distribution of reports.
- Downloading of updates to the repository of the Administration Server.
- Backup of Administration Server data.
- Maintenance of the database.
- Windows Update synchronization.
- Creation of an installation package based on the OS image of a reference device.

On a virtual Administration Server, only the automatic report delivery task and the installation package creation task based on the reference device OS image are available. The repository of the virtual Administration Server displays updates downloaded to the primary Administration Server. Backup of virtual Administration Server data is performed together with backup of primary Administration Server data.

► *To create an Administration Server task:*

1. In the console tree, select the **Tasks** folder.
2. Start creation of the task in one of the following ways:
 - By selecting **New** → **Task** in the context menu of the **Tasks** folder in the console tree.
 - By clicking the **Create a task** button in the workspace of the **Tasks** folder.

The New Task Wizard starts. Follow the instructions of the Wizard.

The Download updates to the repository of the Administration Server, Perform Windows Update synchronization, Database maintenance, and *Backup of Administration Server data* tasks can be created only once. If the *Download updates to the repository of the Administration Server*, *Database maintenance*, *Backup of Administration Server data*, and *Perform Windows Update synchronization* tasks have already been created for the Administration Server, they will not be displayed in the task type selection window of the New Task Wizard.

Creating a task for specific devices

In Kaspersky Security Center, you can create tasks for specific devices. Devices that are in a set can be included in various administration groups or remain outside any administration groups. Kaspersky Security Center can perform the following main tasks for specific devices:

- Install an application remotely (see section "Installing an application on selected devices" on page [335](#))
- Send message to user (see section "Sending messages to device users" on page [647](#))
- Change the Administration Server (see section "Changing the Administration Server for client devices" on page [645](#))
- Manage devices (see section "Turning on, turning off, and restarting client devices remotely" on page [646](#))
- Verify updates (see section "Verifying downloaded updates" on page [422](#))
- Distribute installation packages (see section "Distributing installation packages to secondary Administration Servers" on page [349](#))
- Install an application remotely on secondary Administration Servers (see section "Installing applications on secondary Administration Servers" on page [337](#))
- Uninstall an application remotely (see section "Remote removal of applications" on page [342](#))

► *To create a task for specific devices:*

1. In the console tree, select the **Tasks** folder.
2. Start creation of the task in one of the following ways:
 - By selecting **New** → **Task** in the context menu of the **Tasks** folder in the console tree.
 - By clicking the **Create a task** button in the workspace of the **Tasks** folder.

The New Task Wizard starts. Follow the instructions of the Wizard.

Creating a local task

► *To create a local task for a device:*

1. Select the **Devices** tab in the workspace of the group that includes the device.
2. From the list of devices on the **Devices** tab, select the device for which a local task must be created.
3. Start creating the task for the selected device in one of the following ways:
 - By clicking the **Perform action** button and selecting **Create a task** in the drop-down list.
 - By clicking the **Create a task** link in the workspace of the device.

- From the device properties as follows:
 - a. In the context menu of the device, select **Properties**.
 - b. In the device properties window that opens, select the **Tasks** section and click **Add**.

The New Task Wizard starts. Follow the instructions of the Wizard.



Detailed instructions on how to create and configure local tasks are provided in the Guides for the respective Kaspersky applications.

Displaying an inherited group task in the workspace of a nested group

► *To enable the display of inherited tasks of a nested group in the workspace:*

1. Select the **Tasks** tab in the workspace of a nested group.
2. In the workspace of the **Tasks** tab, click the **Show inherited tasks** button.

Inherited tasks are displayed in the list of tasks with one of the following icons:

- —If they were inherited from a group created on the primary Administration Server.
- —If they were inherited from a top-level group.

If the inheritance mode is enabled, inherited tasks can only be edited in the group in which they have been created. Inherited tasks cannot be edited in the group which inherits the tasks.

Automatically turning on devices before starting a task

Kaspersky Security Center allows you to modify the settings of a task so that before the task is started the operating system is loaded on devices that were turned off.

► *To configure the automatic startup of devices before starting a task:*

1. In the task properties window, select the **Schedule** section.
2. Click the **Advanced** link to open the window for configuring actions on devices.
3. In the **Advanced** window that opens, select the **Activate the device before the task is started through Wake-on-LAN (min)** check box and specify the time interval in minutes.

All devices that were turned off will be automatically turned on for the specified number of minutes before the task start, and the operating system will be loaded onto them.

Automatic loading of the operating system is only available on devices that support the Wake-on-LAN (WoL) standard.

Automatically turning off a device after a task is completed

Kaspersky Security Center allows you to configure a task in such a way that the devices to which it is distributed are automatically turned off after the task completes.

► *To automatically turn off a device after a task is complete:*

1. In the task properties window, select the **Schedule** section.
2. Click the **Advanced** link to open the window for configuring actions on devices.
3. In the **Advanced** window that opens, select the **Shut down device when task is complete** check box.

Limiting task run time

► *To limit the time during which a task is run on devices:*

1. In the task properties window, select the **Schedule** section.
2. Open the window intended for configuration of actions on client devices, by clicking **Advanced**.
3. In the **Advanced** window that opens, select the **Stop if the task is taking longer than (min)** check box and specify the time interval in minutes.

If the task is not yet complete on the device when the specified time interval expires, Kaspersky Security Center stops the task automatically.

Exporting a task

You can export group tasks and tasks for specific devices to a file. Administration Server tasks and local tasks are not available for export.

► *To export a task:*

1. In the context menu of the task, select **All tasks** → **Export**.
2. In the **Save as** window that opens, specify the file name path.
3. Click the **Save** button.

The rights of local users are not exported.

Importing a task

You can import group tasks and tasks for specific devices. Administration Server tasks and local tasks are not available for import.

► *To import a task:*

1. Select the list to which the task must be imported:
 - If you want to import the task to the list of group tasks, in the workspace of the relevant administration group select the **Tasks** tab.
 - If you want to import a task to the list of tasks for specific devices, select the **Tasks** folder in the console tree.
2. Select one of the following options to import the task:

- In the context menu of the list of tasks, select **All tasks** → **Import**.
 - Click the **Import task from file** link in the task list management block.
3. In the window that opens, specify the path to the file from which you want to import a task.
 4. Click the **Open** button.

The task is displayed in the list of tasks.

If a task with a name identical to that of the newly imported task already exists in the selected list, the (<next sequence number>) index is added to the name of the imported task, for example: (1), (2).

Converting tasks

You can use Kaspersky Security Center to convert tasks from earlier versions of Kaspersky applications into those from up-to-date versions of the applications.

Conversion is available for tasks of the following applications:

- Kaspersky Anti-Virus 6.0 for Windows Workstations MP4.
- Kaspersky Endpoint Security 8 for Windows.
- Kaspersky Endpoint Security 10 for Windows.

► *To convert tasks:*

1. In the console tree, select an Administration Server for which you want to convert tasks.
2. In the Administration Server context menu, select **All Tasks** → **Policies and Tasks Batch Conversion Wizard**.

The Policies and Tasks Batch Conversion Wizard starts. Follow the instructions of the Wizard.

After the wizard completes its operation, new tasks are created that use the settings of tasks from earlier versions of the applications.

Starting and stopping a task manually

You can start and stop tasks manually using either of the following methods: through the context menu of the task, or through the properties window of the client device to which that task has been assigned.

Starting group tasks from the context menu of the device is only allowed to users included in the **KLAdmins** group (see section "Access rights to Administration Server and its objects" on page [601](#)).

► *To start or stop a task from the context menu or the properties window of the task:*



1. In the list of tasks, select a task.
2. Start or stop the task in one of the following ways:
 - By selecting **Start** or **Stop** in the context menu of the task.

- By clicking **Start** or **Stop** in the **General** section of the task properties window.

► *To start or stop a task from the context menu or the properties window of the client device:*

1. In the list of devices, select the device.
2. Start or stop the task in one of the following ways:
 - By selecting **All tasks** → **Run Task** in the context menu of the device. Select the relevant task from the list of tasks.
The list of devices to which the task is assigned will be replaced with the device that you have selected. The task starts.



- By clicking the  or  button in the **Tasks** section of the device properties window.

Pausing and resuming a task manually

► *To pause or resume a running task manually:*

1. In the list of tasks, select a task.
2. Pause or resume the task in one of the following ways:
 - By selecting **Pause** or **Resume** in the context menu of the task.
 - By selecting the **General** section in the task properties window and clicking **Pause** or **Resume**.

Monitoring task execution

► *To monitor task execution,*

in the task properties window, select the **General** section.

In the middle part of the **General** section, the current task status is displayed.

Viewing task run results stored on the Administration Server

Kaspersky Security Center allows you to view the results for group tasks, tasks for specific devices, and Administration Server tasks. No run results can be viewed for local tasks.

► *To view the task results:*

1. In the task properties window, select the **General** section.
2. Click the **Results** link to open the **Task results** window.

Configuring filtering of information about task run results

Kaspersky Security Center allows you to filter information about results for group tasks, tasks for specific devices, and Administration Server tasks. No filtering is available for local tasks.

► *To set up the filtering of information about task run results:*

1. In the task properties window, select the **General** section.

2. Click the **Results** link to open the **Task results** window.

The upper table contains a list of all devices for which the task is assigned. The lower table displays the results of the task performed on the selected device.

3. Right-click the relevant table to open the context menu and select **Filter**.

4. In the **Set filter** window that opens, define the filter settings in the **Events**, **Devices**, and **Time** sections. Click **OK**.

The **Task results** window displays information that meets the settings specified in the filter.

Modifying a task. Rolling back changes

► *To modify a task:*

1. In the console tree, select the **Tasks** folder.

2. In the workspace of the **Tasks** folder, select a task and proceed to the task properties window using the context menu.

3. Make the relevant changes.

In the **Exclusions from task scope** section, you can set up the list of subgroups to which the task is not applied.

4. Click **Apply**.

The changes made to the task will be saved in the task properties window, in the **Revision history** section.

You can roll back changes made to a task, if necessary.

► *To roll back changes made to a task:*

1. In the console tree, select the **Tasks** folder.

2. Select the task in which changes must be rolled back, and proceed to the task properties window using the context menu.

3. In the task properties window, select the **Revision history** section.

4. In the list of task revisions, select the number of the revision to which you need to roll back changes.

5. Click the **Advanced** button and select the **Roll back** value in the drop-down list.

Comparing tasks

You can compare tasks of the same type: for example, you can compare two virus scan tasks, but you cannot compare a virus scan task and an update installation task. After the comparison, you have a report that displays which settings of the tasks match and which settings differ. You can print the task comparison report or save it as a file. You may need task comparison when different units within a company are assigned various tasks of the same type. For example, employees at the accounting department have a task of virus scanning only local disks on their computers, while employees at the sales department communicate with customers so they have a task of scanning

both local disks and email. You do not have to view all the task settings to quickly notice such difference; you can simply compare the tasks instead.

Only tasks of the same type can be compared.
Tasks can only be compared in pairs.

You can compare tasks in one of following ways: by selecting one task and comparing it to another, or by comparing any two tasks from the list of tasks.

► *To select one task and compare it to another:*

1. In the console tree, select the **Tasks** folder.
2. In the workspace of the **Tasks** folder, select the task that you want to compare to another.
3. In the context menu of the task, select **All tasks** → **Compare to another task**.
4. In the **Select a task** window, select the task for comparison.
5. Click **OK**.

A report in HTML format that compares the two tasks is displayed.

► *To compare any two tasks from the list of tasks:*

1. In the console tree, select the **Tasks** folder.
2. In the **Tasks** folder, in the list of tasks, press the **SHIFT** or **CTRL** key to select two tasks of the same type.
3. In the context menu, select **Compare**.

A report in HTML format that compares the selected tasks is displayed.

When tasks are compared, if the passwords differ, asterisks (*****) are displayed in the task comparison report.

If the password has been changed in the task properties, asterisks (*****) are displayed in the revision comparison report (*****)

Accounts to start tasks

You can specify an account under which the task should be run.

For example, to perform an on-demand scan task, you must have access rights to the object being scanned, and to perform an update task, you need authorized proxy server user rights. The capability to specify an account for the task run allows you to avoid problems with on-demand scan tasks and update tasks in case the user running a task does not have the required access rights.

During the execution of remote installation/uninstallation tasks, the specified account is used to download to client devices the files required to install/uninstall an application in case Network Agent is not installed or unavailable. If Network Agent is installed and available, the account is used if in accordance with task settings, file delivery is performed only by using Microsoft Windows utilities from the shared folder. In this case, the account must have the following rights on the device:

- Right to start applications remotely.
- Rights to use the Admin\$ resource.

- Right to *Log On As Service*.

If the files are delivered to devices through Network Agent, the account will not be used. All file copying and installation operations are then performed by the **Network Agent (LocalSystem account)**.

Change Tasks Password Wizard

For a non-local task, you can specify an account under which the task must be run. The account can be specified during task creation or in the properties of an existing task. If the specified account is used in accordance with security instructions of the organization, these instructions may require changing the account password from time to time. When the account password expires and you set a new one, the tasks fail to start until you specify the new valid password in the task properties.

The Change Tasks Password Wizard enables you to automatically replace the old password with the new one in all tasks in which the account is specified. Alternatively, you can do it manually in the properties of each task.

► *To start the Change Tasks Password Wizard:*

1. In the console tree, select the **Tasks** node.
2. In the context menu of the node, select **Change Tasks Password Wizard**.

Follow the instructions of the Wizard.

In this section

Step 1. Specifying credentials	383
Step 2. Selecting an action to take	384
Step 3. Viewing the results	384

Step 1. Specifying credentials

In the **Account** and **Password** fields, specify new credentials that are currently valid in your system (for example, in Active Directory). When you switch to the next step of the wizard, Kaspersky Security Center checks if the specified account name matches the account name in the properties of each non-local task. If the account names match, the password in the task properties is automatically replaced with the new one.

If you fill in the **Old password (optional)** field, Kaspersky Security Center replaces password only for those tasks in which both the account name and the old password are found. The replacement is performed automatically. In all other cases you need to choose an action to take on the next step of the wizard.

See also:

Change Tasks Password Wizard	383
Step 2. Selecting an action to take	384
Step 3. Viewing the results	384

Step 2. Selecting an action to take

If you have not specified the old password on the first step of the wizard or the specified old password has not matched the passwords in the tasks, you need to choose an action to take for the found tasks.

For each task that has the *Approval required* status, decide whether you want to remove the password in the task properties or replace it with the new one. If you choose to remove the password, the task is switched to run under the default account.

See also:

Change Tasks Password Wizard	383
Step 1. Specifying credentials	383
Step 3. Viewing the results	384

Step 3. Viewing the results

On the last step of the wizard, view the results for each of the found task. To complete the wizard, click the **Finish** button.

See also:

Change Tasks Password Wizard	383
Step 1. Specifying credentials	383
Step 2. Selecting an action to take	384

Creating a hierarchy of administration groups subordinate to a virtual Administration Server

After the virtual Administration Server is created, it contains by default an administration group named **Managed devices**.

The procedure for creating a hierarchy of administration groups subordinate to a virtual Administration Server is the same as the procedure for creating a hierarchy of administration groups subordinate to the physical Administration Server (see section "Administration groups" on page [49](#)).

You cannot add secondary and virtual Administration Servers to administration groups subordinate to a virtual Administration Server. This is due to limitations of virtual Administration Servers (on page [135](#)).

See also:

Managing administration groups	630
--------------------------------------	---------------------

Hierarchy of policies, using policy profiles

This section provides information about how to apply policies to devices in administration groups. This section also provides information about policy profiles supported in Kaspersky Security Center, starting from version 10 Service Pack 1.

In this section

Hierarchy of policies	385
Policy profiles.....	385
Inheritance of policy settings	387

Hierarchy of policies

In Kaspersky Security Center, you use policies for defining a single collection of settings to multiple devices. For example, the policy scope of application P defined for administration group G includes managed devices with application P installed that have been deployed in group G and all of its subgroups, except for subgroups where the **Inherit from parent group** check box is cleared in the properties.

A policy differs from any local setting by lock (🔒) icons next to its settings. If a setting (or a group of settings) is locked in the policy properties, you must, first, use this setting (or group of settings) when creating effective settings and, second, you must write the settings or group of settings to the downstream policy.

Creation of the effective settings on a device can be described as follows: the values of all settings that have not been locked are taken from the policy, then they are overwritten with the values of local settings, and then the resulting collection is overwritten with the values of locked settings taken from the policy.

Policies of the same application affect each other through the hierarchy of administration groups: Locked settings from the upstream policy overwrite the same settings from the downstream policy.

There is a special policy for out-of-office users. This policy takes effect on a device when the device switches into out-of-office mode. Out-of-office policies do not affect other policies through the hierarchy of administration groups.

The out-of-office policy will not be supported in further versions of Kaspersky Security Center. Policy profiles will be used instead of out-of-office policies.

Policy profiles

Applying policies to devices only through the hierarchy of administration groups may be inconvenient in many circumstances. It may be necessary to create several instances of a single policy that differ in one or two settings for different administration groups, and synchronize the contents of those policies in the future.

To help you avoid such problems, Kaspersky Security Center, starting from version 10 Service Pack 1, supports *policy profiles*. A policy profile is a named subset of policy settings. This subset is distributed on target devices together with the policy, supplementing it under a specific condition called the *profile activation condition*. Profiles only contain settings that differ from the "basic" policy, which is active on the client device (computer or mobile device). Activation of a profile modifies the policy settings that were active on the device before the profile was activated. Those settings take values that have been specified in the profile.

The following restrictions are currently imposed on policy profiles:

- A policy can include a maximum 100 profiles.
- A policy profile cannot contain other profiles.
- A policy profile cannot contain notification settings.

Contents of a profile

A policy profile contains the following constituent parts:

- Name Profiles with identical names affect each other through the hierarchy of administration groups with common rules.
- Subset of policy settings. Unlike the policy, which contains all the settings, a profile only contains settings that are actually required (locked settings).
- Activation condition is a logical expression with the device properties. A profile is active (supplements the policy) only when the profile activation condition becomes true. In all other cases, the profile is inactive and ignored. The following device properties can be included in that logical expression:
 - Status of out-of-office mode.
 - Properties of network environment —Name of the active rule for Network Agent connection (see section "About connection profiles for out-of-office users" on page [287](#)).
 - Presence or absence of specified tags on the device.
 - Device location in Active Directory unit: explicit (the device is right in the specified OU), or implicit (the device is in an OU, which is within the specified OU at any nesting level).
 - Device's membership in an Active Directory security group (explicit or implicit).
 - Device owner's membership in an Active Directory security group (explicit or implicit).
- Profile disabling check box. Disabled profiles are always ignored and their respective activation conditions are not verified.
- Profile priority. The activation conditions of different profiles are independent, so several profiles can be activated simultaneously. If active profiles contain non-overlapping collections of settings, no problems will arise. However, if two active profiles contain different values of the same setting, an ambiguity will occur. This ambiguity is to be avoided through profile priorities: The value of the ambiguous variable will be taken from the profile that has the higher priority (the one that is rated higher in the list of profiles).

Behavior of profiles when policies affect each other through the hierarchy

Profiles with the same name are merged according to the policy merge rules. Profiles of an upstream policy have a higher priority than profiles of a downstream policy. If editing settings is prohibited in the upstream policy (it is locked), the downstream policy uses the profile activation conditions from the upstream one. If editing settings is allowed in the upstream policy, the profile activation conditions from the downstream policy are used.

Since a policy profile may contain the **Device is offline** property in its activation condition, profiles completely replace the feature of policies for out-of-office users, which will no longer be supported.

A policy for out-of-office users may contain profiles, but its profiles can only be activated after the device switches into out-of-office mode.

Inheritance of policy settings

A policy is specified for an administration group. Policy settings can be *inherited*, that is, received in the subgroups (child groups) of the administration group for which they were set. Hereinafter, a policy for a parent group is also referred to as a *parent policy*.

You can enable or disable two options of inheritance: **Inherit settings from parent policy** and **Force inheritance of settings in child policies**:

- If you enable **Inherit settings from parent policy** for a child policy and lock some settings in the parent policy, then you cannot change these settings for the child group. You can, however, change the settings that are not locked in the parent policy.
- If you disable **Inherit settings from parent policy** for a child policy, then you can change all the settings in the child group, even if some settings are locked in the parent policy.
- If you enable **Force inheritance of settings in child policies** in the parent group, this enables the **Inherit settings from parent policy** for each child policy. In this case, you cannot disable this option for any child policy. All the settings that are locked in the parent policy are forcibly inherited in the child groups, and you cannot change these settings in the child groups.
- In policies for the **Managed devices** group, the **Inherit settings from parent policy** does not affect any settings, because the **Managed devices** group does not have any upstream groups and therefore does not inherit any policies.

By default, the **Inherit settings from parent policy** option is enabled for a new policy.

If a policy has profiles, all the child policies inherit these profiles.

Managing policies

The applications installed on client devices are centrally configured by defining policies.

Policies created for applications in an administration group are displayed in the workspace, on the **Policies** tab. Before the name of each policy, an icon with its status (see section "Statuses of devices, tasks, and policies" on page [910](#)) is displayed.

After a policy is deleted or revoked, the application continues working with the settings specified in the policy. Those settings subsequently can be modified manually.

A policy is applied as follows: if a device is running resident tasks (real-time protection tasks), they keep running with the new setting values. Any periodic tasks (on-demand scan, update of application databases) that are started keep running with the values unchanged. Next time, they will be run with the new setting values.

Policies for applications with multitenancy support are inherited to lower-level administration groups as well as to upper-level administration groups: the policy is propagated to all client devices on which the application is installed.

If Administration Servers are structured hierarchically, secondary Administration Servers receive policies from the primary Administration Server and distribute them to client devices. When inheritance is enabled, policy settings can be modified on the primary Administration Server. After this, any changes made to the policy settings are propagated to inherited policies on secondary Administration Servers.

If the connection is terminated between the primary and secondary Administration Servers, the policy on the secondary Server continues, using the applied settings. Policy settings modified on the primary Administration Server are distributed to a secondary Administration Server after the connection is re-established.

If inheritance is disabled, policy settings can be modified on a secondary Administration Server independently from the primary Administration Server.

If the connection between Administration Server and a client device is interrupted, the client device starts running under the out-of-office policy (if it is defined), or the policy keeps running under the applied settings until the connection is re-established.

The results of policy distribution to the secondary Administration Server are displayed in the policy properties window of the console on the primary Administration Server.

The results of policy distribution to client devices are displayed in the policy properties window of the Administration Server to which they are connected.

Do not use private data in policy settings. For example, avoid specifying the domain administrator password.

See also:

Creating a policy	388
Displaying inherited policy in a subgroup	389
Activating a policy	390
Activating a policy automatically at the Virus outbreak event.....	390
Applying an out-of-office policy.....	390
Modifying a policy. Rolling back changes.....	390
Comparing policies	391
Deleting a policy	392
Copying a policy	392
Exporting a policy	392
Importing a policy.....	392
Converting policies	393
Managing policy profiles	393

Creating a policy

In Administration Console, you can create policies directly in the folder of the administration group for which a policy is to be created, or in the workspace of the **Policies** folder.

► *To create a policy in the folder of an administration group:*

1. In the console tree, select an administration group for which you want to create a policy.
2. In the workspace of the group, select the **Policies** tab.
3. Run the New Policy Wizard by clicking the **New policy** button.

The New Policy Wizard starts. Follow the instructions of the Wizard.

► *To create a policy in the workspace of the **Policies** folder:*

1. In the console tree, select the **Policies** folder.
2. Run the New Policy Wizard by clicking the **New policy** button.


The New Policy Wizard starts. Follow the instructions of the Wizard.

You can create several policies for one application from the group, but only one policy can be active at a time. When you create a new active policy, the previous active policy becomes inactive.

When creating a policy, you can specify a minimum set of parameters required for the application to function properly. All other values are set to the default values applied during the local installation of the application. You can change the policy after it is created.

Do not use private data in policy settings. For example, avoid specifying the domain administrator password.

Settings of Kaspersky applications that are changed after policies are applied are described in detail in their respective Guides.



After the policy is created, the settings locked from editing (marked with the  lock) take effect on client devices regardless of which settings were previously specified for the application.

Displaying inherited policy in a subgroup

► *To enable the display of inherited policies for a nested administration group:*

1. In the console tree, select the administration group for which inherited policies have to be displayed.
2. In the workspace of the selected group, select the **Policies** tab.
3. In the context menu of the list of policies, select **View** → **Inherited policies**.

Inherited policies are displayed in the list of policies with the following icon:

-  —If they were inherited from a group created on the primary Administration Server.
-  —If they were inherited from a top-level group.

When the settings inheritance mode is enabled, inherited policies are only available for modification in the group in which they were created. Modification of inherited policies is not available in the group that inherits them.

Activating a policy

► *To make a policy active for the selected group:*

1. In the workspace of the group, on the **Policies** tab select the policy that you have to make active.
2. To activate the policy, perform one of the following actions:
 - From the context menu of the policy select **Active policy**.
 - In the policy properties window open the **General** section and select **Active policy** from the **Policy status** settings group.

The policy becomes active for the selected administration group.

When a policy is applied to a large number of client devices, both the load on the Administration Server and the network traffic increase significantly for some time.

Activating a policy automatically at the Virus outbreak event

► *To make a policy perform automatic activation at a Virus outbreak event:*

1. In the Administration Server properties window, open the **Virus outbreak** section.
2. Open the **Policy activation** window by clicking the **Configure policies to activate when a Virus outbreak event occurs** link and add the policy to the selected list of policies that are activated when a virus outbreak is detected.

If a policy has been activated on the *Virus outbreak* event, you can return to the previous policy only by using the manual mode.

Applying an out-of-office policy

The out-of-office policy takes effect on a device if it is disconnected from the corporate network.

► *To apply out-of-office policy:*

In the policy properties window, open the **General** section and in the **Policy status** settings group, select **Out-of-office policy**.

The out-of-office policy will be applied to the devices if they are disconnected from the corporate network.

Modifying a policy. Rolling back changes

► *To edit a policy:*

1. In the console tree, select the **Policies** folder.
2. In the workspace of the **Policies** folder, select a policy and proceed to the policy properties window using the context menu.

3. Make the relevant changes.
4. Click **Apply**.

The changes made to the policy will be saved in the policy properties, in the **Revision history** section.

You can roll back changes made to the policy, if necessary.

► *To roll back changes made to the policy:*

1. In the console tree, select the **Policies** folder.
2. Select the policy in which changes must to be rolled back, and proceed to the policy properties window using the context menu.
3. In the policy properties window, select the **Revision history** section.
4. In the list of policy revisions, select the number of the revision to which you need to roll back changes.
5. Click the **Advanced** button and select the **Roll back** value in the drop-down list.

Comparing policies

You can compare two policies for a single managed application. After the comparison, you have a report that displays which policy settings match and which settings differ. For example, you may have to compare policies if different administrators in their respective offices have created multiple policies for a single managed application, or if a single top-level policy has been inherited by all local offices and modified for each office. You can compare policies in one of the following ways: by selecting one policy and comparing it to another, or by comparing any two policies from the list of policies.

► *To compare one policy to another:*

1. In the console tree, select the **Policies** folder.
2. In the workspace of the **Policies** folder, select the policy that you require to compare to another.
3. In the context menu of the policy, select **Compare policy to another policy**.
4. In the **Select policy** window, select the policy to which your policy must be compared.
5. Click **OK**.

A report in HTML format is displayed for the comparison of the two policies for the same application.

► *To compare any two policies from the list of policies:*

1. In the **Policies** folder, in the list of policies, use the **SHIFT** or **CTRL** key to select two policies for a single managed application.
2. In the context menu, select **Compare**.

A report in HTML format is displayed for the comparison of the two policies for the same application.

The report on comparison of policy settings for Kaspersky Endpoint Security for Windows also provides details of the comparison of policy profiles. You can minimize the results of policy profile comparison. To minimize the section, click the ▲ icon next to the section name.

Deleting a policy

► To delete a policy:

1. In the workspace of an administration group, on the **Policies** tab, select the policy that you want to delete.
2. Delete the policy in one of the following ways:
 - By selecting **Delete** in the context menu of the policy.
 - By clicking the **Delete policy** link in the information box for the selected policy.

Copying a policy

► To copy a policy:

1. In the workspace of the required group, on the **Policies** tab select a policy.
2. From the context menu of the policy select **Copy**.
3. In the console tree, select a group to which you want to add the policy.

You can add a policy to the group from which it was copied.

4. From the context menu of the list of policies for the selected group, on the **Policies** tab select **Paste**.

The policy is copied with all its settings and is applied to the devices within the group to which it was copied. If you paste the policy into the same group from which it has been copied, the (**<next sequence number>**) index is automatically added to the policy name, for example: **(1)**, **(2)**.

An active policy becomes inactive while it is copied. If necessary, you can make it active.

Exporting a policy

► To export a policy:

1. Export a policy in one of the following ways:
 - By selecting **All tasks** → **Export** in the context menu of the policy.
 - By clicking the **Export policy to file** link in the information box for the selected policy.
2. In the **Save as** window that opens, specify the policy file name and path. Click the **Save** button.

Importing a policy

► To import a policy:

1. In the workspace of the relevant group, on the **Policies** tab select one of the following ways of importing policies:
 - By selecting **All tasks** → **Import** in the context menu of the list of policies.
 - By clicking the **Import policy from file** button in the management block for policy list.

2. In the window that opens, specify the path to the file from which you want to import a policy. Click the **Open** button.

The policy is then displayed in the list of policies.

If a policy with the name identical to that of the newly imported policy already exists in the list of policies, the name of the imported policy is expanded with the (<next sequence number>) index, for example: (1), (2).

Converting policies

Kaspersky Security Center can convert policies from earlier versions of Kaspersky applications into those from up-to-date versions of the same applications.

Conversion is available for policies of the following applications:

- Kaspersky Anti-Virus 6.0 for Windows Workstations MP4.
- Kaspersky Endpoint Security 8 for Windows.
- Kaspersky Endpoint Security 10 for Windows.

► *To convert policies:*

1. In the console tree select the Administration Server for which you want to convert policies.
2. In the Administration Server context menu, select **All Tasks** → **Policies and Tasks Batch Conversion Wizard**.

The Policies and Tasks Batch Conversion Wizard starts. Follow the instructions of the Wizard.

After the wizard completes, new policies are created that use the settings of policies from earlier versions of Kaspersky applications.

Managing policy profiles

This section describes managing policy profiles and provides information about viewing the profiles of a policy, changing a policy profile priority, creating a policy profile, modifying a policy profile, copying a policy profile, creating a policy profile activation rule, and deleting a policy profile.

In this section

About the policy profile	394
Creating a policy profile	395
Modifying a policy profile	396
Removing a policy profile.....	397
Creating a policy profile activation rule.....	397

About the policy profile

Policy profile is a named collection of settings of a policy that is activated on a client device (computer or mobile device) when the device satisfies specified activation rules (see section "Creating a policy profile activation rule" on page [397](#)). Activation of a profile modifies the policy settings that were active on the device before the profile was activated. Those settings take values that have been specified in the profile.

Policy profiles are necessary for devices within a single administration group to run under different policy settings. For example, a situation may occur when policy settings have to be modified for some devices in an administration group. In this case, you can configure policy profiles for such a policy, which allows you to edit policy settings for selected devices in the administration group. For example, the policy prohibits running any GPS navigation software on all devices in the Users administration group. GPS navigation software is necessary only on a single device in the Users administration group—the device owned by the user employed as a courier. You can tag that device as simply "Courier" and reconfigure the policy profile so that it allows GPS navigation software to run only on the device tagged as "Courier", while preserving all the remaining policy settings. In this case, if a device tagged as "Courier" appears in the Users administration group, it will be allowed to run GPS navigation software. Running GPS navigation software will still be prohibited on other devices in the Users administration group unless they are tagged as "Courier", too.

Profiles are only supported by the following policies:

- Policies of Kaspersky Endpoint Security 10 Service Pack 1 for Windows or later
- Policies of Kaspersky Endpoint Security 10 Service Pack 1 for Mac
- Policies of the Kaspersky Mobile Device Management plug-in ranging from version 10 Service Pack 1 to version 10 Service Pack 3 Maintenance Release 1
- Policies of the Kaspersky Device Management for iOS plug-in
- Policies of Kaspersky Security for Virtualization 5.1 Light Agent for Windows
- Policies of Kaspersky Security for Virtualization 5.1 Light Agent for Linux

Policy profiles simplify the management of the client devices that the policies apply to:

- The policy profile settings may differ from the policy settings.
- You do not have to maintain and manually apply several instances of a single policy that differ only by a few settings.
- You do not have to allocate a separate policy for out-of-office users.
- You can export and import policy profiles, as well as create new policy profiles based on existing ones.
- A single policy can have multiple active policy profiles. Only profiles that meet the activation rules effective on the device will be applied to that device.
- Profiles are subject to the policy hierarchy. An inherited policy includes all profiles of the higher-level policy.

Priorities of profiles

Profiles that have been created for a policy are sorted in descending order of priority. For example, if profile X is higher in the list of profiles than profile Y, then X has a higher priority than the latter. Multiple profiles can be simultaneously applied to a single device. If values of a setting vary in different profiles, the value from the highest-priority profile will be applied on the device.

Profile activation rules

A policy profile is activated on a client device when an activation rule is triggered. *Activation rules* are a set of conditions that, when met, start the policy profile on a device. An activation rule can contain the following

conditions:

- Network Agent on a client device connects to the Administration Server that has a specified set of connection settings, such as Administration Server address, port number, and so forth.
- The client device is offline.
- The client device has been assigned specified tags.
- The client device is explicitly (the device is immediately located in the specified unit) or implicitly (the device is located in a unit that is in the specified unit at any nesting level) located in a specific unit of Active Directory®, the device or its owner is located in a security group of Active Directory.
- The client device belongs to a specified owner, or the owner of the device is included in an internal security group of Kaspersky Security Center.
- The owner of the client device has been assigned a specified role.

Policies in the hierarchy of administration groups

If you are creating a policy in a low-level administration group, this new policy inherits all profiles of the active policy from the higher-level group. Profiles with identical names are merged. Policy profiles for the higher-level group have the higher priority. For example, in administration group *A*, policy *P(A)* has profiles *X1*, *X2*, and *X3* (in descending order of priority). In administration group *B*, which is a subgroup of group *A*, policy *P(B)* has been created with profiles *X2*, *X4*, *X5*. Then policy *P(B)* will be modified with policy *P(A)* so that the list of profiles in policy *P(B)* will appear as follows: *X1*, *X2*, *X3*, *X4*, *X5* (in descending order of priority). The priority of profile *X2* will depend on the initial state of *X2* of policy *P(B)* and *X2* of policy *P(A)*. After the policy *P(B)* is created, the policy *P(A)* is no longer displayed in subgroup *B*.

The active policy is recalculated every time you run Network Agent, enable and disable offline mode, or edit the list of tags assigned to the client device. For example, the RAM size has been increased on the device, which, in turn, has activated the policy profile that is applied on devices with large RAM size.

Properties and restrictions of policy profiles

Profiles have the following properties:

- Profiles of an inactive policy have no impact on client devices.
- If a policy is set to the **Out-of-office policy** status, profiles of the policy will also be applied when a device is disconnected from the corporate network.
- Profiles do not support static analysis of access to executable files (see section "Viewing the results of static analysis of startup rules applied to executable files" on page [495](#)).
- A policy profile cannot contain any settings of event notifications.
- If UDP port 15000 is used for connecting a device to Administration Server, the corresponding policy profile is activated within one minute after you assign a tag to the device.
- You can use rules for Network Agent connection to the Administration Server (see section "Creating a Network Agent switching rule by network location" on page [292](#)), when you create policy profile activation rules.

Creating a policy profile

Profile creation is available only for the policies of the following applications:

- Kaspersky Endpoint Security 10 Service Pack 1 for Windows and later versions
- Kaspersky Endpoint Security 10 Service Pack 1 for Mac

- Kaspersky Mobile Device Management plug-in versions 10 Service Pack 1 to 10 Service Pack 3 Maintenance Release 1
- Kaspersky Device Management for iOS plug-in
- Kaspersky Security for Virtualization 5.1 Light Agent for Windows and Linux

► *To create a policy profile:*

1. In the console tree, select the administration group for whose policy you have to create a policy profile.
2. In the workspace of the administration group, select the **Policies** tab.
3. Select a policy and switch to the policy properties window using the context menu.
4. Open the **Policy profiles** section in the policy properties window and click the **Add** button.
The New Policy Profile Wizard starts.
5. In the **Policy profile name** window of the Wizard, specify the following:
 - a. Name of the policy profile
The profile name cannot include more than 100 characters.
 - b. Policy profile status (*Enabled* or *Disabled*)
We recommend that you create and enable inactive policy profiles only after you are completely finished with the settings and conditions of policy profile activation.
6. Select the **After closing the New Policy Profile Wizard, proceed to configuring the policy profile activation rule** check box to start the New Policy Profile Activation Rule Wizard (see section "Creating a policy profile activation rule" on page [397](#)). Follow the Wizard steps.
7. Edit the policy profile settings in the policy profile properties window (see section "Modifying a policy profile" on page [396](#)), in the way you require.
8. Save the changes by clicking **OK**.

The profile is saved. The profile will be activated on devices that meet the activation rules.

You can create multiple profiles for a single policy. Profiles that have been created for a policy are displayed in the policy properties, in the **Policy profiles** section. You can modify a policy profile and change the profile priority (see section "Modifying a policy profile" on page [396](#)), as well as remove the profile (see section "Removing a policy profile" on page [397](#)).

Modifying a policy profile

Editing the settings of a policy profile

The capability to edit a policy profile is only available for policies of Kaspersky Endpoint Security for Windows.

► *To modify a policy profile:*

1. In the console tree, select the administration group for which the policy profile has to be modified.
2. In the workspace of the group, select the **Policies** tab.
3. Select a policy and switch to the policy properties window using the context menu.

4. Open the **Policy profiles** section in the policy properties.

This section contains a list of profiles that have been created for the policy. Profiles are displayed in the list in accordance with their priorities.

5. Select a policy profile and click the **Properties** button.
6. Configure the profile in the properties window:
 - If necessary, in the **General** section, change the profile name and enable or disable the profile using the **Enable profile** check box.
 - In the **Activation rules** section, edit the profile activation rules.
 - Edit the policy settings in the corresponding sections.
7. Click **OK**.

The modified settings will take effect either after the device is synchronized with the Administration Server (if the policy profile is active), or after an activation rule is triggered (if the policy profile is inactive).



Changing the priority of a policy profile

The priorities of policy profiles define the activation order of profiles on a client device. Priorities are used if identical activation rules are set for different policy profiles.

For example, two policy profiles have been created: *Profile 1* and *Profile 2* that differ by the respective values of a single setting (*Value 1* and *Value 2*). The priority of *Profile 1* is higher than that of *Profile 2*. Moreover, there are also profiles with priorities that are lower than that of *Profile 2*. The activation rules for those profiles are identical.

When an activation rule is triggered, *Profile 1* will be activated. The setting on the device will take *Value 1*. If you remove *Profile 1*, then *Profile 2* will have the highest priority, so the setting will take *Value 2*.

On the list of policy profiles, profiles are displayed in accordance with their respective priorities. The profile with the

highest priority is ranked first. You can change the priority of a profile using the  and  buttons.

Removing a policy profile

► *To remove a policy profile:*

1. In the console tree, select the administration group whose policy profile you want to remove.
2. In the workspace of the administration group, select the **Policies** tab.
3. Select a policy and switch to the policy properties window using the context menu.
4. Open the **Policy profiles** section in the properties of the policy of Kaspersky Endpoint Security.
5. Select the policy profile that you want to remove and click the **Delete** button.

The policy profile will be removed. The active status will pass either to another policy profile whose activation rules are triggered on the device, or to the policy.

Creating a policy profile activation rule

► *To create a policy profile activation rule:*

1. In the console tree, select the administration group for which you have to create a policy profile activation rule.

2. In the workspace of the group, select the **Policies** tab.
3. Select a policy and switch to the policy properties window using the context menu.
4. Select the **Policy profiles** section in the policy properties window.
5. Select the policy profile for which you need to create an activation rule, and click the **Properties** button.

The policy profile properties window opens.

If the list of policy profiles is empty, you can create a policy profile (see section "Creating a policy profile" on page [395](#)).

6. Select the **Activation rules** section, and click the **Add** button.
The New Policy Profile Activation Rule Wizard starts.
7. In the **Policy profile activation rules** window, select the check boxes next to the conditions that must affect activation of the policy profile that you are creating:

- **General rules for policy profile activation**

Select this check box to set up policy profile activation rules on the device depending on the status of the device offline mode, rule for connection to Administration Server, and tags assigned to the device.

- **Rules for Active Directory usage**

Select this check box to set up rules for policy profile activation on the device depending on the presence of the device in an Active Directory organizational unit (OU), or on membership of the device (or its owner) in an Active Directory security group.

- **Rules for a specific device owner**

Select this check box to set up rules for policy profile activation on the device depending on the device owner.

- **Rules for hardware specifications**

Select this check box to set up rules for policy profile activation on the device depending on the memory volume and the number of logical processors.

The number of additional windows of the Wizard depends on the settings that you select at this step. You can modify policy profile activation rules later.

8. In the **General conditions** window, specify the following settings:
 - In the **Device is offline** field, in the drop-down list specify the condition for device presence on the network:
 - **Yes**
The device is in an external network, which means that the Administration Server is not available.
 - **No**
The device is on the network, so the Administration Server is available.
 - **No value is selected**
The criterion will not be applied.
 - In the **The device is in the specified network location** box, use the drop-down lists to set up the policy profile activation if the Administration Server connection rule is executed / not executed on this device:

- **Executed / Not executed**

Condition of policy profile activation (whether the rule is executed or not).

- **Rule name**

Network location description of the device for connection to the Administration Server, whose conditions must be met (or must not be met) for activation of the policy profile.

A network location description of devices for connection to an Administration Server can be created or configured in a Network Agent switching rule.

The **General conditions** window is displayed if the **General rules for policy profile activation** check box is selected.

9. In the **Conditions using tags** window, specify the following settings:

- **Tag list**

In the list of tags, specify the rule for device inclusion in the policy profile by selecting the check boxes next to the relevant tags.

You can add new tags to the list by entering them in the field over the list and clicking the **Add** button.

The policy profile includes devices with descriptions containing all the selected tags. If check boxes are cleared, the criterion is not applied. By default, these check boxes are cleared.

- **Apply to devices without the specified tags**

Select this check box if you have to invert your selection of tags.

If this check box is selected, the policy profile includes devices with descriptions that contain none of the selected tags. If this check box is cleared, the criterion is not applied. By default, this check box is cleared.

The **Conditions using tags** window is displayed if the **General rules for policy profile activation** check box is selected.

10. In the **Conditions using Active Directory** window, specify the following settings:

- **Device owner's membership in Active Directory security group**

If this check box is selected, the policy profile is activated on the device whose owner is a member of the specified security group. If this check box is cleared, the profile activation criterion is not applied. By default, this check box is cleared.

- **Device membership in Active Directory security group**

If this check box is selected, the policy profile is activated on the device. If this check box is cleared, the profile activation criterion is not applied. By default, this check box is cleared.

- **Device allocation in Active Directory organizational unit**

If this check box is selected, the policy profile is activated on the device, which is included in the specified Active Directory OU. If this check box is cleared, the profile activation criterion is not applied. By default, this check box is cleared.

The **Conditions using Active Directory** window is displayed if the **Rules for Active Directory usage** check box is selected.

1. In the **Conditions using the device owner** window, specify the following settings:

- **Device owner**

Select this check box to configure and enable the rule for profile activation on the device according to its owner. In the drop-down list under this check box, you can select a criterion for the profile activation:

- The device belongs to the specified owner ("=" sign).
- The device does not belong to the specified owner ("#" sign).

If this check box is selected, the profile is activated on the device in accordance with the criterion configured. You can specify the device owner when the check box is selected. If this check box is cleared, the profile activation criterion is not applied. By default, this check box is cleared.

- **The device owner is included in an internal security group**

Select this check box to configure and enable the rule of profile activation on the device by the owner's membership in an internal security group of Kaspersky Security Center. In the drop-down list under this check box, you can select a criterion for the profile activation:

- The device owner is a member of the specified security group ("=" sign).
- The device owner is not a member of the specified security group ("#" sign).

If this check box is selected, the profile is activated on the device in accordance with the criterion configured. You can specify a security group of Kaspersky Security Center when this check box is selected. If this check box is cleared, the profile activation criterion is not applied. By default, this check box is cleared.

- **Activate policy profile by specific role of device owner**

Select this option to configure and enable the rule of profile activation on the device depending on the owner's role (see section "Configuring access rights to application features. Role-based access control" on page [683](#)). Add the role manually from the list of existing roles.

If this option is enabled, the profile is activated on the device in accordance with the criterion configured.

The **Conditions using the device owner** window opens if the **Rules for a specific device owner** check box is selected.

1. In the **Conditions using equipment specifications** window, specify the following settings:

- **RAM size, in MB**

Select this check box to configure and enable the rule of profile activation on the device by the RAM volume available on that device. In the drop-down list under this check box, you can select a criterion for the profile activation:

- The device RAM size is less than the specified value ("<" sign).
- The device RAM size is greater than the specified value (">" sign).

If this check box is selected, the profile is activated on the device in accordance with the criterion configured. When this check box is selected, you can specify the RAM volume

on the device. If this check box is cleared, the profile activation criterion is not applied. By default, this check box is cleared.

- **Number of logical processors**

Select this check box to configure and enable the rule of profile activation on the device by the number of logical processors on that device. In the drop-down list under this check box, you can select a criterion for the profile activation:

- The number of logical processors on the device is less than or equal to the specified value (" $<$ " sign).
- The number of logical processors on the device is greater than or equal to the specified value (" $>$ " sign).

If this check box is selected, the profile is activated on the device in accordance with the criterion configured. When this check box is selected, you can specify the number of logical processors on the device. If this check box is cleared, the profile activation criterion is not applied. By default, this check box is cleared.

The **Conditions using equipment specifications** window is displayed if the **Rules for hardware specifications** check box is selected.

2. In the **Name of policy profile activation rule** window, in the **Rule name** field, specify a name for the rule.

The profile will be saved. The profile will be activated on the device when activation rules are triggered.

Policy profile activation rules created for the profile are displayed in the policy profile properties in the **Activation rules** section. You can modify or remove any policy profile activation rule.

Multiple activation rules can be triggered simultaneously.

Device moving rules

It is advisable to set automatic allocation of devices to administration groups through *device moving rules*. A device moving rule consists of three main parts: a name, an execution condition (logical expression with the device attributes), and a target administration group. A rule moves a device to the target administration group if the device attributes meet the rule execution condition.

All device moving rules have priorities. The Administration Server checks the device attributes as to whether they meet the execution condition of each rule, in ascending order of priority. If the device attributes meet the execution condition of a rule, the device is moved to the target group, so the rule processing is complete for this device. If the device attributes meet the conditions of multiple rules, the device is moved to the target group of the rule with the highest priority (that is, has the highest rank in the list of rules).

Device moving rules can be created implicitly. For example, in the properties of an installation package or a remote installation task, you can specify the administration group to which the device must be moved after Network Agent is installed on it. Also, device moving rules can be created explicitly by the administrator of Kaspersky Security Center, in the list of moving rules. The list is located in Administration Console, in the properties of the **Unassigned devices** group.

By default, a device moving rule is intended for one-time initial allocation of devices to administration groups. The rule moves devices from the **Unassigned devices** group only once. If a device once was moved by this rule, the rule will never move it again, even if you return the device to the **Unassigned devices** group manually. This is the recommended way of applying moving rules.

You can move devices that have already been allocated to some of the administration groups. To do this, in the properties of a rule, clear the **Move only devices that do not belong to an administration group** check box.

Applying moving rules to devices that have already been allocated to some of the administration groups, significantly increases the load on the Administration Server.

You can create a moving rule that would affect a single device repeatedly.

We strongly recommend that you avoid moving a single device from one group to another repeatedly (for example, in order to apply a special policy to that device, run a special group task, or update the device through a specific distribution point).

Such scenarios are not supported, because they increase the load on Administration Server and network traffic to an extreme degree. These scenarios also conflict with the operating principles of Kaspersky Security Center (particularly in the area of access rights, events, and reports). Another solution must be found, for example, through the use of policy profiles (on page [385](#)), tasks for device selections (see section "Tasks" on page [52](#)), assignment of Network Agents according to the standard scenario (see section "Adjustment of distribution points and connection gateways" on page [587](#)), and so on.

See also:

Scenario: Discovering networked devices.....	303
--	---------------------

Cloning device moving rules

When you have to create multiple device-moving rules with similar settings, you can clone an existing rule and then change the settings of the cloned rule. For example, this is useful when you must have several identical device-moving rules with different IP ranges and target groups.

► *To clone a device moving rule:*

1. Open the main application window.
2. In the **Unassigned devices** folder, click **Configure rules**.
The **Properties: Unassigned devices** window opens.
3. In the **Move devices** section, select the device moving rule that you want to clone.
4. Click **Clone rule**.

A clone of the selected device moving rule will be added at the end of the list.

A new rule is created in the disabled state. You can edit and enable the rule at any time.

Software categorization

The main tool for monitoring the running of applications are *Kaspersky categories* (hereinafter also referred to as *KL categories*). KL categories help Kaspersky Security Center administrators to simplify the support of software categorization and minimize traffic going to managed devices.

User categories must only be created for applications that cannot be classified in any of the existing KL categories (for example, for custom-made software). User categories are created on the basis of an application installation package (MSI) or a folder with installation packages.

If a large collection of software is available, which has not been categorized through KL categories, it may be useful to create an automatically updated category. The checksums of executable files will be automatically added to this category on every modification of the folder containing distribution packages.

No automatically updated categories of software can be created on the basis of the folders My Documents, %windir%, and %ProgramFiles%. The pool of files in these folders is subject to frequent changes, which leads to an increased load on Administration Server and increased network traffic. You must create a dedicated folder with the collection of software and periodically add new items to it.

Prerequisites for installing applications on devices of a client organization

The process of remote installation of applications on devices of a client organization is identical to the remote installation process within an enterprise (see section "Kaspersky applications. Centralized deployment" on page [332](#)).

To install applications on devices of a client organization, the following actions must be performed:

- Before installing applications on devices of the client organization for the first time, install Network Agent on them.

When configuring the Network Agent installation package by the service provider, in Kaspersky Security Center, adjust the following settings in the properties window of the installation package:

- In the **Connection** section, in the **Administration Server** string, specify the address of the same virtual Administration Server that was specified during local installation of Network Agent on the distribution point.
- In the **Advanced** section, select the **Connect to Administration Server by using connection gateway** check box. In the **Connection gateway address** string, specify the distribution point address. You can use either the device IP address or device name in the Windows network.
- Select **Using operating system resources through distribution points** as the download method for the Network Agent installation package. You can select the download method as follows:
 - If you install application by using the remote installation task, you can specify the download method in one of the following ways:
 - When creating a remote installation task in the **Settings** window
 - In the remote installation task properties window, through the **Settings** section

- If you install applications using the Remote Installation Wizard, you can select the download method in the **Settings** window of this Wizard.
- The account used by the distribution point for authorization must have access to the Admin\$ resource on all client devices.

Viewing and editing local application settings

The Kaspersky Security Center administration system allows you to remotely manage local application settings on devices through Administration Console.

Local application settings are the settings of an application that are specific for a device. You can use Kaspersky Security Center to set local application settings for devices included in administration groups.

Detailed descriptions of settings of Kaspersky applications are provided in respective Guides.

► *To view or change the local settings of an application:*

1. In the workspace of the group to which the relevant device belongs, select the **Devices** tab.
2. In the device properties window, in the **Applications** section, select the relevant application.
3. Open the application properties window by double-clicking the application name or by clicking the **Properties** button.

The local settings window of the selected application opens so that you can view and edit those settings.

You can change the values of settings that have not been barred from modification by a group policy (that is, those not marked with the lock (🔒) in a policy).

Updating Kaspersky Security Center and managed applications

This section describes steps you must take to update Kaspersky Security Center and managed applications.

In this chapter

Scenario: Upgrading Kaspersky Security Center and managed applications	405
About updating Kaspersky databases, software modules, and applications	406
Using diff files for updating Kaspersky databases and software modules	412
Creating the task for downloading updates to the repository of the Administration Server	413
Creating the Downloading updates to the repositories of distribution points task	417
Configuring the Download updates to the repository of the Administration Server task	421
Verifying downloaded updates	422
Configuring test policies and auxiliary tasks	423
Viewing downloaded updates	424
Automatic distribution of updates	424
Deleting software updates from the repository	431
Algorithm of patch installation for a Kaspersky application in cluster mode	431

Scenario: Upgrading Kaspersky Security Center and managed applications

This section describes the main brief scenario for Kaspersky Security Center upgrade.

The Kaspersky Security Center deployment scenario proceeds in stages:

a. Planning the resources

Make sure that you have enough disk space to create the backup of the Administration Server data.

b. Getting the installer file for Kaspersky Security Center

Get the executable file for the current version of Kaspersky Security Center and save it on the device that will work as the Administration Server. Read the Release Notes of the current version of Kaspersky Security Center.

c. Creating a backup copy of the previous version

Use the data backup and recovery utility (see section "Data backup and recovery utility (klbackup)" on page [618](#)) to create a backup copy of the Administration Server data.

d. Running the installer

Run the executable file for version 13 (see section "Custom installation" on page [232](#)). When running the file, specify that you have a backup copy and specify its location. Your data will be restored from the backup.

e. Upgrading the managed applications

You can upgrade the application if there is a newer version available. Make sure that the version of Kaspersky Security Center is compatible with this application. Then perform the upgrade of the application as described in its Release Notes.

See also:

Ports used by Kaspersky Security Center	65
Interaction of Kaspersky Security Center components and security applications: more information.....	108
Basic concepts.....	44
Architecture.....	58

About updating Kaspersky databases, software modules, and applications

To be sure that the protection of your Administration Servers and managed devices is up-to-date, you must provide timely updates of the following:

- Kaspersky databases and software modules
- Installed Kaspersky applications, including Kaspersky Security Center components and security applications

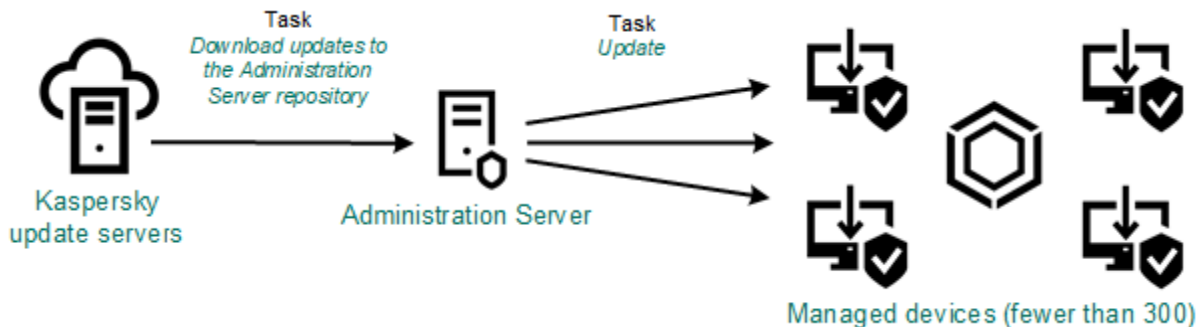
Depending on the configuration of your network, you can use the following schemes of downloading and distributing the required updates to the managed devices:

- Using the *Download updates to the Administration Server repository* task
- Using two tasks:
 - The *Download updates to the Administration Server repository* task
 - The *Download updates to the repositories of distribution points* task
- Manually through a local folder, a shared folder, or an FTP server
- Directly from Kaspersky update servers to Kaspersky Endpoint Security for Windows on the managed devices

Using the Download updates to the Administration Server repository task

In this scheme, Kaspersky Security Center downloads updates through the *Download updates to the Administration Server repository* task. In small networks that contain less than 300 managed devices in a single network segment

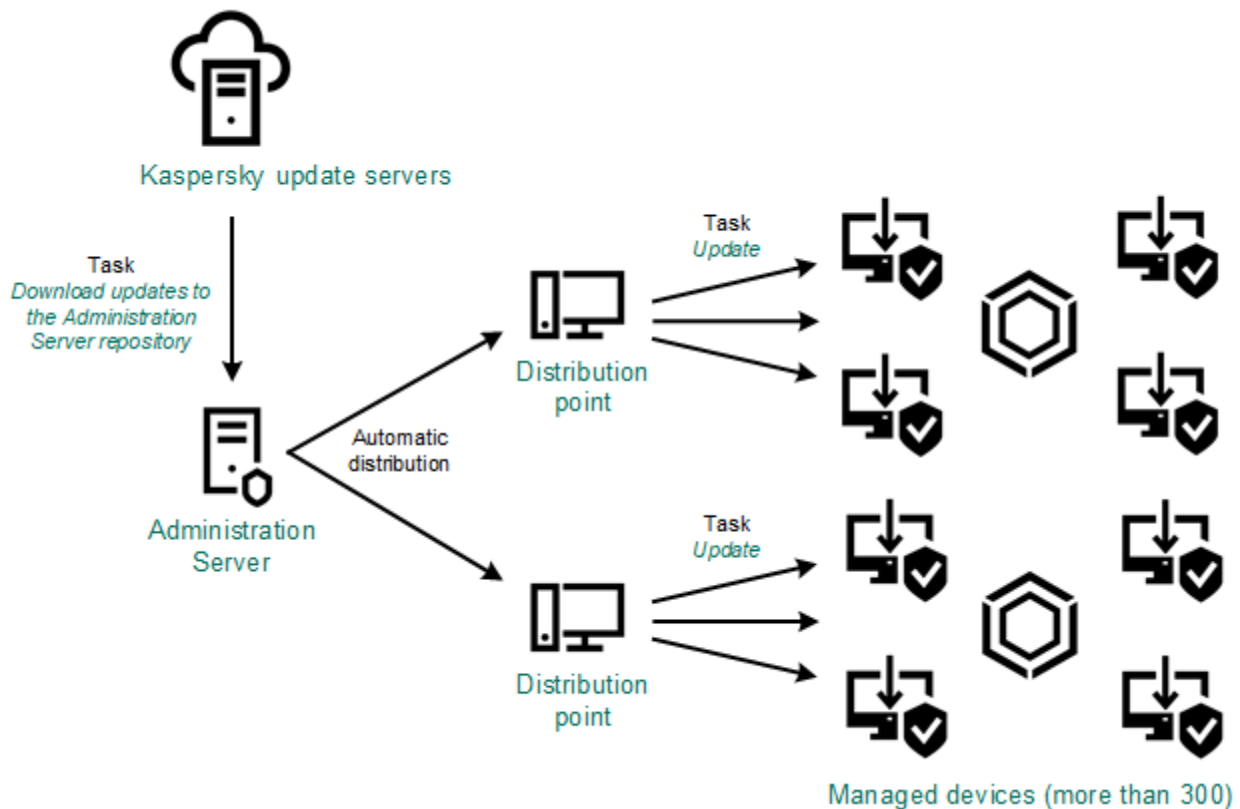
or less than 10 managed devices in each network segment, the updates are distributed to the managed devices directly from the Administration Server repository (see figure below).



By default, the Administration Server communicates with Kaspersky update servers and downloads updates by using the HTTPS protocol. You can configure the Administration Server to use the HTTP protocol instead of HTTPS.

If your network contains more than 300 managed devices in a single network segment or if your network consists of several network segments with more than 9 managed devices in each network segment, we recommend that you use distribution points (see section "About distribution points" on page [133](#)) to propagate the updates to the managed devices (see figure below). Distribution points reduce the load on the Administration Server and optimize traffic between the Administration Server and the managed devices. You can calculate (see section "Calculating the number and configuration of distribution points" on page [134](#)) the number and configuration of distribution points required for your network.

In this scheme, the updates are automatically downloaded from the Administration Server repository to the repositories of the distribution points. The managed devices included in the scope of a distribution point download the updates from the repository of the distribution point instead of the Administration Server repository.



When the *Download updates to the Administration Server repository* task is complete, the following updates are downloaded to the Administration Server repository:

- Kaspersky databases and software modules for Kaspersky Security Center
These updates are installed automatically.
- Kaspersky databases and software modules for the security applications on the managed devices
These updates are installed through the Update task for Kaspersky Endpoint Security for Windows (see section "Automatic installation of updates for Kaspersky Endpoint Security for Windows" on page [1195](#)).
- Updates for the Administration Server
These updates are not installed automatically. The administrator must explicitly approve and run installation of the updates.

Local administrator rights are required for installing patches on the Administration Server.

- Updates for the components of Kaspersky Security Center
By default, these updates are installed automatically. You can change the settings in the Network Agent policy (see section "Enabling and disabling automatic updating and patching for Kaspersky Security Center components" on page [1194](#)).
- Updates for the security applications

By default, Kaspersky Endpoint Security for Windows installs only those updates that you approve (see section "Approving and declining software updates" on page [1197](#)). The updates are installed through the Update task and can be configured in the properties of this task.

The Download updates to the repository of the Administration Server task is not available on virtual Administration Servers. The repository of the virtual Administration Server displays updates downloaded to the primary Administration Server.

You can configure the updates to be verified for operability and errors on a set of test devices. If the verification is successful, the updates are distributed to other managed devices.

Each Kaspersky application requests required updates from Administration Server. Administration Server aggregates these requests and downloads only those updates that are requested by any application. This ensures that the same updates are not downloaded multiple times and that unnecessary updates are not downloaded at all. When running the *Download updates to the Administration Server repository* task, Administration Server sends the following information to Kaspersky update servers automatically in order to ensure the downloading of relevant versions of Kaspersky databases and software modules:

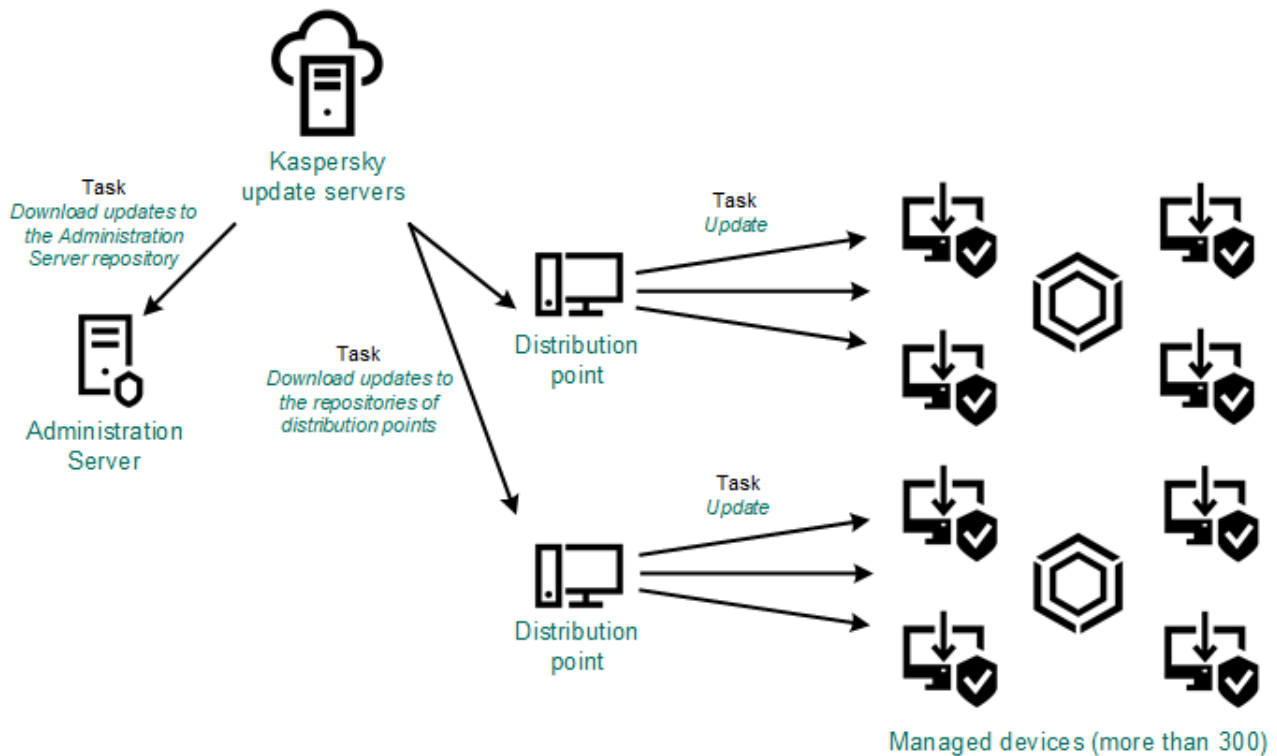
- Application ID and version
- Application setup ID
- Active key ID
- *Download updates to the repository of the Administration Server* task run ID

None of the transmitted information contains personal or other confidential data. AO Kaspersky Lab protects information in accordance with requirements established by law.

Using two tasks: the Download updates to the Administration Server repository task and the Download updates to the repositories of distribution points task

You can download updates to the repositories of distribution points directly from the Kaspersky update servers instead of the Administration Server repository, and then distribute the updates to the managed devices (see figure below). Download to the repositories of distribution points is preferable if the traffic between the Administration

Server and the distribution points is more expensive than the traffic between the distribution points and Kaspersky update servers, or if your Administration Server does not have Internet access.



By default, the Administration Server and distribution points communicate with Kaspersky update servers and download updates by using the HTTPS protocol. You can configure the Administration Server and/or distribution points to use the HTTP protocol instead of HTTPS.

To implement this scheme, create the *Download updates to the repositories of distribution points* task in addition to the *Download updates to the Administration Server repository* task. After that the distribution points will download updates from Kaspersky update servers, and not from the Administration Server repository.

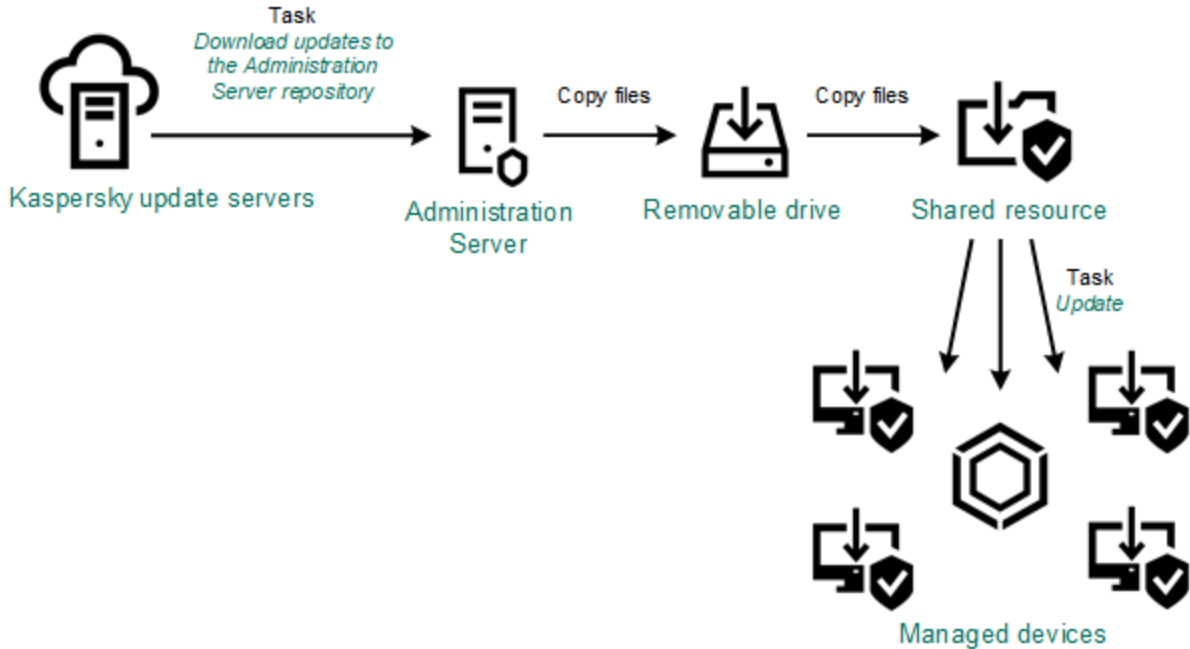
The *Download updates to the repositories of distribution points* task works only on distribution point devices running Windows. Distribution point devices running Linux or macOS cannot download updates from Kaspersky update servers.

If one or more devices running Linux or macOS are within the scope of the *Download updates to the repositories of distribution points* task, the task completes with the *Failed* status, even if it has successfully completed on all Windows devices.

The *Download updates to the Administration Server repository* task is also required for this scheme, because this task is used to download Kaspersky databases and software modules for Kaspersky Security Center.

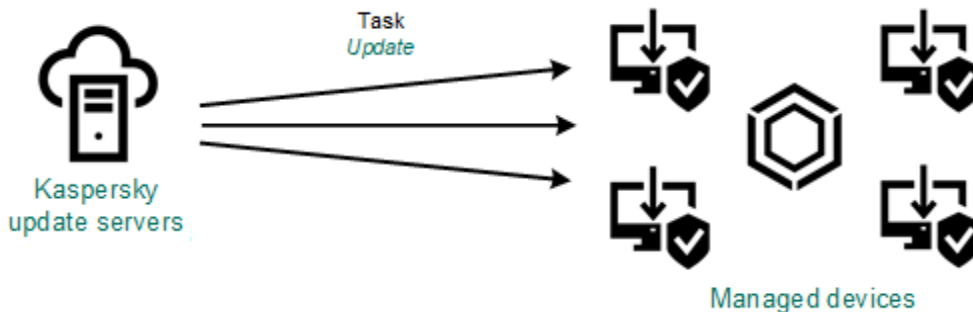
Manually through a local folder, a shared folder, or an FTP server

If the client devices do not have a connection to the Administration Server, you can use a local folder or a shared resource as a source for updating Kaspersky databases, software modules, and applications (see section "Updating Kaspersky databases and software modules on offline devices" on page [1200](#)). In this scheme, you need to copy required updates from the Administration Server repository to a removable drive, then copy the updates to the local folder or the shared resource specified as an update source in the settings of Kaspersky Endpoint Security for Windows (see figure below).



Directly from Kaspersky update servers to Kaspersky Endpoint Security for Windows on the managed devices

On the managed devices, you can configure Kaspersky Endpoint Security for Windows to receive updates directly from Kaspersky update servers (see figure below).



In this scheme, the security application does not use the repositories provided by Kaspersky Security Center. To receive updates directly from Kaspersky update servers, specify Kaspersky update servers as an update source in the interface of the security application. For a full description of these settings, please refer to the Kaspersky Endpoint Security for Windows documentation.

See also:

Scenario: Regular updating Kaspersky databases and applications[1174](#)

Using diff files for updating Kaspersky databases and software modules

When Kaspersky Security Center downloads updates from Kaspersky update servers, it optimizes traffic by using diff files. You can also enable the usage of diff files by devices (Administration Servers, distribution points, and client devices) that take updates from other devices on your network.

About the Downloading diff files feature

A diff file describes the differences between two versions of a file of a database or software module. The usage of diff files saves traffic inside your company's network because diff files occupy less space than entire files of databases and software modules. If the *Downloading diff files* feature is enabled on Administration Server or a distribution point, the diff files are saved on this Administration Server or distribution point. As a result, devices that take updates from this Administration Server or distribution point can use the saved diff files to update their databases and software modules.

To optimize the usage of diff files, we recommend that you synchronize the update schedule of devices with the update schedule of the Administration Server or distribution point from which the devices take updates. However, the traffic can be saved even if devices are updated several times less often than are the Administration Server or distribution point from which the devices take updates.

The Downloading diff files feature can be enabled only on Administration Servers and distribution points of versions starting from version 11. To save diff files on Administration Servers and distribution points of earlier versions, upgrade them to version 11 or higher.

The Downloading diff files feature is incompatible with the offline model of update download (on page [442](#)).

This means that Network Agents that use the offline model of update download do not download diff files even if the Downloading diff files feature is enabled on the Administration Server or distribution point that delivers updates to these Network Agents.

Distribution points do not use IP multicasting for automatic distribution of diff files.

Scenario of enabling the Downloading diff files feature

Prerequisites for the scenario are as follows:

- Administration Servers and distribution points are upgraded to version 11 or higher.
- Offline model of update download is disabled in the settings of the Network Agent policy.

The scenario of enabling the downloading diff files feature consists of the following steps:

a. Enable the feature on Administration Server.

The feature is enabled in the settings of a Download updates to the repository of the Administration Server task (see section "Download updates to the repository of the Administration Server task settings" on page [934](#)).

- b. **Enable the feature for a distribution point that receives updates by means of a Download updates to the repositories of distribution points task.**

The feature is enabled in the settings of this task (see section "Download updates to the repositories of distribution points task settings" on page [936](#)).

- c. **Enable the feature for a distribution point that receives updates from Administration Server.**

The feature is enabled in the Network Agent policy settings (on page [665](#)) and—if the distribution points are assigned manually and if you want to override policy settings—in the **Distribution points** section of the Administration Server properties (see section "Downloading updates by distribution points" on page [430](#)).

To check that the Downloading diff files feature is successfully enabled, you can measure the internal traffic before and after you perform the scenario.

See also:

Scenario: Regular updating Kaspersky databases and applications[1174](#)

Creating the task for downloading updates to the repository of the Administration Server

The Download updates to the repository of the Administration Server task of the Administration Server is created automatically by the Kaspersky Security Center Quick Start Wizard. You can create only one Download updates to the repository of the Administration Server task. Therefore, you can create a Download updates to the repository of the Administration Server task only if this task was removed from the Administration Server tasks list.

► *To create a Download updates to the repository of the Administration Server task:*

1. In the console tree, select the **Tasks** folder.
2. Start creation of the task in one of the following ways:
 - In the context menu of the **Tasks** folder in the console tree, select **New** → **Task**.
 - In the workspace of the **Tasks** folder, click the **Create a task** button.The New Task Wizard starts. Proceed through the Wizard by using the **Next** button.
3. On the **Select the task type** page of the Wizard, select **Download updates to the Administration Server repository**.
4. On the **Settings** page of the Wizard, specify the task settings as follows:
 - **Sources of updates**

The following resources can be used as a source of updates for the Administration Server:

- Kaspersky update servers.
HTTP(S) servers at Kaspersky from which Kaspersky applications download database and application module updates. By default, the Administration Server communicates with Kaspersky update servers and downloads updates by using the HTTPS protocol. You can configure the Administration Server to use the HTTP protocol instead of HTTPS.
Selected by default.
- Primary Administration Server. (This option might not work in Kaspersky Security Center 13 Web Console.)

This resource applies to tasks created for a secondary or virtual Administration Server.

- Local or network folder.

A local or network folder that contains the latest updates. A network folder can be an FTP or HTTP server, or an SMB share. When selecting a local folder, you must specify a folder on the device that has Administration Server installed.

An FTP or HTTP server or a network folder used by an update source must contain a folders structure (with updates) that matches the structure created when using Kaspersky update servers.

- **Other settings:**

- **Force update of secondary Administration Servers**

If this option is enabled, the Administration Server starts the update tasks on the secondary Administration Servers as soon as new updates are downloaded. Otherwise, the update tasks on the secondary Administration Servers start according to their schedules.

By default, this option is disabled.

- **Copy downloaded updates to additional folders**

After the Administration Server receives updates, it copies them to the specified folders. Use this option if you want to manually manage the distribution of updates on your network.

For example, you may want to use this option in the following situation: the network of your organization consists of several independent subnets, and devices from each of the subnets do not have access to other subnets. However devices in all of the subnets have access to a common network share. In this case, you set Administration Server in one of the subnets to download updates from Kaspersky update servers, enable this option, and then specify this network share. In downloaded updates to the repository tasks for other Administration Servers, specify the same network share as the update source.

By default, this option is disabled.

- **Do not force updating of devices and secondary Administration Servers unless copying is complete**

The tasks of downloading updates to client devices and secondary Administration Servers start only after those updates are copied from the main update folder to additional update folders.

This option must be enabled if client devices and secondary Administration Servers download updates from additional network folders.

By default, this option is disabled.

- **Update Network Agent modules (for Network Agent versions earlier than 10 Service Pack 2)**

If this option is enabled, updates for software modules of Network Agent are installed automatically after the Administration Server completes the download updates to the repository task. Otherwise, updates received for Network Agent modules can be installed manually.

By default, this option is enabled.

1. On the **Configure task schedule** page of the Wizard, you can create a schedule for task start. If necessary, specify the following settings:

- **Scheduled start:**

Select the schedule according to which the task runs, and configure the selected schedule.

- **Every N hours**

The task runs regularly, with the specified interval in hours, starting from the specified date and time.

By default, the task runs every six hours, starting from the current system date and time.

- **Every N days**

The task runs regularly, with the specified interval in days. Additionally, you can specify a date and time of the first task run. These additional options become available, if they are supported by the application for which you create the task.

By default, the task runs every day, starting from the current system date and time.

- **Every N weeks**

The task runs regularly, with the specified interval in weeks, on the specified day of week and at the specified time.

By default, the task runs every Monday at the current system time.

- **Every N minutes**

The task runs regularly, with the specified interval in minutes, starting from the specified time on the day that the task is created.

By default, the task runs every 30 minutes, starting from the current system time.

- **Daily (daylight saving time is not supported)**

The task runs regularly, with the specified interval in days. This schedule does not support observance of daylight saving time (DST). It means that when clocks jump one hour forward or backward at the beginning or ending of DST, the actual task start time does not change.

We do not recommend that you use this schedule. It is needed for backward compatibility of Kaspersky Security Center.

By default, the task starts every day at the current system time.

- **Weekly**

The task runs every week on the specified day and at the specified time.

- **By days of week**

The task runs regularly, on the specified days of week, at the specified time.

By default, the task runs every Friday at 6:00:00 P.M.

- **Monthly**

The task runs regularly, on the specified day of the month, at the specified time.

In months that lack the specified day, the task runs on the last day.

By default, the task runs on the first day of each month, at the current system time.

- **Manually (selected by default)**

The task does not run automatically. You can only start it manually.

- **Every month on specified days of selected weeks**

The task runs regularly, on the specified days of each month, at the specified time.

By default, no days of month are selected; the default start time is 6:00:00 P.M.

- **On virus outbreak**

The task runs after a *Virus outbreak* event occurs. Select application types that will monitor virus outbreaks. The following application types are available:

- Anti-virus for workstations and file servers
- Anti-virus for perimeter defense
- Anti-virus for mail systems

By default, all application types are selected.

You may want to run different tasks depending on the anti-virus application type that reports a virus outbreak. In this case, remove the selection of the application types that you do not need.

- **On completing another task**

The current task starts after another task completes. You can select how the previous task must complete (successfully or with error) to trigger the start of the current task. For example, you may want to run the Manage devices task with the **Turn on the device** option and, after it completes, run the Virus scan task.

- **Run missed tasks**

This option determines the behavior of a task if a client device is not visible on the network when the task is about to start.

If this option is enabled, the system attempts to start the task the next time the Kaspersky application is run on the client device. If the task schedule is **Manually**, **Once** or **Immediately**, the task is started immediately after the device becomes visible on the network or immediately after the device is included in the task scope.

If this option is disabled, only scheduled tasks run on client devices; for **Manually**, **Once** and **Immediately**, tasks run only on those client devices that are visible on the network. For example, you may want to disable this option for a resource-consuming task that you want to run only outside of business hours.

By default, this option is enabled.

- **Use automatically randomized delay for task starts**

If this option is enabled, the task is started on client devices randomly within a specified time interval, that is, *distributed task start*. A distributed task start helps to avoid a large number of simultaneous requests by client devices to the Administration Server when a scheduled task is running.

The distributed start time is calculated automatically when a task is created, depending on the number of client devices to which the task is assigned. Later, the task is always started on the calculated start time. However when task settings are edited or the task is started manually, the calculated value of the task start time changes.

If this option is disabled, the task starts on client devices according to the schedule.

- **Use randomized delay for task starts within an interval of (min)**

If this option is enabled, the task is started on client devices randomly within the specified time interval. A distributed task start helps to avoid a large number of simultaneous

requests by client devices to the Administration Server when a scheduled task is running.

If this option is disabled, the task starts on client devices according to the schedule.

By default, this option is disabled. The default time interval is one minute.

1. On the **Define the task name** page of the Wizard, specify the name for the task that you are creating. A task name cannot be more than 100 characters long and cannot include any special characters ("* <>? \:|).
2. On the **Finish task creation** page of the Wizard, click the **Finish** button to close the Wizard.

If you want the task to start as soon as the Wizard finishes, select the **Run the task after the Wizard finishes** check box.

After the Wizard finishes, **Download updates to the Administration Server repository** appears in the list of Administration Server tasks in the workspace.

In addition to the settings that you specify during task creation, you can change other properties of a created task.

When Administration Server performs the Download updates to the repository of the Administration Server task, updates to databases and software modules are downloaded from the updates source and stored in the shared folder of Administration Server. If you create this task for an administration group, it will only be applied to Network Agents included in the specified administration group.

Updates are distributed to client devices and secondary Administration Servers from the shared folder of Administration Server.

See also:

Scenario: Regular updating Kaspersky databases and applications	1174
Verifying downloaded updates	422
Download updates to the repository of the Administration Server task settings	934

Creating the Downloading updates to the repositories of distribution points task

The *Download updates to the repositories of distribution points* task works only on distribution point devices running Windows. Distribution point devices running Linux or macOS cannot download updates from Kaspersky update servers.

If one or more devices running Linux or macOS are within the scope of the *Download updates to the repositories of distribution points* task, the task completes with the *Failed* status, even if it has successfully completed on all Windows devices.

You can create the *Download updates to the repositories of distribution points* task for an administration group. This task will run for distribution points included in the specified administration group.

You can use this task, for example, if the traffic between the Administration Server and the distribution point(s) is more expensive than the traffic between the distribution point(s) and Kaspersky update servers, or if your Administration Server does not have internet access.

► *To create the **Downloading updates to the repositories of distribution points** task for a selected administration group:*

1. In the console tree, select the **Tasks** folder.
2. In the workspace of this folder, click the **Create a task** button.
The New Task Wizard starts. Proceed through the Wizard by using the **Next** button.
3. On the **Select the task type** page of the Wizard, select the **Kaspersky Security Center 13 Administration Server** node, expand the **Advanced** folder, and then select the **Download updates to the repositories of distribution points** task.
4. On the **Settings** page of the Wizard, specify the task settings as follows:
 - **Sources of updates**

The following resources can be used as a source of updates for the Administration Server:

- Kaspersky update servers.
HTTP(S) servers at Kaspersky from which Kaspersky applications download database and application module updates. By default, the Administration Server communicates with Kaspersky update servers and downloads updates by using the HTTPS protocol. You can configure the Administration Server to use the HTTP protocol instead of HTTPS.
Selected by default.
- Primary Administration Server. (This option might not work in Kaspersky Security Center 13 Web Console.)
This resource applies to tasks created for a secondary or virtual Administration Server.
- Local or network folder.
A local or network folder that contains the latest updates. A network folder can be an FTP or HTTP server, or an SMB share. When selecting a local folder, you must specify a folder on the device that has Administration Server installed.

An FTP or HTTP server or a network folder used by an update source must contain a folders structure (with updates) that matches the structure created when using Kaspersky update servers.

- **Other settings:**
 - **Folder for storing updates**

The folder is used to download updates. Specify a local folder on the devices that are assigned to act as distribution point. You can use system variables.

1. On the **Select Administration group** page of the Wizard, click **Browse** and select the administration group to which the task applies.
2. On the **Configure task schedule** page of the Wizard, you can create a schedule for task start. If necessary, specify the following settings:
 - **Scheduled start:**

Select the schedule according to which the task runs, and configure the selected schedule.

- **Every N hours**

The task runs regularly, with the specified interval in hours, starting from the specified date and time.

By default, the task runs every six hours, starting from the current system date and time.

- **Every N days**

The task runs regularly, with the specified interval in days. Additionally, you can specify a date and time of the first task run. These additional options become available, if they are supported by the application for which you create the task.

By default, the task runs every day, starting from the current system date and time.

- **Every N weeks**

The task runs regularly, with the specified interval in weeks, on the specified day of week and at the specified time.

By default, the task runs every Monday at the current system time.

- **Every N minutes**

The task runs regularly, with the specified interval in minutes, starting from the specified time on the day that the task is created.

By default, the task runs every 30 minutes, starting from the current system time.

- **Daily (daylight saving time is not supported)**

The task runs regularly, with the specified interval in days. This schedule does not support observance of daylight saving time (DST). It means that when clocks jump one hour forward or backward at the beginning or ending of DST, the actual task start time does not change.

We do not recommend that you use this schedule. It is needed for backward compatibility of Kaspersky Security Center.

By default, the task starts every day at the current system time.

- **Weekly**

The task runs every week on the specified day and at the specified time.

- **By days of week**

The task runs regularly, on the specified days of week, at the specified time.

By default, the task runs every Friday at 6:00:00 P.M.

- **Monthly**

The task runs regularly, on the specified day of the month, at the specified time.

In months that lack the specified day, the task runs on the last day.

By default, the task runs on the first day of each month, at the current system time.

- **Manually (selected by default)**

The task does not run automatically. You can only start it manually.

- **Every month on specified days of selected weeks**

The task runs regularly, on the specified days of each month, at the specified time.

By default, no days of month are selected; the default start time is 6:00:00 P.M.

- **On virus outbreak**

The task runs after a *Virus outbreak* event occurs. Select application types that will monitor virus outbreaks. The following application types are available:

- Anti-virus for workstations and file servers
- Anti-virus for perimeter defense
- Anti-virus for mail systems

By default, all application types are selected.

You may want to run different tasks depending on the anti-virus application type that reports a virus outbreak. In this case, remove the selection of the application types that you do not need.

- **On completing another task**

The current task starts after another task completes. You can select how the previous task must complete (successfully or with error) to trigger the start of the current task. For example, you may want to run the Manage devices task with the **Turn on the device** option and, after it completes, run the Virus scan task.

- **Run missed tasks**

This option determines the behavior of a task if a client device is not visible on the network when the task is about to start.

If this option is enabled, the system attempts to start the task the next time the Kaspersky application is run on the client device. If the task schedule is **Manually**, **Once** or **Immediately**, the task is started immediately after the device becomes visible on the network or immediately after the device is included in the task scope.

If this option is disabled, only scheduled tasks run on client devices; for **Manually**, **Once** and **Immediately**, tasks run only on those client devices that are visible on the network. For example, you may want to disable this option for a resource-consuming task that you want to run only outside of business hours.

By default, this option is enabled.

- **Use automatically randomized delay for task starts**

If this option is enabled, the task is started on client devices randomly within a specified time interval, that is, *distributed task start*. A distributed task start helps to avoid a large number of simultaneous requests by client devices to the Administration Server when a scheduled task is running.

The distributed start time is calculated automatically when a task is created, depending on the number of client devices to which the task is assigned. Later, the task is always started on the calculated start time. However when task settings are edited or the task is started manually, the calculated value of the task start time changes.

If this option is disabled, the task starts on client devices according to the schedule.

- **Use randomized delay for task starts within an interval of (min)**

If this option is enabled, the task is started on client devices randomly within the specified time interval. A distributed task start helps to avoid a large number of simultaneous requests by client devices to the Administration Server when a scheduled task is running.

If this option is disabled, the task starts on client devices according to the schedule.

By default, this option is disabled. The default time interval is one minute.

1. On the **Define the task name** page of the Wizard, specify the name for the task that you are creating. A task name cannot be more than 100 characters long and cannot include any special characters ("* <>? \:|).
2. On the **Finish task creation** page of the Wizard, click the **Finish** button to close the Wizard.

If you want the task to start as soon as the Wizard finishes, select the **Run the task after the Wizard finishes** check box.

When the Wizard completes its operation, **Download updates to the repositories of distribution points** appears in the list of Network Agent tasks in the target administration group and in the **Tasks** workspace of the console.

In addition to the settings that you specify during task creation, you can change other properties of a created task.

When the *Download updates to the repositories of distribution points* task is performed, updates for databases and software modules are downloaded from the update source and stored in the shared folder. Downloaded updates will only be used by distribution points that are included in the specified administration group and that have no update download task explicitly set for them.

In the Administration Server properties window, in the **Sections** pane select **Distribution points**. In the properties of each distribution point, in the **Update source** section you can specify the update source (**Retrieve from Administration Server** or **Use task for forced download of updates**). By default, **Retrieve from Administration Server** is selected for a distribution point that is assigned manually or automatically. These distribution points will use the results of the *Download updates to the repositories of distribution points* task.

The properties of each distribution point specify the network folder that has been set up for that distribution point individually. The names of folders may vary for different distribution points. For this reason, we do not recommend that you change the network folder in the task properties if the task is created for a group of devices.

You can change the network folder with updates in the properties of the *Download updates to the repositories of distribution points* task if you are creating a local task for a device.

The previous versions of the application (Kaspersky Security Center 10 Service Pack 2 and earlier) allowed you to create the update download task for distribution points as a local task only. Starting from Kaspersky Security Center 10 Service Pack 3, this restriction has been lifted, which has resulted in decreased traffic rates.

See also:

Download updates to the repositories of distribution points task settings.....[936](#)

Configuring the Download updates to the repository of the Administration Server task

► *To configure the Download updates to the repository of the Administration Server task:*

1. In the workspace of the **Tasks** console tree folder, select **Download updates to the Administration Server repository** in the task list.
2. Open the task properties window in one of the following ways:

- By selecting **Properties** in the context menu of the task.
- By clicking the **Configure task** link in the information box for the selected task.

The Download updates to the repository of the Administration Server task properties window opens. In this window, you can configure how the updates are downloaded to the Administration Server repository.

See also:

Download updates to the repository of the Administration Server task settings..... [934](#)

Verifying downloaded updates

- *To make Kaspersky Security Center verify downloaded updates before distributing them to client devices:*
1. In the workspace of **Tasks** folder, select the **Download updates to the Administration Server repository** task in the list of tasks.
 2. Open the task properties window in one of the following ways:
 - By selecting **Properties** in the context menu of the task.
 - By clicking the **Configure task** link in the information box for the selected task.
 3. In the task properties window that opens, in the **Update verification** section, select the **Verify updates before distributing** check box and then select the update verification task in one of the following ways:
 - By clicking the **Browse** button to choose an existing update verification task.
 - By clicking the **Create** button to create an update verification task.

The Update Verification Task Wizard starts. Follow the instructions of the Wizard.

When creating the update verification task, select the administration group that contains devices on which the task will be run. Devices included in this group are called *test devices*.

It is recommended to use devices with the most reliable protection and the most popular application configuration across the network. This approach increases the quality of scans, and minimizes the risk of false positives and the probability of virus detection during scans. If viruses are detected on test devices, the update verification task is considered unsuccessful.

4. Click **OK** to close the properties window of the Download updates to the repository of the Administration Server task.

The update verification task is performed as part of the Download updates to the repository of the Administration Server task. The Administration Server will download updates from the source, save them in the temporary repository, and run the update verification task. If the task completes successfully, the updates will be copied from the temporary repository to the Administration Server shared folder (<Kaspersky Security Center installation folder>\Share\Updates). They will be distributed to all client devices for which the Administration Server is the source of updates.

If, as a result of the update verification task, updates located in the temporary repository are incorrect or if the update verification task completes with an error, such updates will not be copied to the shared folder. The Administration Server will retain the previous set of updates. Also, the tasks that have the **When new updates are**

downloaded to the repository schedule type are not started then. These operations will be performed at the next start of the Download updates to the repository of the Administration Server task if scanning of the new updates completes successfully.

A set of updates is considered invalid if any of the following conditions is met on at least one test device:

- An update task error occurred.
- The real-time protection status of the security application changed after the updates were applied.
- An infected object was detected during running of the on-demand scan task.
- A runtime error of a Kaspersky application occurred.

If none of the listed conditions is true for any test device, the set of updates is considered valid, and the update verification task is considered to have completed successfully.

See also:

Scenario: Regular updating Kaspersky databases and applications[1174](#)

Configuring test policies and auxiliary tasks

When creating an update verification task, the Administration Server generates test policies, auxiliary group update tasks, and on-demand scan tasks.

Auxiliary group update and on-demand scan tasks take some time. These tasks are performed when the update verification task is executed. The update verification task is performed during execution of the Download updates to the repository task. The duration of the Download updates to the repository task includes auxiliary group update and on-demand scan tasks.

You can change the settings of test policies and auxiliary tasks.

► *To change settings of a test policy or an auxiliary task:*

1. In the console tree, select a group for which the update verification task is created.
2. In the group workspace, select one of the following tabs:
 - **Policies**, if you want to edit the test policy settings.
 - **Tasks**, if you want to change auxiliary task settings.
3. In the tab workspace, select a policy or a task, whose settings you want to change.
4. Open the policy (task) properties window in one of the following ways:
 - By selecting **Properties** in the context menu of the policy (task).
 - By clicking the **Configure policy (Configure task)** link in the information box for the selected policy (task).

To verify updates correctly, set the following restrictions on the modification of test policies and auxiliary tasks:

- In the auxiliary task settings:

- Save all tasks with the **Critical event** and **Functional failure** importance levels on Administration Server. Using the events of these types, the Administration Server analyzes the operation of applications.
- Use Administration Server as the source of updates.
- Specify the task schedule type: **Manually**.
- In the settings of test policies:
 - Disable the iChecker, iSwift, and iStream scanning acceleration technologies.
 - Select actions on infected objects: **Disinfect; delete if disinfection fails / Disinfect; block if disinfection fails / Block**.
- In the settings of test policies and auxiliary tasks:

If the device requires a restart after installation of updates for software modules, it must be performed immediately. If the device is not restarted, it is not possible to test this type of updates. For some applications, installation of updates that require a restart may be prohibited or configured to prompt the user for confirmation first. These restrictions should be disabled in the settings of test policies and auxiliary tasks.

Viewing downloaded updates

► *To view the list of downloaded updates,*

In the console tree, in the **Repositories** folder, select the **Updates for Kaspersky databases and software modulesupdates and patches** subfolder.

The workspace of the **Updates for Kaspersky databases and software modules** folder shows the list of updates that have been saved on the Administration Server.

Automatic distribution of updates

Kaspersky Security Center allows automatic distribution and installation of updates on client devices and secondary Administration Servers.

In this section

Distributing updates to client devices automatically	425
Distributing updates to secondary Administration Servers automatically	425
Installing updates for software modules of Network Agents automatically	426
Assigning distribution points automatically	426
Assigning a device a distribution point manually	427
Removing a device from the list of distribution points	430
Downloading updates by distribution points	430

Distributing updates to client devices automatically

► *To distribute updates of the selected application to client devices automatically immediately after they are downloaded to the Administration Server repository:*

1. Connect to the Administration Server, which manages the client devices.
2. Create an update deployment task for the selected client devices in one of the following ways:
 - If you need to distribute updates to client devices that belong to a selected administration group, create a task for the selected group (see section "Creating a task" on page [374](#)).
 - If you need to distribute updates to client devices that belong to different administration groups or belong to none of the administration groups, create a task for specific devices (see section "Creating a task for specific devices" on page [376](#)).

The New Task Wizard starts. Follow its instructions and perform the following actions:

- a. In the **Task type** Wizard window, in the node of the required application select the updates deployment task.

The name of the updates deployment task displayed in the **Task type** window depends on the application for which you create this task. For detailed information about names of update tasks for the selected Kaspersky applications, see the corresponding Guides.

- b. In the **Schedule** Wizard window, in the **Scheduled start** field, select **When new updates are downloaded to the repository**.

The newly created update distribution task will start for the selected devices every time any updates are downloaded to the Administration Server repository.

If an update distribution task for the required application has already been created for the selected devices, to automatically distribute updates to client devices, in the task properties window, in the **Schedule** section, select **When new updates are downloaded to the repository** as the start option in the **Scheduled start** field.

Distributing updates to secondary Administration Servers automatically

► *To distribute the updates of the selected application to secondary Administration Servers immediately after the updates are downloaded to the primary Administration Server repository:*

1. In the console tree, in the primary Administration Server node, select the **Tasks** folder.
2. In the list of tasks in the workspace, select the Download updates to the repository of the Administration Server task of the Administration Server.
3. Open the **Settings** section of the selected task in one of the following ways:
 - By selecting **Properties** in the context menu of the task.
 - By clicking the **Edit settings** link in the information box for the selected task.
4. In the **Settings** section of the task properties window, select the **Other settings** subsection, and then click the **Configure** link.
5. In the **Other settings** window that opens, select the **Force update of secondary Administration Servers** check box.

In the settings of the updates download task of the Administration Server, on the **Settings** tab of the task properties window, select the **Force update of secondary Administration Servers** check box.

After the primary Administration Server retrieves updates, the update download tasks automatically start on secondary Administration Servers regardless of their schedule.

Installing updates for software modules of Network Agents automatically

► *To install updates for software modules of Network Agents automatically after they are uploaded to the Administration Server repository:*

1. In the console tree, in the primary Administration Server node, select the **Tasks** folder.
2. In the list of tasks in the workspace, select the Download updates to the repository of the Administration Server task of the Administration Server.
3. Open the properties window of the selected task in one of the following ways:
 - By selecting **Properties** in the context menu of the task.
 - By clicking the **Configure task** link in the information box for the selected task.
4. In the task properties window, select the **Settings** section.
5. Click the **Configure** link in the **Other settings** section to open the **Other settings** window.
6. In the **Other settings** window that opens, select the **Update Network Agent modules** check box.

If this check box is selected, updates for software modules of Network Agent will be automatically installed after they are uploaded to the Administration Server repository. If this check box is cleared, Network Agent updates will not be installed automatically. Retrieved updates can be installed manually. By default, this check box is selected.

Network Agent software modules can only be installed automatically for Network Agent 10 Service Pack 1 or later.

7. Click **OK**.

Updates for Network Agent software modules will be installed automatically.

Assigning distribution points automatically

We recommend that you opt to assign distribution points automatically. Kaspersky Security Center will then select on its own which devices must be assigned distribution points.

► *To assign distribution points automatically:*

1. Open the main application window.
2. In the console tree, select the node with the name of the Administration Server for which you want to assign distribution points automatically.
3. In the context menu of the Administration Server, click **Properties**.
4. In the Administration Server properties window, in the **Sections** pane select **Distribution points**.
5. In the right part of the window, select the **Automatically assign distribution points** option.

If automatic assignment of devices as distribution points is enabled, you cannot configure distribution points manually or edit the list of distribution points.

6. Click **OK**.

Administration Server assigns and configures distribution points automatically.

Assigning a device a distribution point manually

Kaspersky Security Center allows you to assign devices to act as distribution points.

We recommend that you assign distribution points automatically. In this case, Kaspersky Security Center will select on its own which devices must be assigned distribution points. However, if you have to opt out of assigning distribution points automatically for any reason (for example, if you want to use exclusively assigned servers), you can assign distribution points manually after you calculate their number and configuration (see section "Calculating the number and configuration of distribution points" on page [134](#)).

Devices functioning as distribution points must be protected, including physical protection, against any unauthorized access.

► *To manually assign a device to act as distribution point:*

1. In the console tree, select the **Administration Server** node.
2. In the context menu of the Administration Server, select **Properties**.
3. In the Administration Server properties window, select the **Distribution points** section and click the **Add** button. This button is available if **Manually assign distribution points** has been selected.

The **Add distribution point** window opens.

4. In the **Add distribution point** window, perform the following actions:
 - a. Select a device that will act as distribution point (select one in an administration group, or specify the IP address of a device). When selecting a device, keep in mind the operation features of distribution points and the requirements set for the device that acts as distribution point (on page [55](#)).
 - b. Indicate the specific devices to which the distribution point will distribute updates. You can specify an administration group or a network location description.
5. Click **OK**.

The distribution point that you have added will be displayed in the list of distribution points, in the **Distribution points** section.

6. Select the newly added distribution point in the list and click the **Properties** button to open its properties window.
7. Configure the distribution point in the properties window:
 - The **General** section contains the settings of interaction between the distribution point and client devices.
 - **SSL port**

The number of the SSL port for encrypted connection between client devices and the distribution point using SSL.

By default, port 13000 is used.

- **Use multicast**

If this check box is selected, IP multicasting will be used for automatic distribution of installation packages to client devices within the group.

IP multicasting decreases the time required to install an application from an installation package to a group of client devices, but increases the installation time when you install an application to a single client device.

- **IP multicast address**

IP address that will be used for multicasting. You can define an IP address in the range of 224.0.0.0 – 239.255.255.255

By default, Kaspersky Security Center automatically assigns a unique IP multicast address within the given range.

- **IP multicast port number**

Number of the port for IP multicasting.

By default, the port number is 15001. If the device with Administration Server installed is specified as the distribution point, port 13001 is used for SSL connection by default.

- **Deploy updates**

If this check box is selected, updates are distributed to client devices through this distribution point.

By default, this check box is selected.

- **Deploy installation packages**

If this check box is selected, installation packages with this update are distributed to client devices through this distribution point.

By default, this check box is selected.

- In the **Scope** section, specify the scope to which the distribution point will distribute updates (administration groups and / or network location).

- In the **KSN Proxy** section, you can configure the application to use the distribution point to forward KSN requests from the managed devices.

- **Enable KSN Proxy on distribution point side**

The KSN Proxy service is run on the device that is used as a distribution point. Use this feature to redistribute and optimize traffic on the network.

The distribution point sends the KSN statistics, which are listed in the Kaspersky Security Network statement, to Kaspersky. By default, the KSN statement is located in %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\ksneula.

By default, this option is disabled. Enabling this option takes effect only if the **Use Administration Server as proxy server** and **I agree to use Kaspersky Security Network** options are enabled (see section "Setting up access to Kaspersky Security Network" on page [786](#)) in the Administration Server properties window.

You can assign a node of an active-passive cluster to a distribution point and enable KSN Proxy on this node.

- **Forward KSN requests to Administration Server**

The distribution point forwards KSN requests from the managed devices to the Administration Server.

By default, this option is enabled.

- **Access KSN Cloud / Private KSN directly over Internet**

The distribution point forwards KSN requests from managed devices to the KSN Cloud or Private KSN. The KSN requests generated on the distribution point itself are also sent directly to the KSN Cloud or Private KSN.

The distribution points that have Network Agent version 11 (or earlier) installed cannot access Private KSN directly. If you want to reconfigure the distribution points to send KSN requests to Private KSN, enable the **Forward KSN requests to Administration Server** option for each distribution point.

The distribution points that have Network Agent version 12 (or later) installed can access Private KSN directly.

- **Ignore KSC proxy server settings when connecting to Private KSN**

Enable this option, if you have the proxy server settings configured in the distribution point properties or in the Network Agent policy, but your network architecture requires that you use Private KSN directly. Otherwise, requests from the managed applications cannot reach Private KSN.

- **TCP port**

The number of the TCP port that the managed devices will use to connect to KSN Proxy server. The default port number is 13111.

- **UDP port**

If you need the managed devices to connect to KSN Proxy server through a UDP port, enable the **Use UDP port** option and specify a **UDP port** number. By default, this option is enabled. The default UDP port to connect to the KSN Proxy server is 15111.

- In the **Device discovery** section, configure the polling of Windows domains, Active Directory, and IP ranges by the distribution point.

- **Windows domains**

You can enable device discovery for Windows domains and set the schedule for the discovery.

- **Active Directory**

You can enable network polling for Active Directory and set the schedule for the poll.

If you select the **Enable network polling** check box, you can select one of the following options:

- **Poll current Active Directory domain.**
- **Poll Active Directory domain forest.**
- **Poll selected Active Directory domains only.** If you select this option, add one or more Active Directory domains to the list.

- **IP ranges**

You can enable device discovery for IP ranges.

If you select the **Enable range polling** check box, you can add scan ranges and set the schedule for them.

You can add IP ranges to the list of scanned ranges (see section "Adding IP ranges to the scanned ranges list of a distribution point" on page [594](#)).

- In the **Advanced** section, specify the folder that the distribution point must use to store distributed data.
 - **Use default folder**

If you select this option, the application uses the Network Agent installation folder on the distribution point.

- **Use specified folder**

If you select this option, in the field below, you can specify the path to the folder. It can be a local folder on the distribution point, or it can be a folder on any device on the corporate network.

The user account used on the distribution point to run Network Agent must have read/write access to the specified folder.

The selected devices act as distribution points.

Only devices running a Windows operating system can determine their network location. Network location cannot be determined for devices running other operating systems.

See also:

Scenario: Regular updating Kaspersky databases and applications[1174](#)

Removing a device from the list of distribution points

► *To remove a device from the list of distribution points:*

1. In the console tree, select the **Administration Server** node.
2. In the context menu of the Administration Server, select **Properties**.
3. In the Administration Server properties window, in the **Distribution points** section, select the device that acts as distribution point, and click the **Remove** button.

The device will be removed from the list of distribution points and will stop acting as distribution point.

You cannot remove a device from the list of distribution points if it was assigned by the Administration Server automatically (see section "Assigning a device a distribution point manually" on page [427](#)).

Downloading updates by distribution points

Kaspersky Security Center allows distribution points to receive updates from the Administration Server, Kaspersky servers, or from a local or network folder.

► *To configure update download for a distribution point:*

1. In the console tree, select the **Administration Server** node.
2. In the context menu of the Administration Server, select **Properties**.
3. In the Administration Server properties window, in the **Distribution points** section select the distribution point through which updates will be delivered to client devices in the group.

4. Click the **Properties** button to open the properties window of the selected distribution point.
5. In the distribution point properties window, select the **Sources of updates** section.
6. Select an update source for the distribution point:
 - To allow the distribution point to receive updates from the Administration Server, select **Retrieve from Administration Server**:
 - **Download diff files**

This option enables the downloading diff files feature (see section "Using diff files for updating Kaspersky databases and software modules" on page [412](#)).

By default, this option is enabled.

- To allow the distribution point to receive updates by using a task, select **Use task for forced download of updates**:
 - Click the **Browse** button if such a task already exists on the device, and select the task in the list that appears.
 - Click the **New task** button to create a task if no such task yet exists on the device. The New Task Wizard starts. Follow the instructions of the Wizard.

The Download updates to the repositories of distribution points task is a local task. You have to create a new task for each device that acts as distribution point.

The distribution point will receive updates from the specified source.

Deleting software updates from the repository

► *To delete software updates from the Administration Server repository:*

1. In the **Application management** folder of the console tree, select the **Software updates** subfolder.
2. In the workspace of the **Software updates** folder, select the update that you want to delete.
3. In the context menu of the update, select **Delete update files**.

Software updates will be deleted from the Administration Server repository.

Algorithm of patch installation for a Kaspersky application in cluster mode

Kaspersky Security Center only supports manual installation of patches for Kaspersky applications in cluster mode.

To install a patch for a Kaspersky application:

1. Download the patch to each node of the cluster.
2. Run patch installation on the active node.
Wait for the patch to be successfully installed.
3. Run the patch on all subnodes of the cluster consecutively.

If you are running the patch from the command line, use the `-CLUSTER_SECONDARY_NODE` key.

The patch is now installed on all nodes of the cluster.

4. Run the Kaspersky cluster services manually.

Every node of the cluster is displayed in Administration Console as a device with Network Agent installed.

For information about installed patches, see the **Software updates** folder or the report on the versions of updates for software modules of Kaspersky applications.

See also:

Adjusting the general settings of Administration Server	609
---	---------------------

Managing third-party applications on client devices

Kaspersky Security Center allows you to manage applications by Kaspersky and other vendors installed on client devices.

The administrator can perform the following actions:

- Create application categories based on specified criteria.
- Manage application categories using specially created rules.
- Manage applications run on devices.
- Perform inventories and maintain a registry of software installed on devices.
- Fix vulnerabilities in software installed on devices.
- Install updates from Windows Update and other software makers on devices.
- Monitor the use of license keys for licensed applications groups.

In this section

Installation of third-party software updates	432
Fixing third-party software vulnerabilities	459
Groups of applications	485

Installation of third-party software updates

Kaspersky Security Center allows you to manage updates of software installed on client devices and fix vulnerabilities in Microsoft applications and other software makers' products through installation of required updates.

Kaspersky Security Center searches for updates through the update search task and downloads them to the updates repository. After completing the search of updates, the application provides the administrator with information about available updates and vulnerabilities in applications that can be fixed using those updates.

Information about available updates for Microsoft Windows is provided by Windows Update service. Administration Server can be used as Windows Server Update Services (WSUS) server. To use Administration Server as WSUS server, you should configure synchronization of updates with Windows Update. After you have configured data synchronization with Windows Update, Administration Server provides updates to Windows Update services on devices in centralized mode and with the set frequency.

You can also manage software updates through a Network Agent policy. To do this, you should create a Network Agent policy and configure software updating in the corresponding windows of the New Policy Wizard.

The administrator can view a list of available updates in the **Software updates** subfolder included in the **Application management** folder. This folder contains a list of updates for Microsoft applications and other software makers' products retrieved by Administration Server that can be distributed to devices. After viewing information about available updates, the administrator can install them to devices.

Kaspersky Security Center updates some applications by removing the previous version of the application and installing the new one.

A user interaction may be required when you update a third-party application or fix a vulnerability in a third-party application on a managed device. For example, the user may be prompted to close the third-party application if it's currently open.

Before installing the updates to all of the devices, you can perform a test installation to make sure installed updates will cause no failures to the operation of applications on the devices.

You can find the details of third-party software that can be updated through Kaspersky Security Center, by visiting the Technical Support website, on the Kaspersky Security Center page, in the Server Management (<https://support.kaspersky.com/14758>) section.

In this section

Viewing information about available updates	434
Approving and declining software updates	435
Synchronizing updates from Windows Update with Administration Server	436
Automatic installation of Kaspersky Endpoint Security updates on devices	441
Offline model of update download	442
Enabling and disabling the offline model of update download	443
Installing updates on devices manually	444
Configuring Windows updates in a Network Agent policy	455
Automatic updating and patching for Kaspersky Security Center components	457
Enabling and disabling automatic updating and patching for Kaspersky Security Center components	458

Viewing information about available updates

- ▶ *To view a list of available updates for applications installed on client devices,*

In the **Advanced** → **Application management** folder in the console tree, select the **Software updates** subfolder.

In the workspace of the folder, you can view a list of available updates for applications installed on devices.

- ▶ *To view the properties of an update,*

In the workspace of the **Software updates** folder, in the context menu of the update select **Properties**.

The following information is available for viewing in the properties window of the update:

- Basic information (such as the severity level or language).

The value of the **Installed automatically** field (in the **Attributes** section of the properties window for the selected update) is displayed only after the appropriate application has been run at least once.

The **Automatically** value of the **Installed automatically** field corresponds to the case when Kaspersky Security Center automatically downloads updates from the web address provided by the vendor of third-party software. After that, Kaspersky Security Center installs the updates using the Install required updates and fix vulnerabilities task.

The **Manually** value of the **Installed automatically** field corresponds to the case when Kaspersky Security Center cannot automatically download updates. You can set up this value, for example, for the previous version of update. In this case, you must download and install updates on your own.

- List of client devices for which the update is intended.
- List of system components (prerequisites), which have to be installed before the update (if any).
- Software vulnerabilities that the update will fix.

See also:

| Scenario: Updating third-party software[1208](#)

Approving and declining software updates

The settings of an update installation task may require approval of updates that are to be installed. You can approve updates that must be installed and decline updates that must not be installed.

For example, you may want to first check the installation of updates in a test environment and make sure that they do not interfere with the operation of devices, and only then allow the installation of these updates on client devices.

The usage of the *Approved* status to manage third-party update installation is efficient for a small amount of updates. To install multiple third-party updates, use the rules that you can configure in the *Install required updates and fix vulnerabilities* task. We recommend that you set the *Approved* status for only those specific updates that do not meet the criteria specified in the rules. When you manually approve a large amount of updates, performance of Administration Server decreases and may lead to Administration Server overload.

► *To approve or decline one or several updates:*

1. In the console tree, select the **Advanced** → **Application management** → **Software updates** node.
2. In the workspace of the **Software updates** folder, click the **Refresh** button in the upper right corner. A list of updates appears.
3. Select the updates that you want to approve or decline.
The information box for the selected objects appears on the right side of the workspace.
4. In the **Update approval status** drop-down list, select **Approved** to approve the selected updates or **Declined** to decline the selected updates.

The default value is **Undefined**.

The updates for which you set the **Approved** status are placed in a queue for installation.

The updates for which you set **Declined** status are uninstalled (if possible) from all devices on which they were previously installed. Also, they will not be installed on other devices in future.

Some updates for Kaspersky applications cannot be uninstalled. If you set **Declined** status for them, Kaspersky Security Center will not uninstall these updates from the devices on which they were previously installed. However, these updates will never be installed on other devices in future.

If an update for Kaspersky applications cannot be uninstalled, this property is displayed in the update properties window: in the **Sections** pane select **General**, and in the workspace the property will appear under **Installation requirements**.

If you set **Declined** status for third-party software updates, these updates will not be installed on devices for which they were planned for installation but have not yet been installed. Updates will still remain on devices on which they were already installed. If you have to delete them, you can manually delete them locally.

See also:

Scenario: Regular updating Kaspersky databases and applications	1174
Scenario: Updating third-party software	1208

Synchronizing updates from Windows Update with Administration Server

If you have selected **Use Administration Server as a WSUS server** in the **Update management settings** window of the Quick Start Wizard, the Windows Update synchronization task is created automatically. You can run the task in the **Tasks** folder. The functionality of a Microsoft software update is only available after the **Perform Windows Update synchronization** task is successfully completed.

The **Perform Windows Update synchronization** task only downloads metadata from Microsoft servers. If the network does not use a WSUS server, each client device downloads Microsoft updates from external servers independently.

► *To create a task for synchronizing Windows Updates with Administration Server:*

1. In the **Advanced** → **Application management** folder in the console tree, select the **Software updates** subfolder.
2. Click the **Additional actions** button and select **Configure Windows Update synchronization** in the drop-down list.

The Wizard creates the **Perform Windows Update synchronization** task displayed in the **Tasks** folder.

The Windows Update Center Data Retrieval Task Creation Wizard starts. Follow the instructions of the Wizard.

You can also create the Windows Update synchronization task in the **Tasks** folder by clicking **Create a task**.

Microsoft regularly deletes outdated updates from the company's servers so the number of current updates is always between 200 000 and 300 000. In Kaspersky Security Center 10 Service Pack 2 Maintenance Release 1 and earlier versions, all updates were retained: no outdated updates were deleted. As a result, the database continuously grew in size. To reduce disk space usage and database size, deletion of outdated updates that are no longer present on Microsoft update servers has been implemented in Kaspersky Security Center 10 Service Pack 3.

When running the **Perform Windows Update synchronization** task, the application receives a list of current updates from a Microsoft update server. Next, Kaspersky Security Center compiles a list of updates that have become outdated. At the next start of the **Find vulnerabilities and required updates** task, Kaspersky Security Center flags all outdated updates and sets the deletion time for them. At the next start of the **Perform Windows Update synchronization** task, all updates flagged for deletion 30 days ago are deleted. Kaspersky Security Center also checks for outdated updates that were flagged for deletion more than 180 days ago, and then deletes those older updates.

When the **Perform Windows Update synchronization** task completes and outdated updates are deleted, the database may still have the hash codes pertaining to the files of deleted updates, as well as corresponding files in the %AllUsersProfile%\Application Data\KasperskyLab\adminkit\1093\working\wusfiles files (if they were downloaded earlier). You can run the **Administration Server maintenance** (see section "**Administration Server maintenance**" on page [892](#)) task to delete these outdated records from the database and corresponding files.

See also:

Scenario: Updating third-party software	1208
Step 1. Settings	437
Step 2. Applications	437
Step 3. Update categories	437
Step 4. Updates languages	438
Step 5. Selecting the account to start the task	438
Step 6. Configuring a task start schedule	438
Step 7. Defining the task name	440
Step 8. Completing creation of the task.....	441

Step 1. Settings

When Kaspersky Security Center synchronizes updates with Microsoft Windows Update Servers, information about all files is saved in the Administration Server database. All files required for an update are also downloaded to the drive during interaction with the Windows Update Agent. In particular, Kaspersky Security Center saves information about express update files to the database and downloads them when necessary. Downloading express update files leads to decreased free space on the drive.

To avoid a decrease in disk space volume and to reduce traffic, clear the **Download express installation files** check box.

If the check box is selected, express update files are downloaded when running the task.

By default, this check box is cleared.

Step 2. Applications

In this section you can select applications for which updates will be downloaded.

If the **All applications** check box is selected, updates will be downloaded for all existing applications, and for all applications that may be released in the future.

By default, the **All applications** check box is selected.

Step 3. Update categories

In this section, you can select categories of updates that will be downloaded to the Administration Server.

If the **All categories** check box is selected, updates will be downloaded for all existing updates categories, and for all categories that may appear in the future.

By default, the **All categories** check box is selected.

Step 4. Updates languages

In this window you can select localization languages of updates that will be downloaded to Administration Server. Select one of the following options for downloading localization languages of updates:

- **Download all languages, including new ones**

If this option is selected, all the available localization languages of updates will be downloaded to Administration Server. By default, this option is selected.
- **Download selected languages**

If this option is selected, you can select from the list localization languages of updates that should be downloaded to Administration Server.

Step 5. Selecting the account to start the task

In the **Selecting an account to run the task** window, you can specify which account to use when running the task. Select one of the following options:

- **Default account**

The task will be run under the same account as the application that performs this task. By default, this option is selected.
- **Specify account**

Fill in the **Account** and **Password** fields to specify the details of an account under which the task is run. The account must have sufficient rights for this task.
- **Account**

Account under which the task is run.
- **Password**

Password of the account under which the task will be run.

Step 6. Configuring a task start schedule

On the **Configure task schedule** wizard page, you can create a schedule for task start. If necessary, specify the following settings:

- **Scheduled start:**

Select the schedule according to which the task runs, and configure the selected schedule.

- **Every N hours**

The task runs regularly, with the specified interval in hours, starting from the specified date and time.

By default, the task runs every six hours, starting from the current system date and time.
- **Every N days**

The task runs regularly, with the specified interval in days. Additionally, you can specify a date and time of the first task run. These additional options become available, if they are supported by the application for which you create the task.

By default, the task runs every day, starting from the current system date and time.
- **Every N weeks**

The task runs regularly, with the specified interval in weeks, on the specified day of week and at the specified time.

By default, the task runs every Monday at the current system time.

- **Every N minutes**

The task runs regularly, with the specified interval in minutes, starting from the specified time on the day that the task is created.

By default, the task runs every 30 minutes, starting from the current system time.

- **Daily (daylight saving time is not supported)**

The task runs regularly, with the specified interval in days. This schedule does not support observance of daylight saving time (DST). It means that when clocks jump one hour forward or backward at the beginning or ending of DST, the actual task start time does not change.

We do not recommend that you use this schedule. It is needed for backward compatibility of Kaspersky Security Center.

By default, the task starts every day at the current system time.

- **Weekly**

The task runs every week on the specified day and at the specified time.

- **By days of week**

The task runs regularly, on the specified days of week, at the specified time.

By default, the task runs every Friday at 6:00:00 P.M.

- **Monthly**

The task runs regularly, on the specified day of the month, at the specified time.

In months that lack the specified day, the task runs on the last day.

By default, the task runs on the first day of each month, at the current system time.

- **Manually**

The task does not run automatically. You can only start it manually.

- **Once**

- **Every month on specified days of selected weeks**

The task runs regularly, on the specified days of each month, at the specified time.

By default, no days of month are selected; the default start time is 6:00:00 P.M.

- **On virus outbreak**

The task runs after a *Virus outbreak* event occurs. Select application types that will monitor virus outbreaks. The following application types are available:

- Anti-virus for workstations and file servers
- Anti-virus for perimeter defense
- Anti-virus for mail systems

By default, all application types are selected.

You may want to run different tasks depending on the anti-virus application type that reports a virus outbreak. In this case, remove the selection of the application types that

you do not need.

- **On completing another task**

The current task starts after another task completes. You can select how the previous task must complete (successfully or with error) to trigger the start of the current task. For example, you may want to run the Manage devices task with the **Turn on the device** option and, after it completes, run the Virus scan task.

- **Run missed tasks**

This option determines the behavior of a task if a client device is not visible on the network when the task is about to start.

If this option is enabled, the system attempts to start the task the next time the Kaspersky application is run on the client device. If the task schedule is **Manually, Once** or **Immediately**, the task is started immediately after the device becomes visible on the network or immediately after the device is included in the task scope.

If this option is disabled, only scheduled tasks run on client devices; for **Manually, Once** and **Immediately**, tasks run only on those client devices that are visible on the network. For example, you may want to disable this option for a resource-consuming task that you want to run only outside of business hours.

By default, this option is enabled.

- **Use automatically randomized delay for task starts**

If this option is enabled, the task is started on client devices randomly within a specified time interval, that is, *distributed task start*. A distributed task start helps to avoid a large number of simultaneous requests by client devices to the Administration Server when a scheduled task is running.

The distributed start time is calculated automatically when a task is created, depending on the number of client devices to which the task is assigned. Later, the task is always started on the calculated start time. However when task settings are edited or the task is started manually, the calculated value of the task start time changes.

If this option is disabled, the task starts on client devices according to the schedule.

- **Use randomized delay for task starts within an interval of (min)**

If this option is enabled, the task is started on client devices randomly within the specified time interval. A distributed task start helps to avoid a large number of simultaneous requests by client devices to the Administration Server when a scheduled task is running.

If this option is disabled, the task starts on client devices according to the schedule.

By default, this option is disabled. The default time interval is one minute.

Step 7. Defining the task name

In the **Define the task name** window, specify the name for the task that you are creating. A task name cannot be more than 100 characters long and cannot include any special characters (" * < > ? \ : |). The default value is *Perform Windows Update synchronization*.

Step 8. Completing creation of the task

In the **Finish task creation** window, click the **Finish** button to finish the Wizard.

If you want the task to start as soon as the Wizard finishes, select the **Run the task after the Wizard finishes** check box.

The newly created Windows Update synchronization task will appear in the list of tasks in the **Tasks** folder of the console tree.

Automatic installation of Kaspersky Endpoint Security updates on devices

You can configure automatic updates of databases and software modules of Kaspersky Endpoint Security on client devices.

► *To configure download and automatic installation of Kaspersky Endpoint Security updates on devices:*

1. In the console tree, select the **Tasks** folder.
2. Create an **Update** task in one of the following ways:
 - By selecting **New** → **Task** in the context menu of the **Tasks** folder in the console tree.
 - By clicking the **New task** button in the workspace of the **Tasks** folder.

The New Task Wizard starts. Proceed through the Wizard by using the **Next** button.

3. On the **Select the task type** page of the Wizard, select **Kaspersky Endpoint Security** as the task type, and then select **Update** as the task subtype.
4. Follow the rest of the Wizard instructions.

After the Wizard finishes, an update task for Kaspersky Endpoint Security is created. The newly created task is displayed in the list of tasks in the workspace of the **Tasks** folder.

5. In the workspace of the **Tasks** folder, select the update task that you have created.
6. In the context menu of the task, select **Properties**.
7. In the task properties window that opens, in the **Sections** pane select **Options**.

In the **Options** section, you can define the update task settings in local or mobile mode:

- **Update settings for local mode:** Connection is established between the device and the Administration Server.
 - **Update settings for mobile mode:** No connection is established between Kaspersky Security Center and the device (for example, when the device is not connected to the Internet).
8. Click the **Settings** button to select the update source.
 9. Select the **Download updates of application modules** check box to download and install software module updates together with the application databases.

If the check box is selected, Kaspersky Endpoint Security notifies the user about available software module updates and includes software module updates in the update package when running the update task.

Configure the use of update modules:

- **Install critical and approved updates.** If any updates are available for software modules, Kaspersky Endpoint Security automatically installs those that have *Critical* status; the remaining updates will be installed after you approve them.

- **Install only approved updates.** If any software module updates are available, Kaspersky Endpoint Security installs them after their installation is approved; they will be installed locally through the application interface or through Kaspersky Security Center.

If updating the software module requires reviewing and accepting the terms of the License Agreement and Privacy Policy, the application installs updates after the terms of the License Agreement and Privacy Policy have been accepted by the user.

10. Select the **Copy updates to folder** check box in order for the application to save downloaded updates to a folder, and then click the **Browse** button to specify the folder.
11. Click **OK**.

When the **Update** task is running, the application sends requests to Kaspersky update servers.

Some updates require installation of the latest versions of management plug-ins.

See also:

Scenario: Regular updating Kaspersky databases and applications	1174
---	----------------------

Offline model of update download

Network Agent on managed devices may sometimes not connect to the Administration Server to receive updates. For example, Network Agent may have been installed on a laptop that sometimes has no Internet connection and no local network access. Moreover, the administrator may limit the time for connecting devices to the network. In such cases, devices with Network Agent installed cannot receive updates from the Administration Server according to the existing schedule. If you have configured the updating of managed applications (such as Kaspersky Endpoint Security) using Network Agent, each update requires a connection to the Administration Server. When no connection is established between Network Agent and the Administration Server, updating is not possible. You can configure the connection between Network Agent and the Administration Server so that Network Agent connects to the Administration Server at specified time intervals. At worst, if the specified connection intervals are overlaid with periods when no connection is available, the databases will never be updated. In addition, issues may occur when multiple managed applications simultaneously attempt to access the Administration Server to receive updates. In this case, the Administration Server may stop responding to requests (similarly to a DDoS attack).

To avoid such problems as those described above, an offline model for downloading updates and modules of managed applications is implemented in Kaspersky Security Center. This model provides a mechanism for distribution of updates, regardless of temporary problems caused by inaccessibility of Administration Server communication channels. The model also reduces load on the Administration Server.

How the offline model of update download works

When the Administration Server receives updates, it notifies Network Agent (on devices where it is installed) of the updates that will be required for managed applications. When Network Agent receives information about these updates, it downloads the relevant files from the Administration Server in advance. At the first connection with Network Agent, the Administration Server initiates an update download. After Network Agent downloads all the updates to a client device, the updates become available for applications on that device.

When a managed application on a client device attempts to access Network Agent for updates, Network Agent checks whether it has all required updates. If the updates are received from the Administration Server not more than 25 hours before they were requested by the managed application, Network Agent does not connect to the Administration Server but supplies the managed application with updates from the local cache instead. Connection with the Administration Server may not be established when Network Agent provides updates to applications on client devices, but connection is not required for updating.

To distribute the load on the Administration Server, Network Agent on a device connects to the Administration Server and download updates in random order during the time interval specified by the Administration Server. This time interval depends on the number of devices with Network Agent installed that download updates and on the size of those updates. To reduce the load on the Administration Server, you can use Network Agent as distribution points.

If the offline model of update download is disabled, updates are distributed according to the schedule of the update download task.

By default, the offline model of update download is enabled.

The offline model of update download is only used with managed devices on which the task for retrieving updates by managed applications has **When new updates are downloaded to the repository** selected as the schedule type. For other managed devices, the standard scheme is used for retrieving updates from the Administration Server in real-time mode.

We recommend that you disable the offline model of update download by using the settings of the Network Agent policies of relevant administration groups in these cases: if managed applications have the retrieval of updates set not from the Administration Server, but from Kaspersky servers or a network folder, and if the update download task has **When new updates are downloaded to the repository** selected as the schedule type.

See also:

Scenario: Regular updating Kaspersky databases and applications	1174
Enabling and disabling the offline model of update download	443

Enabling and disabling the offline model of update download

We recommend that you avoid disabling the offline model of update download. Disabling it may cause failures in update delivery to devices. In certain cases, a Kaspersky Technical Support specialist may recommend that you clear the **Download updates and anti-virus databases from Administration Server in advance** check box. Then, you will have to make sure that the task for receiving updates for Kaspersky applications has been set up.

► *To enable or disable the offline model of update download for an administration group:*

1. In the console tree, select the administration group for which you need to enable the offline model of update download.
2. In the group workspace, open the **Policies** tab.
3. On the **Policies** tab, select the Network Agent policy.

4. In the context menu of the policy, select **Properties**.
Open the properties window of the Network Agent policy.
5. In the policy properties window, select the **Manage patches and updates** section.
6. Select or clear the **Download updates and anti-virus databases from Administration Server in advance (recommended)** check box to enable or disable, respectively, the offline model of update download.

By default, the offline model of update download is enabled.

The offline model of update download will be enabled or disabled.

See also:

Scenario: Regular updating Kaspersky databases and applications	1174
Offline model of update download	442

Installing updates on devices manually

If you have selected **Find and install required updates** on the **Update management settings** page of the Quick Start Wizard, the install required updates and fix vulnerabilities task is created automatically. You can run or stop the task in the **Managed devices** folder on the **Tasks** tab.

If you have selected **Search for required updates** in the Quick Start Wizard, you can install software updates on client devices through the **Install required updates and fix vulnerabilities** task.

You can do any of the following:

- Create a task for installing updates.
- Add a rule for installing an update to an existing update installation task.
- In the settings of an existing update installation task, configure a test installation of updates.

A user interaction may be required when you update a third-party application or fix a vulnerability in a third-party application on a managed device. For example, the user may be prompted to close the third-party application if it's currently open.

Installing updates by creating an installation task

You can do any of the following:

- Create a task for installing certain updates.
- Select an update and create a task for installing it and similar updates.

► *To install specific updates:*

1. In the **Advanced** → **Application management** folder in the console tree, select the **Software updates** subfolder.
2. In the workspace, select the updates that you want to install.

3. Do any of the following:
 - Right-click one of the selected updates in the list, and then select **Install update** → **New task**.
 - Click the **Install update (create task)** link in the information box for the selected updates.
4. Make your choice in the displayed prompt about installing all previous application updates. Click **Yes** if you agree to the installation of successive application versions incrementally if this is required for installing the selected updates. Click **No** if you want to update applications in a straightforward fashion, without installing successive versions. If installing the selected updates is not possible without installing previous versions of applications, the updating of the application fails.

The Updates Installation and Vulnerabilities Fix Task Creation Wizard starts. Proceed through the Wizard by using the **Next** button.

5. On the **Selecting an operating system restart option** page of the Wizard, select the action to perform when the operating system on client devices must be restarted after the operation:

- **Do not restart the device**

Client devices are not restarted automatically after the operation. To complete the operation, you must restart a device (for example, manually or through a device management task). Information about the required restart is saved in the task results and in the device status. This option is suitable for tasks on servers and other devices where continuous operation is critical.

- **Restart the device**

Client devices are always restarted automatically if a restart is required for completion of the operation. This option is useful for tasks on devices that provide for regular pauses in their operation (shutdown or restart).

- **Prompt user for action**

The restart reminder is displayed on the screen of the client device, prompting the user to restart it manually. Some advanced settings can be defined for this option: text of the message for the user, the message display frequency, and the time interval after which a restart will be forced (without the user's confirmation). This option is most suitable for workstations where users must be able to select the most convenient time for a restart.

By default, this option is selected.

- **Repeat prompt every (min)**

If this option is enabled, the application prompts the user to restart the operating system with the specified frequency.

By default, this option is enabled. The default interval is 5 minutes. Available values are between 1 and 1 440 minutes.

If this option is disabled, the prompt is displayed only once.

- **Restart after (min)**

After prompting the user, the application forces restart of the operating system upon expiration of the specified time interval.

By default, this option is enabled. The default delay is 30 minutes. Available values are between 1 and 1 440 minutes.

- **Force closure of applications in blocked sessions**

Running applications may prevent a restart of the client device. For example, if a document is being edited in a word processing application and is not saved, the application does not allow the device to restart.

If this option is enabled, such applications on a locked device are forced to close before the device restart. As a result, users may lose their unsaved changes.

If this option is disabled, a locked device is not restarted. The task status on this device states that a device restart is required. Users have to manually close all applications running on locked devices and restart these devices.

By default, this option is disabled.

1. On the **Configure task schedule** page of the Wizard, you can create a schedule for task start. If necessary, specify the following settings:

- **Scheduled start:**

Select the schedule according to which the task runs, and configure the selected schedule.

- **Every N hours**

The task runs regularly, with the specified interval in hours, starting from the specified date and time.

By default, the task runs every six hours, starting from the current system date and time.

- **Every N days**

The task runs regularly, with the specified interval in days. Additionally, you can specify a date and time of the first task run. These additional options become available, if they are supported by the application for which you create the task.

By default, the task runs every day, starting from the current system date and time.

- **Every N weeks**

The task runs regularly, with the specified interval in weeks, on the specified day of week and at the specified time.

By default, the task runs every Monday at the current system time.

- **Every N minutes**

The task runs regularly, with the specified interval in minutes, starting from the specified time on the day that the task is created.

By default, the task runs every 30 minutes, starting from the current system time.

- **Daily (daylight saving time is not supported)**

The task runs regularly, with the specified interval in days. This schedule does not support observance of daylight saving time (DST). It means that when clocks jump one hour forward or backward at the beginning or ending of DST, the actual task start time does not change.

We do not recommend that you use this schedule. It is needed for backward compatibility of Kaspersky Security Center.

By default, the task starts every day at the current system time.

- **Weekly**

The task runs every week on the specified day and at the specified time.

- **By days of week**

The task runs regularly, on the specified days of week, at the specified time.

By default, the task runs every Friday at 6:00:00 P.M.
- **Monthly**

The task runs regularly, on the specified day of the month, at the specified time.

In months that lack the specified day, the task runs on the last day.

By default, the task runs on the first day of each month, at the current system time.
- **Manually** (selected by default)

The task does not run automatically. You can only start it manually.
- **Every month on specified days of selected weeks**

The task runs regularly, on the specified days of each month, at the specified time.

By default, no days of month are selected; the default start time is 6:00:00 P.M.
- **On virus outbreak**

The task runs after a *Virus outbreak* event occurs. Select application types that will monitor virus outbreaks. The following application types are available:

 - Anti-virus for workstations and file servers
 - Anti-virus for perimeter defense
 - Anti-virus for mail systems

By default, all application types are selected.

You may want to run different tasks depending on the anti-virus application type that reports a virus outbreak. In this case, remove the selection of the application types that you do not need.
- **On completing another task**

The current task starts after another task completes. You can select how the previous task must complete (successfully or with error) to trigger the start of the current task. For example, you may want to run the Manage devices task with the **Turn on the device** option and, after it completes, run the Virus scan task.
- **Run missed tasks**

This option determines the behavior of a task if a client device is not visible on the network when the task is about to start.

If this option is enabled, the system attempts to start the task the next time the Kaspersky application is run on the client device. If the task schedule is **Manually**, **Once** or **Immediately**, the task is started immediately after the device becomes visible on the network or immediately after the device is included in the task scope.

If this option is disabled, only scheduled tasks run on client devices; for **Manually**, **Once** and **Immediately**, tasks run only on those client devices that are visible on the network. For example, you may want to disable this option for a resource-consuming task that you want to run only outside of business hours.

By default, this option is enabled.
- **Use automatically randomized delay for task starts**

If this option is enabled, the task is started on client devices randomly within a specified

time interval, that is, *distributed task start*. A distributed task start helps to avoid a large number of simultaneous requests by client devices to the Administration Server when a scheduled task is running.

The distributed start time is calculated automatically when a task is created, depending on the number of client devices to which the task is assigned. Later, the task is always started on the calculated start time. However when task settings are edited or the task is started manually, the calculated value of the task start time changes.

If this option is disabled, the task starts on client devices according to the schedule.

- **Use randomized delay for task starts within an interval of (min)**

If this option is enabled, the task is started on client devices randomly within the specified time interval. A distributed task start helps to avoid a large number of simultaneous requests by client devices to the Administration Server when a scheduled task is running.

If this option is disabled, the task starts on client devices according to the schedule.

By default, this option is disabled. The default time interval is one minute.

1. On the **Define the task name** page of the Wizard, specify the name for the task that you are creating. A task name cannot be more than 100 characters long and cannot include any special characters ("* <>? \:|).
2. On the **Finish task creation** page of the Wizard, click the **Finish** button to close the Wizard.

If you want the task to start as soon as the Wizard finishes, select the **Run the task after the Wizard finishes** check box.

After the Wizard completes its operation, **Install required updates and fix vulnerabilities** appears in the **Tasks** folder.

You can enable automatic installation of system components (prerequisites) prior to installation of an update in the Install required updates and fix vulnerabilities task properties. When this option is enabled, all required system components are installed before the update. A list of the required components can be found in properties of the update.

In the properties of Install required updates and fix vulnerabilities task, you can allow installation of updates that upgrade application to a new version.

If the task settings provide rules for installation of third-party updates, the Administration Server downloads all relevant updates from their vendors' websites. Updates are saved to the Administration Server repository and then distributed and installed on devices where they are applicable.

If the task settings provide rules for installation of Microsoft updates and the Administration Server acts as a WSUS server, the Administration Server downloads all relevant updates to the repository and then distributes them to managed devices. If the network does not use a WSUS server, each client device downloads Microsoft updates from external servers independently.

► *To install a certain update and similar ones:*

1. In the **Advanced** → **Application management** folder in the console tree, select the **Software updates** subfolder.
2. In the workspace, select the update that you want to install.
3. Click the **Run Update Installation Wizard** button.

The Update Installation Wizard starts.

The Update Installation Wizard features are only available under the Vulnerability and Patch Management license.

Proceed through the Wizard by using the **Next** button.

4. On the **Search for existing update installation tasks** page, specify the following settings:
 - **Search for tasks that install this update**

If this option is enabled, the Update Installation Wizard searches for existing tasks that install the selected update.

If this option is disabled or if the search retrieves no applicable tasks, the Update Installation Wizard prompts you to create a rule or task for installing the update.

By default, this option is enabled.

- **Approve update installation**

The selected update will be approved for installation. Enable this option if some applied rules of update installation allow installation of approved updates only.

By default, this option is disabled.

1. If you choose to search for existing update installation tasks and if the search retrieves some tasks, you can view properties of these tasks or start them manually. No further actions are required.
Otherwise, click the **New update installation task** button.
2. Select the type of the installation rule to be added to the new task, and then click the **Finish** button.
3. Make your choice in the displayed prompt about installing all previous application updates. Click **Yes** if you agree to the installation of successive application versions incrementally if this is required for installing the selected updates. Click **No** if you want to update applications in a straightforward fashion, without installing successive versions. If installing the selected updates is not possible without installing previous versions of applications, the updating of the application fails.

The Updates Installation and Vulnerabilities Fix Task Creation Wizard starts. Proceed through the Wizard by using the **Next** button.

4. On the **Selecting an operating system restart option** page of the Wizard, select the action to perform when the operating system on client devices must be restarted after the operation:

- **Do not restart the device**

Client devices are not restarted automatically after the operation. To complete the operation, you must restart a device (for example, manually or through a device management task). Information about the required restart is saved in the task results and in the device status. This option is suitable for tasks on servers and other devices where continuous operation is critical.

- **Restart the device**

Client devices are always restarted automatically if a restart is required for completion of the operation. This option is useful for tasks on devices that provide for regular pauses in their operation (shutdown or restart).

- **Prompt user for action**

The restart reminder is displayed on the screen of the client device, prompting the user to restart it manually. Some advanced settings can be defined for this option: text of the

message for the user, the message display frequency, and the time interval after which a restart will be forced (without the user's confirmation). This option is most suitable for workstations where users must be able to select the most convenient time for a restart.

By default, this option is selected.

- **Repeat prompt every (min)**

If this option is enabled, the application prompts the user to restart the operating system with the specified frequency.

By default, this option is enabled. The default interval is 5 minutes. Available values are between 1 and 1 440 minutes.

If this option is disabled, the prompt is displayed only once.

- **Restart after (min)**

After prompting the user, the application forces restart of the operating system upon expiration of the specified time interval.

By default, this option is enabled. The default delay is 30 minutes. Available values are between 1 and 1 440 minutes.

- **Force closure of applications in blocked sessions**

Running applications may prevent a restart of the client device. For example, if a document is being edited in a word processing application and is not saved, the application does not allow the device to restart.

If this option is enabled, such applications on a locked device are forced to close before the device restart. As a result, users may lose their unsaved changes.

If this option is disabled, a locked device is not restarted. The task status on this device states that a device restart is required. Users have to manually close all applications running on locked devices and restart these devices.

By default, this option is disabled.

1. On the **Select devices to which the task will be assigned** page of the Wizard, select one of the following options:

- **Select networked devices detected by Administration Server**

The task is assigned to specific devices. The specific devices can include devices in administration groups as well as unassigned devices.

For example, you may want to use this option in a task of installing Network Agent on unassigned devices.

- **Specify device addresses manually or import addresses from a list**

You can specify NetBIOS names, DNS names, IP addresses, and IP subnets of devices to which you want to assign the task.

You may want to use this option to execute a task for a specific subnet. For example, you may want to install a certain application on devices of accountants or to scan devices in a subnet that is probably infected.

- **Assign task to a device selection**

The task is assigned to devices included in a device selection. You can specify one of the existing selections.

For example, you may want to use this option to run a task on devices with a specific operating system version.

- **Assign task to an administration group**

The task is assigned to devices included in an administration group. You can specify one of the existing groups or create a new one.

For example, you may want to use this option to run a task of sending a message to users if the message is specific for devices included in a specific administration group.

2. On the **Configure task schedule** page of the Wizard, you can create a schedule for task start. If necessary, specify the following settings:

- **Scheduled start:**

Select the schedule according to which the task runs, and configure the selected schedule.

- **Every N hours**

The task runs regularly, with the specified interval in hours, starting from the specified date and time.

By default, the task runs every six hours, starting from the current system date and time.

- **Every N days**

The task runs regularly, with the specified interval in days. Additionally, you can specify a date and time of the first task run. These additional options become available, if they are supported by the application for which you create the task.

By default, the task runs every day, starting from the current system date and time.

- **Every N weeks**

The task runs regularly, with the specified interval in weeks, on the specified day of week and at the specified time.

By default, the task runs every Monday at the current system time.

- **Every N minutes**

The task runs regularly, with the specified interval in minutes, starting from the specified time on the day that the task is created.

By default, the task runs every 30 minutes, starting from the current system time.

- **Daily (daylight saving time is not supported)**

The task runs regularly, with the specified interval in days. This schedule does not support observance of daylight saving time (DST). It means that when clocks jump one hour forward or backward at the beginning or ending of DST, the actual task start time does not change.

We do not recommend that you use this schedule. It is needed for backward compatibility of Kaspersky Security Center.

By default, the task starts every day at the current system time.

- **Weekly**

The task runs every week on the specified day and at the specified time.

- **By days of week**

The task runs regularly, on the specified days of week, at the specified time.

By default, the task runs every Friday at 6:00:00 P.M.

- **Monthly**

The task runs regularly, on the specified day of the month, at the specified time.

In months that lack the specified day, the task runs on the last day.

By default, the task runs on the first day of each month, at the current system time.

- **Manually** (selected by default)

The task does not run automatically. You can only start it manually.

- **Every month on specified days of selected weeks**

The task runs regularly, on the specified days of each month, at the specified time.

By default, no days of month are selected; the default start time is 6:00:00 P.M.

- **On virus outbreak**

The task runs after a *Virus outbreak* event occurs. Select application types that will monitor virus outbreaks. The following application types are available:

- Anti-virus for workstations and file servers
- Anti-virus for perimeter defense
- Anti-virus for mail systems

By default, all application types are selected.

You may want to run different tasks depending on the anti-virus application type that reports a virus outbreak. In this case, remove the selection of the application types that you do not need.

- **On completing another task**

The current task starts after another task completes. You can select how the previous task must complete (successfully or with error) to trigger the start of the current task. For example, you may want to run the Manage devices task with the **Turn on the device** option and, after it completes, run the Virus scan task.

- **Run missed tasks**

This option determines the behavior of a task if a client device is not visible on the network when the task is about to start.

If this option is enabled, the system attempts to start the task the next time the Kaspersky application is run on the client device. If the task schedule is **Manually**, **Once** or **Immediately**, the task is started immediately after the device becomes visible on the network or immediately after the device is included in the task scope.

If this option is disabled, only scheduled tasks run on client devices; for **Manually**, **Once** and **Immediately**, tasks run only on those client devices that are visible on the network. For example, you may want to disable this option for a resource-consuming task that you want to run only outside of business hours.

By default, this option is enabled.

- **Use randomized delay for task starts within an interval of (min)**

If this option is enabled, the task is started on client devices randomly within a specified time interval, that is, *distributed task start*. A distributed task start helps to avoid a large number of simultaneous requests by client devices to the Administration Server when a scheduled task is running.

The distributed start time is calculated automatically when a task is created, depending on the number of client devices to which the task is assigned. Later, the task is always started on the calculated start time. However when task settings are edited or the task is started manually, the calculated value of the task start time changes.

If this option is disabled, the task starts on client devices according to the schedule.

- **Use randomized delay for task starts within an interval of (min)**

If this option is enabled, the task is started on client devices randomly within the specified time interval. A distributed task start helps to avoid a large number of simultaneous requests by client devices to the Administration Server when a scheduled task is running.

If this option is disabled, the task starts on client devices according to the schedule.

By default, this option is disabled. The default time interval is one minute.

1. On the **Define the task name** page of the Wizard, specify the name for the task that you are creating. A task name cannot be more than 100 characters long and cannot include any special characters ("*<>?:\.!).
2. On the **Finish task creation** page of the Wizard, click the **Finish** button to close the Wizard.

If you want the task to start as soon as the Wizard finishes, select the **Run the task after the Wizard finishes** check box.

When the Wizard finishes, the **Install required updates and fix vulnerabilities** task is created and displayed in the **Tasks** folder.

In addition to the settings that you specify during task creation, you can change other properties of a created task.

Upgrading to a new version of the application may cause a malfunction of dependent applications on devices.

Installing an update by adding a rule to an existing installation task

► *To install an update by adding a rule to an existing installation task:*

1. In the **Advanced** → **Application management** folder in the console tree, select the **Software updates** subfolder.
2. In the workspace, select the update that you want to install.
3. Click the **Run Update Installation Wizard** button.

The Update Installation Wizard starts.

The Update Installation Wizard features are only available under the Vulnerability and Patch Management license.

Proceed through the Wizard by using the **Next** button.

4. On the **Search for existing update installation tasks** page, specify the following settings:
 - **Search for tasks that install this update**

If this option is enabled, the Update Installation Wizard searches for existing tasks that install the selected update.

If this option is disabled or if the search retrieves no applicable tasks, the Update Installation Wizard prompts you to create a rule or task for installing the update.

By default, this option is enabled.

- **Approve update installation**

The selected update will be approved for installation. Enable this option if some applied rules of update installation allow installation of approved updates only.

By default, this option is disabled.

1. If you choose to search for existing update installation tasks and if the search retrieves some tasks, you can view properties of these tasks or start them manually. No further actions are required.
Otherwise, click the **Add an update installation rule** button.
2. Select the task to which you want to add a rule, and then click the **Add rule** button.
Also, you can view properties of the existing tasks, start them manually, or create a new task.
3. Select the type of the rule to be added to the selected task, and then click the **Finish** button.
4. Make your choice in the displayed prompt about installing all previous application updates. Click **Yes** if you agree to the installation of successive application versions incrementally if this is required for installing the selected updates. Click **No** if you want to update applications in a straightforward fashion, without installing successive versions. If installing the selected updates is not possible without installing previous versions of applications, the updating of the application fails.

A new rule for installing the update is added to the existing **Install required updates and fix vulnerabilities** task.

Configuring a test installation of updates

► *To configure a test installation of updates:*

1. In the console tree, select the **Install required updates and fix vulnerabilities** task in the **Managed devices** folder on the **Tasks** tab.
2. From the context menu of the task, select **Properties**.
The properties window of the **Install required updates and fix vulnerabilities** task opens.
3. In the properties window of the task, in the **Test installation** section select one of the available options for test installation:
 - **Do not scan.** Select this option if you do not want to perform a test installation of updates.
 - **Run scan on selected devices.** Select this option if you want to test updates installation on selected devices. Click the **Add** button and select devices on which you need to perform test installation of updates.
 - **Run scan on devices in the specified group.** Select this option if you want to test updates installation on a group of devices. In the **Specify a test group** field, specify a group of devices on which you want to perform a test installation.
 - **Run scan on specified percentage of devices.** Select this option if you want to test updates installation on some portion of devices. In the **Percentage of test devices out of all target devices** field, specify the percentage of devices on which you want to perform a test installation of updates.

4. Upon selecting any option except **Do not scan**, in the **Time to make the decision if the installation is to be continued (h)** field specify the number of hours that must elapse from the test installation of updates until the start of installation of the updates on all devices.

Configuring Windows updates in a Network Agent policy

► *To configure Windows Updates in a Network Agent policy:*

1. In the console tree, select **Managed devices**.
2. In the workspace, select the **Policies** tab.
3. Select a Network Agent policy.
4. In the context menu of the policy, select **Properties**.
The properties window for the Network Agent policy opens.
5. In the **Sections** pane, select **Software updates and vulnerabilities**.
6. Select the **Use Administration Server as a WSUS server** check box to download Windows updates to the Administration Server and then distribute them to client devices through Network Agent.
If this check box is cleared, Windows updates are not downloaded to the Administration Server. In this case, client devices receive Windows updates directly from Microsoft servers.
7. Select the set of updates that the users can install on their devices manually by using Windows Update.

On devices running Windows 10, if Windows Update already has updates found for the device, the new option that you select under **Allow users to manage installation of Windows Update updates** will be applied only after the found updates are installed.

Select an item in the drop-down list:

- **Allow users to install all applicable Windows Update updates**

Users can install all of the Microsoft Windows Update updates that are applicable to their devices.

Select this option if you do not want to interfere in the installation of updates.

When the user installs Microsoft Windows Update updates manually, the updates may be downloaded from Microsoft servers rather than from Administration Server. This is possible if Administration Server has not yet downloaded these updates. Downloading updates from Microsoft servers results in extra traffic.

- **Allow users to install only approved Windows Update updates**

Users can install all of the Microsoft Windows Update updates that are applicable to their devices and that are approved by you.

For example, you may want to first check the installation of updates in a test environment and make sure that they do not interfere with the operation of devices, and only then allow the installation of these approved updates on client devices.

When the user installs Microsoft Windows Update updates manually, the updates may be downloaded from Microsoft servers rather than from Administration Server. This is possible if Administration Server has not yet downloaded these updates. Downloading updates from Microsoft servers results in extra traffic.

- **Do not allow users to install Windows Update updates**

Users cannot install Microsoft Windows Update updates on their devices manually. All of the applicable updates are installed as configured by you.

Select this option if you want to manage the installation of updates centrally.

For example, you may want to optimize the update schedule so that the network does not become overloaded. You can schedule after-hours updates, so that they do not interfere with user productivity.

1. Select the Windows Update search mode:

- **Active**

If this option is selected, Administration Server with support from Network Agent initiates a request from Windows Update Agent on the client device to the update source: Windows Update Servers or WSUS. Next, Network Agent passes information received from Windows Update Agent to Administration Server.

The option takes effect only if **Connect to the update server to update data** option of the *Find vulnerabilities and required updates* task is selected.

By default, this option is selected.

- **Passive**

If you select this option, Network Agent periodically passes Administration Server information about updates retrieved at the last synchronization of Windows Update Agent with the update source. If no synchronization of Windows Update Agent with an update source is performed, information about updates on Administration Server becomes out-of-date.

Select this option if you want to get updates from the memory cache of the update source.

- **Disabled**

If this option is selected, Administration Server does not request any information about updates.

Select this option if, for example, you want to test the updates on your local device first.

2. Select the **Scan executable files for vulnerabilities when running them** check box if you want to scan executable files for vulnerabilities when they are being run.

3. Click **Apply**.

See also:

| Scenario: Updating third-party software [1208](#)

Automatic updating and patching for Kaspersky Security Center components

By default, any updates and patches that have been downloaded are installed automatically for the following application components (starting from version 10 Service Pack 2):

- Network Agent for Windows
- Administration Console
- Exchange Mobile Device Server
- iOS MDM Server

Automatic updating and patching for Kaspersky Security Center components is available only for devices running Windows. You can disable automatic updating and patching for these components. In this case, any updates and patches that have been downloaded will be installed only after you change their status to *Approved*. Updates and patches with *Undefined* status will not be installed.

See also:

- Scenario: Regular updating Kaspersky databases and applications[1174](#)
- Enabling and disabling automatic updating and patching for Kaspersky Security Center components[458](#)

Enabling and disabling automatic updating and patching for Kaspersky Security Center components

Automatic installation of updates and patches for Kaspersky Security Center components is enabled by default during Network Agent installation on the device. You can disable it during Network Agent installation, or disable it later by using a policy.

► *To disable automatic updating and patching for Kaspersky Security Center components during local installation of Network Agent on a device:*

1. Start local installation of Network Agent on the device (see section "Local installation of Network Agent" on page [178](#)).
2. At the **Advanced settings** step, clear the **Automatically install applicable updates and patches for components that have Undefined status** check box.
3. Follow the instructions of the Wizard.

Network Agent with disabled automatic updating and patching for Kaspersky Security Center components will be installed on the device. You can enable automatic updating and patching later by using a policy.

► *To disable automatic updating and patching for Kaspersky Security Center components during Network Agent installation on the device through an installation package:*

1. In the console tree, select the **Remote installation** → **Installation packages** folder.
2. In the context menu of the **Kaspersky Security Center Network Agent <version number>** package, select **Properties**.
3. In the installation package properties, in the **Settings** section clear the **Automatically install applicable updates and patches for components that have the Undefined status** check box.

Network Agent with disabled automatic updating and patching for Kaspersky Security Center components will be installed from this package. You can enable automatic updating and patching later by using a policy.

If this check box was selected (or cleared) during Network Agent installation on the device, you can subsequently enable (or disable) automatic updating by using the Network Agent policy.

► *To enable or disable automatic updating and patching for Kaspersky Security Center components by using the Network Agent policy:*

1. In the console tree, select the administration group for which you have to enable or disable automatic updating and patching.
2. In the group workspace, open the **Policies** tab.
3. On the **Policies** tab, select the Network Agent policy.
4. In the context menu of the policy, select **Properties**.
Open the properties window of the Network Agent policy.
5. In the policy properties window, select the **Manage patches and updates** section.
6. Select or clear the **Automatically install applicable updates and patches for components that have the Undefined status** check box to enable or disable, respectively, automatic updating and patching.
7. Set the lock for this check box.

The policy will be applied to the selected devices, and automatic updating and patching for Kaspersky Security Center components will be enabled (or disabled) on these devices.

See also:

Scenario: Regular updating Kaspersky databases and applications	1174
Automatic updating and patching for Kaspersky Security Center components	457

Fixing third-party software vulnerabilities

This section describes the features of Kaspersky Security Center that relate to fixing vulnerabilities in the software installed on managed devices.

In this section

Scenario: Finding and fixing vulnerabilities in third-party software	459
About finding and fixing software vulnerabilities.....	462
Viewing information about software vulnerabilities.....	463
Viewing statistics of vulnerabilities on managed devices	463
Scanning applications for vulnerabilities.....	464
Fixing vulnerabilities in applications	469
Ignoring software vulnerabilities	480
Selecting user fixes for vulnerabilities in third-party software.....	481
Rules for update installation	482

Scenario: Finding and fixing vulnerabilities in third-party software

This section provides a scenario for finding and fixing vulnerabilities on the managed devices running Windows. You can find and fix software vulnerabilities in the operating system and in third-party software, including Microsoft software.

Prerequisites

- Kaspersky Security Center is deployed in your organization.
- There are managed devices running Windows in your organization.
- Internet connection is required for Administration Server to perform the following tasks:
 - To make a list of recommended fixes for vulnerabilities in Microsoft software. The list is created and regularly updated by Kaspersky specialists.
 - To fix vulnerabilities in third-part software other than Microsoft software.

Stages

Finding and fixing software vulnerabilities proceeds in stages:

a. Scanning for vulnerabilities in the software installed on the managed devices

To find vulnerabilities in the software installed on the managed devices, run the *Find vulnerabilities and required updates* task. When this task is complete, Kaspersky Security Center receives the lists of detected vulnerabilities and required updates for the third-party software installed on the devices that you specified in the task properties.

The *Find vulnerabilities and required updates* task is created automatically by Kaspersky Security Center Quick Start Wizard. If you did not run the Wizard, start it now or create the task manually.

How-to instructions:

- Administration Console: Scanning applications for vulnerabilities (on page [464](#)), Scheduling the Find vulnerabilities and required updates task (on page [372](#))

or

- Kaspersky Security Center 13 Web Console: Creating the Find vulnerabilities and required updates task (see section "Creating the Find vulnerabilities and required updates task" on page [1216](#)), Find vulnerabilities and required updates task settings (on page [1219](#))

b. Analyzing the list of detected software vulnerabilities

View the **Software vulnerabilities** list and decide which vulnerabilities are to be fixed. To view detailed information about each vulnerability, click the vulnerability name in the list. For each vulnerability in the list, you can also view the statistics on the vulnerability on managed devices.

How-to instructions:

- Administration Console: Viewing information about software vulnerabilities (on page [463](#)), Viewing statistics of vulnerabilities on managed devices (on page [463](#))

or

- Kaspersky Security Center 13 Web Console: Viewing information software vulnerabilities (see section "Viewing information about software vulnerabilities detected on all managed devices" on page [1254](#)), Viewing statistics of vulnerabilities on managed devices (on page [1255](#))

c. Configuring vulnerabilities fix

When the software vulnerabilities are detected, you can fix the software vulnerabilities on the managed devices by using the *Install required updates and fix vulnerabilities* (see section "Creating the *Install required updates and fix vulnerabilities* task" on page [1221](#)) task or the *Fix vulnerabilities* (see section "Creating the *Fix vulnerabilities* task" on page [1244](#)) task.

The *Install required updates and fix vulnerabilities* task is used to update and fix vulnerabilities in third-party software, including Microsoft software, installed on the managed devices. This task allows you to install multiple updates and fix multiple vulnerabilities according to certain rules. Note that this task can be created only if you have the license for the Vulnerability and Patch Management feature. To fix software vulnerabilities the *Install required updates and fix vulnerabilities* task uses recommended software updates.

The *Fix vulnerabilities* task does not require the license option for the Vulnerability and Patch Management feature. To use this task, you must manually specify user fixes for vulnerabilities in third-party software listed in the task settings. The *Fix vulnerabilities* task uses recommended fixes for Microsoft software and user fixes for third-party software.

You can start Vulnerabilities Fix Wizard that creates one of these tasks automatically, or you can create one of these tasks manually.

How-to instructions:

- Administration Console: Selecting user fixes for vulnerabilities in third-party software (on page [481](#)), Fixing vulnerabilities in applications (on page [469](#))

or

- Kaspersky Security Center 13 Web Console: Selecting user fixes for vulnerabilities in third-party software (on page [1253](#)), Fixing vulnerabilities in third-party software (on page [1241](#)), Creating the Install required updates and fix vulnerabilities task (on page [1221](#))

d. Scheduling the tasks

To be sure that the vulnerabilities list is always up-to-date, schedule the *Find vulnerabilities and required updates* task to run it automatically from time to time. The recommended average frequency is once a week.

If you have created the *Install required updates and fix vulnerabilities* task, you can schedule it to run with the same frequency as the *Find vulnerabilities and required updates* task or less often. When scheduling the *Fix vulnerabilities* task, note that you have to select fixes for Microsoft software or specify user fixes for third-party software every time before starting the task.

When scheduling the tasks, make sure that a task to fix vulnerability starts after the *Find vulnerabilities and required updates* task is complete.

e. Ignoring software vulnerabilities (optional)

If you want, you can ignore software vulnerabilities to be fixed on all managed devices or only on the selected managed devices.

How-to instructions:

- Administration Console: Ignoring software vulnerabilities (on page [480](#))

or

- Kaspersky Security Center 13 Web Console: Ignoring software vulnerabilities (on page [1256](#))

f. Running a vulnerability fix task

Start the *Install required updates and fix vulnerabilities* task or the *Fix vulnerability* task. When the task is complete, make sure that it has the *Completed successfully* status in the task list.

g. Create the report on results of fixing software vulnerabilities (optional)

To view detailed statistics on the vulnerabilities fix, generate the Report on vulnerabilities. The report displays information about software vulnerabilities that are not fixed. Thus you can have an idea about finding and fixing vulnerabilities in third-party software, including Microsoft software, in your organization.

How-to instructions:

- Administration Console: Creating and viewing a report (on page [509](#))

or

- Kaspersky Security Center 13 Web Console: Generating and viewing a report (on page [1287](#))

h. Checking configuration of finding and fixing vulnerabilities in third-party software

Be sure you have done the following:

- Obtained and reviewed the list of software vulnerabilities on managed devices
- Ignored software vulnerabilities if you wanted
- Configured the task to fix vulnerabilities

- Scheduled the tasks to find and to fix software vulnerabilities so that they start sequentially
- Checked that the task to fix software vulnerabilities was run

Results

If you have created and configured the *Install required updates and fix vulnerabilities* task, the vulnerabilities are fixed on the managed devices automatically. When the task is run, it correlates the list of available software updates to the rules specified in the task settings. All software updates that meet the criteria in the rules will be downloaded to the Administration Server repository and will be installed to fix software vulnerabilities.

If you have created the *Fix vulnerabilities* task, only software vulnerabilities in Microsoft software are fixed.

About finding and fixing software vulnerabilities

Kaspersky Security Center detects and fixes software vulnerabilities on managed devices running Microsoft Windows families operating systems. Vulnerabilities are detected in the operating system and in third-party software, including Microsoft software.

Finding software vulnerabilities

To find software vulnerabilities, Kaspersky Security Center uses characteristics from the database of known vulnerabilities. This database is created by Kaspersky specialists. It contains information about vulnerabilities, such as vulnerability description, vulnerability detect date, vulnerability severity level. You can find the details of software vulnerabilities on Kaspersky website (<https://threats.kaspersky.com/en/>).

Kaspersky Security Center uses the *Find vulnerabilities and required updates* task to find software vulnerabilities.

Fixing software vulnerabilities

To fix software vulnerabilities Kaspersky Security Center uses software updates issued by the software vendors. The software updates metadata is downloaded to the Administration Server repository as a result of the following tasks run:

- *Download updates to the Administration Server repository.* This task is intended to download updates metadata for Kaspersky and third-party software. This task is created automatically by the Kaspersky Security Center Quick Start Wizard. You can create the Download updates to the Administration Server repository task (see section "Creating the task for downloading updates to the repository of the Administration Server" on page [1184](#)) manually.
- *Perform Windows Update synchronization.* This task is intended to download updates metadata for Microsoft software.

Software updates to fix vulnerabilities can be represented as full distribution packages or patches. Software updates that fix software vulnerabilities are named *fixes*. *Recommended fixes* are those that are recommended for installation by Kaspersky specialists. *User fixes* are those that are manually specified for installation by users. To install a user fix, you have to create an installation package containing this fix.

If you have the Kaspersky Security Center license with the Vulnerability and Patch Management feature, to fix software vulnerabilities you can use *Install required updates and fix vulnerabilities* task. This task automatically fixes multiple vulnerabilities installing recommended fixes. For this task, you can manually configure certain rules to fix multiple vulnerabilities.

If you do not have the Kaspersky Security Center license with the Vulnerability and Patch Management feature, to fix software vulnerabilities, you can use the *Fix vulnerabilities* task. By means of this task, you can fix vulnerabilities by installing recommended fixes for Microsoft software and user fixes for other third-party software.

A user interaction may be required when you update a third-party application or fix a vulnerability in a third-party application on a managed device. For example, the user may be prompted to close the third-party application if it's currently open.

To fix some software vulnerabilities, you must accept the End User License Agreement (EULA) of the software that is being installed, if EULA acceptance is requested. If you decline the EULA, the software vulnerability is not fixed.

Viewing information about software vulnerabilities

- ▶ *To view a list of vulnerabilities detected on client devices,*

In the **Advanced** → **Application management** folder in the console tree, select the **Software vulnerabilities** subfolder.

The page displays a list of vulnerabilities in applications detected on managed devices.

- ▶ *To obtain information about a selected vulnerability,*

Select **Properties** from the context menu of the vulnerability.

The properties window of the vulnerability opens, displaying the following information:

- Application in which the vulnerability has been detected.
- List of devices on which the vulnerability has been detected.
- Information on whether the vulnerability has been fixed.

- ▶ *To view the report on all detected vulnerabilities,*

In the **Software vulnerabilities** folder, click the **View report on vulnerabilities** link.

A report on vulnerabilities in applications installed on devices will be generated. You can view this report in the node with the name of the relevant Administration Server, by opening the **Reports** tab.

Viewing statistics of vulnerabilities on managed devices

You can view statistics for each software vulnerability on managed devices. Statistics is represented as a diagram. The diagram displays the number of devices with the following statuses:

- *Ignored on: <number of devices>.* The status is assigned if, in the vulnerability properties, you have manually set the option to ignore the vulnerability.
- *Fixed on: <number of devices>.* The status is assigned if the task to fix the vulnerability has successfully completed.
- *Fix scheduled on: <number of devices>.* The status is assigned if you have created the task to fix the vulnerability but the task is not performed yet.
- *Patch applied on: <number of devices>.* The status is assigned if you have manually selected a software update to fix the vulnerability but this software updated has not fixed the vulnerability.

Fix required on: <number of devices>. The status is assigned if the vulnerability was fixed only on the part of managed devices, and it is required to be fixed on the rest part of managed devices.

► *To view the statistics of a vulnerability on managed devices:*

1. In the **Advanced** → **Application management** folder in the console tree, select the **Software vulnerabilities** subfolder.

The page displays a list of vulnerabilities in applications detected on managed devices.

2. Select a vulnerability for which you want to view the statistics.

In the block for working with a selected object, a diagram of the vulnerability statuses is displayed. Clicking a status opens a list of devices on which the vulnerability has the selected status.

Scanning applications for vulnerabilities

If you have configured the application through the Quick Start Wizard, the Vulnerability scan task is created automatically. You can view the task in the **Managed devices** folder, on the **Tasks** tab.

► *To create a task for vulnerability scanning in applications installed on client devices:*

1. In the console tree, select **Advanced** → **Application management**, and then select the **Software vulnerabilities** subfolder.

2. In the workspace, select **Additional actions** → **Configure vulnerability scan**.

If a task for vulnerability scanning already exists, the **Tasks** tab of the **Managed devices** folder is displayed, with the existing task selected. Otherwise, the Vulnerabilities and Required Updates Search Task Creation Wizard starts. Proceed through the Wizard by using the **Next** button.

3. In the **Select the task type** window, select **Find vulnerabilities and required updates**.

4. On the **Settings** page of the Wizard, specify the task settings as follows:

- **Search for vulnerabilities and updates listed by Microsoft**

When searching for vulnerabilities and updates, Kaspersky Security Center uses the information about applicable Microsoft updates from the source of Microsoft updates, which are available at the present moment.

For example, you may want to disable this option if you have different tasks with different settings for Microsoft updates and updates of third-party applications.

By default, this option is enabled.

- **Connect to the update server to update data**

Windows Update Agent on a managed device connects to the source of Microsoft updates. The following servers can act as a source of Microsoft updates:

- Kaspersky Security Center Administration Server (see the settings of Network Agent policy (see section "Network Agent policy settings" on page [665](#)))
- Windows Server with Microsoft Windows Server Update Services (WSUS) deployed in your organization's network
- Microsoft Updates servers

If this option is enabled, Windows Update Agent on a managed device connects to the source of Microsoft updates to refresh the information about applicable Microsoft Windows updates.

If this option is disabled, Windows Update Agent on a managed device uses the information about applicable Microsoft Windows updates that was received from the source of Microsoft updates earlier and that is stored in the device's cache.

Connecting to the source of Microsoft updates can be resource-consuming. You might want to disable this option if you set regular connection to this source of updates in another task or in the properties of Network Agent policy, in the section **Software updates and vulnerabilities**. If you do not want to disable this option, then, to reduce the Server overload, you can configure the task schedule to randomize delay for task starts within 360 minutes.

By default, this option is enabled.

Combination of the following options of the settings of Network Agent policy defines the mode of getting updates:

- Windows Update Agent on a managed device connects to the Update Server to get updates only if the **Connect to the update server to update data** option is enabled and the **Active** option, in the **Windows Update search mode** settings group, is selected.
- Windows Update Agent on a managed device uses the information about applicable Microsoft Windows updates that was received from the source of Microsoft updates earlier and that is stored in the device's cache, if the **Connect to the update server to update data** option is enabled and the **Passive** option, in the **Windows Update search mode** settings group, is selected, or if the **Connect to the update server to update data** option is disabled and the **Active** option, in the **Windows Update search mode** settings group, is selected.
- Irrespective of the **Connect to the update server to update data** option's status (enabled or disabled), if **Disabled** option, in the **Windows Update search mode** settings group is selected, Kaspersky Security Center does not request any information about updates.

- **Search for third-party vulnerabilities and updates listed by Kaspersky**

If this option is enabled, Kaspersky Security Center searches for vulnerabilities and required updates for third-party applications (applications made by software vendors other than Kaspersky and Microsoft) in Windows Registry and in the folders specified under **Specify paths for advanced search of applications in file system**. The full list of supported third-party applications is managed by Kaspersky.

If this option is disabled, Kaspersky Security Center does not search for vulnerabilities and required updates for third-party applications. For example, you may want to disable this option if you have different tasks with different settings for Microsoft Windows updates and updates of third-party applications.

By default, this option is enabled.

- **Specify paths for advanced search of applications in file system**

The folders in which Kaspersky Security Center searches for third-party applications that require vulnerability fix and update installation. You can use system variables.

Specify the folders to which applications are installed. By default, the list contains system folders to which most of the applications are installed.

- **Enable advanced diagnostics**

If this feature is enabled, Network Agent writes traces even if tracing is disabled for Network Agent in Kaspersky Security Center Remote Diagnostics Utility. Traces are written to two files in turn; the total size of both files is determined by the **Maximum size**,

in MB, of advanced diagnostics files value. When both files are full, Network Agent starts writing to them again. The files with traces are stored in the %WINDIR%\Temp folder. These files are accessible in the remote diagnostics utility (see section "Remote diagnostics of client devices. Kaspersky Security Center remote diagnostics utility" on page [651](#)), you can download or delete them there.

If this feature is disabled, Network Agent writes traces according to the settings in Kaspersky Security Center Remote Diagnostics Utility. No additional traces are written.

When creating a task, you do not have to enable advanced diagnostics. You may want to use this feature later if, for example, a task run fails on some of the devices and you want to collect additional information during another task run.

By default, the feature is disabled.

- **Maximum size, in MB, of advanced diagnostics files**

The default value is 100 MB, and available values are between 1 MB and 2 048 MB. You may be asked to change the default value by Kaspersky Technical Support specialists when information in the advanced diagnostics files sent by you is not enough to troubleshoot the problem.

1. On the **Configure task schedule** page of the Wizard, you can create a schedule for task start. If necessary, specify the following settings:

- **Scheduled start:**

Select the schedule according to which the task runs, and configure the selected schedule.

- **Every N hours**

The task runs regularly, with the specified interval in hours, starting from the specified date and time.

By default, the task runs every six hours, starting from the current system date and time.

- **Every N days**

The task runs regularly, with the specified interval in days. Additionally, you can specify a date and time of the first task run. These additional options become available, if they are supported by the application for which you create the task.

By default, the task runs every day, starting from the current system date and time.

- **Every N weeks**

The task runs regularly, with the specified interval in weeks, on the specified day of week and at the specified time.

By default, the task runs every Monday at the current system time.

- **Every N minutes**

The task runs regularly, with the specified interval in minutes, starting from the specified time on the day that the task is created.

By default, the task runs every 30 minutes, starting from the current system time.

- **Daily (daylight saving time is not supported)**

The task runs regularly, with the specified interval in days. This schedule does not support observance of daylight saving time (DST). It means that when clocks jump one hour forward or backward at the beginning or ending of DST, the actual task start time does not change.

We do not recommend that you use this schedule. It is needed for backward compatibility of Kaspersky Security Center.

By default, the task starts every day at the current system time.

- **Weekly**

The task runs every week on the specified day and at the specified time.

- **By days of week**

The task runs regularly, on the specified days of week, at the specified time.

By default, the task runs every Friday at 6:00:00 P.M.

- **Monthly**

The task runs regularly, on the specified day of the month, at the specified time.

In months that lack the specified day, the task runs on the last day.

By default, the task runs on the first day of each month, at the current system time.

- **Manually** (selected by default)

The task does not run automatically. You can only start it manually.

- **Every month on specified days of selected weeks**

The task runs regularly, on the specified days of each month, at the specified time.

By default, no days of month are selected; the default start time is 6:00:00 P.M.

- **When new updates are downloaded to the repository**

The task runs after updates are downloaded to the repository. For example, you may want to use this schedule for the find vulnerabilities and required updates task.

- **On virus outbreak**

The task runs after a *Virus outbreak* event occurs. Select application types that will monitor virus outbreaks. The following application types are available:

- Anti-virus for workstations and file servers
- Anti-virus for perimeter defense
- Anti-virus for mail systems

By default, all application types are selected.

You may want to run different tasks depending on the anti-virus application type that reports a virus outbreak. In this case, remove the selection of the application types that you do not need.

- **On completing another task**

The current task starts after another task completes. You can select how the previous task must complete (successfully or with error) to trigger the start of the current task. For example, you may want to run the Manage devices task with the **Turn on the device** option and, after it completes, run the Virus scan task.

- **Run missed tasks**

This option determines the behavior of a task if a client device is not visible on the network when the task is about to start.

If this option is enabled, the system attempts to start the task the next time the Kaspersky application is run on the client device. If the task schedule is **Manually**, **Once** or

Immediately, the task is started immediately after the device becomes visible on the network or immediately after the device is included in the task scope.

If this option is disabled, only scheduled tasks run on client devices; for **Manually**, **Once** and **Immediately**, tasks run only on those client devices that are visible on the network. For example, you may want to disable this option for a resource-consuming task that you want to run only outside of business hours.

By default, this option is enabled.

- **Use automatically randomized delay for task starts**

If this option is enabled, the task is started on client devices randomly within a specified time interval, that is, *distributed task start*. A distributed task start helps to avoid a large number of simultaneous requests by client devices to the Administration Server when a scheduled task is running.

The distributed start time is calculated automatically when a task is created, depending on the number of client devices to which the task is assigned. Later, the task is always started on the calculated start time. However when task settings are edited or the task is started manually, the calculated value of the task start time changes.

If this option is disabled, the task starts on client devices according to the schedule.

- **Use randomized delay for task starts within an interval of (min)**

If this option is enabled, the task is started on client devices randomly within the specified time interval. A distributed task start helps to avoid a large number of simultaneous requests by client devices to the Administration Server when a scheduled task is running.

If this option is disabled, the task starts on client devices according to the schedule.

By default, this option is disabled. The default time interval is one minute.

1. On the **Define the task name** page of the Wizard, specify the name for the task that you are creating. A task name cannot be more than 100 characters long and cannot include any special characters ("*<>?:\|)."
2. On the **Finish task creation** page of the Wizard, click the **Finish** button to close the Wizard.

If you want the task to start as soon as the Wizard finishes, select the **Run the task after the Wizard finishes** check box.

After the Wizard completes its operation, the Find vulnerabilities and required updates task appears in the list of tasks in the **Managed devices** folder, on the **Tasks** tab.

In addition to the settings that you specify during task creation, you can change other properties of a created task.

When the Find vulnerabilities and required updates task is complete, Administration Server displays a list of vulnerabilities found in applications installed on the device; it also displays all software updates required to fix the vulnerabilities detected.

If the task results contain the 0x80240033 "Windows Update Agent error 80240033 ("License terms could not be downloaded.")" error, you can resolve this issue through the Windows Registry (see section "Problems with tasks when using Administration Server as WSUS server" on page [886](#)).

Administration Server does not display the list of required software updates when you sequentially run two tasks—the Perform Windows Update synchronization task that has the **Download express installation files** option disabled, and then the Find vulnerabilities and required updates task. In order to view the list of required software updates, you must run the Find vulnerabilities and required updates task again.

Network Agent receives information about any available Windows updates and other Microsoft product updates from Windows Update or the Administration Server, if the Administration Server acts as the WSUS server. Information is transmitted when applications are started (if this is provided for by the policy) and at each routine run of the Find vulnerabilities and required updates task on client devices.

You can find the details of third-party software that can be updated through Kaspersky Security Center by visiting the Technical Support website, on the Kaspersky Security Center page, in the **Server Management** (<https://support.kaspersky.com/14758>) section.

See also:

Scenario: Deployment for cloud environment.....	821
Scenario: Finding and fixing vulnerabilities in third-party software	459
Scenario: Updating third-party software	1208

Fixing vulnerabilities in applications

If you have selected **Find and install required updates** on the **Update management settings** page of the Quick Start Wizard, the **Install required updates and fix vulnerabilities** task is created automatically. The task is displayed in the workspace of the **Managed devices** folder, on the **Tasks** tab.

Otherwise, you can do any of the following:

- Create a task for fixing vulnerabilities by installing available updates.
- Add a rule for fixing a vulnerability to an existing vulnerability fix task.

A user interaction may be required when you update a third-party application or fix a vulnerability in a third-party application on a managed device. For example, the user may be prompted to close the third-party application if it's currently open.

Fixing vulnerabilities by creating a vulnerability fix task

You can do any of the following:

- Create a task for fixing multiple vulnerabilities that meet certain rules.
- Select a vulnerability and create a task for fixing it and similar vulnerabilities.

► *To fix vulnerabilities that meet certain rules:*

1. In the console tree, select the **Managed devices** folder.
2. In the workspace, select the **Tasks** tab.

3. Click the **Create a task** button to run the New Task Wizard. Proceed through the Wizard by using the **Next** button.
4. On the **Select the task type** page of the Wizard, select **Install required updates and fix vulnerabilities**.
5. On the **Settings** page of the Wizard, specify the task settings as follows:
 - **Specify rules for installing updates**

These rules are applied to installation of updates on client devices. If rules are not specified, the task has nothing to perform. For information about operations with rules, refer to Rules for update installation (on page [482](#)).

- **Start installation at device restart or shutdown**

If this option is enabled, updates are installed when the device is restarted or shut down. Otherwise, updates are installed according to a schedule.

Use this option if installing the updates might affect the device performance.

By default, this option is disabled.

- **Install required general system components**

If this option is enabled, before installing an update the application automatically installs all general system components (prerequisites) that are required to install the update. For example, these prerequisites can be operating system updates

If this option is disabled, you may have to install the prerequisites manually.

By default, this option is disabled.

- **Allow installation of new application versions during updates**

If this option is enabled, updates are allowed when they result in installation of a new version of a software application.

If this option is disabled, the software is not upgraded. You can then install new versions of the software manually or through another task. For example, you may use this option if your company infrastructure is not supported by a new software version or if you want to check an upgrade in a test infrastructure.

By default, this option is enabled.

Upgrading an application may cause malfunction of dependent applications installed on client devices.

- **Download updates to the device without installing them**

If this option is enabled, the application downloads updates to the device but does not install them automatically. You can then Install downloaded updates manually.

Microsoft updates are downloaded to the system Windows storage. Updates of third-party applications (applications made by software vendors other than Kaspersky and Microsoft) are downloaded to the folder specified in the **Folder for downloading updates** field.

If this option is disabled, the updates are installed to the device automatically.

By default, this option is disabled.

- **Folder for downloading updates**

This folder is used to download updates of third-party applications (applications made by software vendors other than Kaspersky and Microsoft).

- **Enable advanced diagnostics**

If this feature is enabled, Network Agent writes traces even if tracing is disabled for Network Agent in Kaspersky Security Center Remote Diagnostics Utility. Traces are written to two files in turn; the total size of both files is determined by the **Maximum size, in MB, of advanced diagnostics files** value. When both files are full, Network Agent starts writing to them again. The files with traces are stored in the %WINDIR%\Temp folder. These files are accessible in the remote diagnostics utility (see section "Remote diagnostics of client devices. Kaspersky Security Center remote diagnostics utility" on page [651](#)), you can download or delete them there.

If this feature is disabled, Network Agent writes traces according to the settings in Kaspersky Security Center Remote Diagnostics Utility. No additional traces are written.

When creating a task, you do not have to enable advanced diagnostics. You may want to use this feature later if, for example, a task run fails on some of the devices and you want to collect additional information during another task run.

By default, the feature is disabled.

- **Maximum size, in MB, of advanced diagnostics files**

The default value is 100 MB, and available values are between 1 MB and 2 048 MB. You may be asked to change the default value by Kaspersky Technical Support specialists when information in the advanced diagnostics files sent by you is not enough to troubleshoot the problem.

1. On the **Selecting an operating system restart option** page of the Wizard, select the action to perform when the operating system on client devices must be restarted after the operation:

- **Do not restart the device**

Client devices are not restarted automatically after the operation. To complete the operation, you must restart a device (for example, manually or through a device management task). Information about the required restart is saved in the task results and in the device status. This option is suitable for tasks on servers and other devices where continuous operation is critical.

- **Restart the device**

Client devices are always restarted automatically if a restart is required for completion of the operation. This option is useful for tasks on devices that provide for regular pauses in their operation (shutdown or restart).

- **Prompt user for action**

The restart reminder is displayed on the screen of the client device, prompting the user to restart it manually. Some advanced settings can be defined for this option: text of the message for the user, the message display frequency, and the time interval after which a restart will be forced (without the user's confirmation). This option is most suitable for workstations where users must be able to select the most convenient time for a restart.

By default, this option is selected.

- **Repeat prompt every (min)**

If this option is enabled, the application prompts the user to restart the operating system with the specified frequency.

By default, this option is enabled. The default interval is 5 minutes. Available values are between 1 and 1 440 minutes.

If this option is disabled, the prompt is displayed only once.

- **Restart after (min)**

After prompting the user, the application forces restart of the operating system upon expiration of the specified time interval.

By default, this option is enabled. The default delay is 30 minutes. Available values are between 1 and 1 440 minutes.

- **Force closure of applications in blocked sessions**

Running applications may prevent a restart of the client device. For example, if a document is being edited in a word processing application and is not saved, the application does not allow the device to restart.

If this option is enabled, such applications on a locked device are forced to close before the device restart. As a result, users may lose their unsaved changes.

If this option is disabled, a locked device is not restarted. The task status on this device states that a device restart is required. Users have to manually close all applications running on locked devices and restart these devices.

By default, this option is disabled.

1. On the **Configure task schedule** page of the Wizard, you can create a schedule for task start. If necessary, specify the following settings:

- **Scheduled start:**

Select the schedule according to which the task runs, and configure the selected schedule.

- **Every N hours**

The task runs regularly, with the specified interval in hours, starting from the specified date and time.

By default, the task runs every six hours, starting from the current system date and time.

- **Every N days**

The task runs regularly, with the specified interval in days. Additionally, you can specify a date and time of the first task run. These additional options become available, if they are supported by the application for which you create the task.

By default, the task runs every day, starting from the current system date and time.

- **Every N weeks**

The task runs regularly, with the specified interval in weeks, on the specified day of week and at the specified time.

By default, the task runs every Monday at the current system time.

- **Every N minutes**

The task runs regularly, with the specified interval in minutes, starting from the specified time on the day that the task is created.

By default, the task runs every 30 minutes, starting from the current system time.

- **Daily (daylight saving time is not supported)**

The task runs regularly, with the specified interval in days. This schedule does not support observance of daylight saving time (DST). It means that when clocks jump one hour forward or backward at the beginning or ending of DST, the actual task start time does not change.

We do not recommend that you use this schedule. It is needed for backward compatibility of Kaspersky Security Center.

By default, the task starts every day at the current system time.

- **Weekly**

The task runs every week on the specified day and at the specified time.
- **By days of week**

The task runs regularly, on the specified days of week, at the specified time.
By default, the task runs every Friday at 6:00:00 P.M.
- **Monthly**

The task runs regularly, on the specified day of the month, at the specified time.
In months that lack the specified day, the task runs on the last day.
By default, the task runs on the first day of each month, at the current system time.
- **Manually** (selected by default)

The task does not run automatically. You can only start it manually.
- **Every month on specified days of selected weeks**

The task runs regularly, on the specified days of each month, at the specified time.
By default, no days of month are selected; the default start time is 6:00:00 P.M.
- **On virus outbreak**

The task runs after a *Virus outbreak* event occurs. Select application types that will monitor virus outbreaks. The following application types are available:

 - Anti-virus for workstations and file servers
 - Anti-virus for perimeter defense
 - Anti-virus for mail systems

By default, all application types are selected.

You may want to run different tasks depending on the anti-virus application type that reports a virus outbreak. In this case, remove the selection of the application types that you do not need.
- **On completing another task**

The current task starts after another task completes. You can select how the previous task must complete (successfully or with error) to trigger the start of the current task. For example, you may want to run the Manage devices task with the **Turn on the device** option and, after it completes, run the Virus scan task.
- **Run missed tasks**

This option determines the behavior of a task if a client device is not visible on the network when the task is about to start.

If this option is enabled, the system attempts to start the task the next time the Kaspersky

application is run on the client device. If the task schedule is **Manually**, **Once** or **Immediately**, the task is started immediately after the device becomes visible on the network or immediately after the device is included in the task scope.

If this option is disabled, only scheduled tasks run on client devices; for **Manually**, **Once** and **Immediately**, tasks run only on those client devices that are visible on the network. For example, you may want to disable this option for a resource-consuming task that you want to run only outside of business hours.

By default, this option is enabled.

- **Use automatically randomized delay for task starts**

If this option is enabled, the task is started on client devices randomly within a specified time interval, that is, *distributed task start*. A distributed task start helps to avoid a large number of simultaneous requests by client devices to the Administration Server when a scheduled task is running.

The distributed start time is calculated automatically when a task is created, depending on the number of client devices to which the task is assigned. Later, the task is always started on the calculated start time. However when task settings are edited or the task is started manually, the calculated value of the task start time changes.

If this option is disabled, the task starts on client devices according to the schedule.

- **Use randomized delay for task starts within an interval of (min)**

If this option is enabled, the task is started on client devices randomly within the specified time interval. A distributed task start helps to avoid a large number of simultaneous requests by client devices to the Administration Server when a scheduled task is running.

If this option is disabled, the task starts on client devices according to the schedule.

By default, this option is disabled. The default time interval is one minute.

1. On the **Define the task name** page of the Wizard, specify the name for the task that you are creating. A task name cannot be more than 100 characters long and cannot include any special characters ("*<>?:\:").
2. On the **Finish task creation** page of the Wizard, click the **Finish** button to close the Wizard.

If you want the task to start as soon as the Wizard finishes, select the **Run the task after the Wizard finishes** check box.

After the Wizard completes its operation, the **Install required updates and fix vulnerabilities** task is created and displayed in the **Tasks** folder.

In addition to the settings that you specify during task creation, you can change other properties of a created task.

If the task results contain the 0x80240033 "Windows Update Agent error 80240033 ("License terms could not be downloaded.")" error, you can resolve this issue through the Windows Registry (see section "Problems with tasks when using Administration Server as WSUS server" on page [886](#)).

► *To fix a specific vulnerability and similar ones:*

1. In the **Advanced** → **Application management** folder in the console tree, select the **Software vulnerabilities** subfolder.
2. Select the vulnerability that you want to fix.

3. Click the **Run Vulnerability Fix Wizard** button.

The Vulnerability Fix Wizard starts.

The Vulnerability Fix Wizard features are only available under the Vulnerability and Patch Management license.

Proceed through the Wizard by using the **Next** button.

4. In the **Search for existing vulnerability fix tasks** window, specify the following parameters:

- **Show only tasks that fix this vulnerability**

If this option is enabled, the Vulnerability Fix Wizard searches for existing tasks that fix the selected vulnerability.

If this option is disabled or if the search yields no applicable tasks, the Vulnerability Fix Wizard prompts you to create a rule or task for fixing the vulnerability.

By default, this option is enabled.

- **Approve updates that fix this vulnerability**

Updates that fix a vulnerability will be approved for installation. Enable this option if some applied rules of update installation only allow the installation of approved updates.

By default, this option is disabled.

1. If you choose to search for existing vulnerability fix tasks and if the search retrieves some tasks, you can view properties of these tasks or start them manually. No further actions are required.

Otherwise, click the **New vulnerability fix task** button.

2. Select the type of the vulnerability fix rule to be added to the new task, and then click the **Finish** button.
3. Make your choice in the displayed prompt about installing all previous application updates. Click **Yes** if you agree to the installation of successive application versions incrementally if this is required for installing the selected updates. Click **No** if you want to update applications in a straightforward fashion, without installing successive versions. If installing the selected updates is not possible without installing previous versions of applications, the updating of the application fails.

The Updates Installation and Vulnerabilities Fix Task Creation Wizard starts. Proceed through the Wizard by using the **Next** button.

4. On the **Selecting an operating system restart option** page of the Wizard, select the action to perform when the operating system on client devices must be restarted after the operation:

- **Do not restart the device**

Client devices are not restarted automatically after the operation. To complete the operation, you must restart a device (for example, manually or through a device management task). Information about the required restart is saved in the task results and in the device status. This option is suitable for tasks on servers and other devices where continuous operation is critical.

- **Restart the device**

Client devices are always restarted automatically if a restart is required for completion of the operation. This option is useful for tasks on devices that provide for regular pauses in their operation (shutdown or restart).

- **Prompt user for action**

The restart reminder is displayed on the screen of the client device, prompting the user to restart it manually. Some advanced settings can be defined for this option: text of the message for the user, the message display frequency, and the time interval after which a restart will be forced (without the user's confirmation). This option is most suitable for workstations where users must be able to select the most convenient time for a restart.

By default, this option is selected.

- **Repeat prompt every (min)**

If this option is enabled, the application prompts the user to restart the operating system with the specified frequency.

By default, this option is enabled. The default interval is 5 minutes. Available values are between 1 and 1 440 minutes.

If this option is disabled, the prompt is displayed only once.

- **Restart after (min)**

After prompting the user, the application forces restart of the operating system upon expiration of the specified time interval.

By default, this option is enabled. The default delay is 30 minutes. Available values are between 1 and 1 440 minutes.

- **Force closure of applications in blocked sessions**

Running applications may prevent a restart of the client device. For example, if a document is being edited in a word processing application and is not saved, the application does not allow the device to restart.

If this option is enabled, such applications on a locked device are forced to close before the device restart. As a result, users may lose their unsaved changes.

If this option is disabled, a locked device is not restarted. The task status on this device states that a device restart is required. Users have to manually close all applications running on locked devices and restart these devices.

By default, this option is disabled.

1. On the **Select devices to which the task will be assigned** page of the Wizard, select one of the following options:

- **Select networked devices detected by Administration Server**

The task is assigned to specific devices. The specific devices can include devices in administration groups as well as unassigned devices.

For example, you may want to use this option in a task of installing Network Agent on unassigned devices.

- **Specify device addresses manually or import addresses from a list**

You can specify NetBIOS names, DNS names, IP addresses, and IP subnets of devices to which you want to assign the task.

You may want to use this option to execute a task for a specific subnet. For example, you may want to install a certain application on devices of accountants or to scan devices in a subnet that is probably infected.

- **Assign task to a device selection**

The task is assigned to devices included in a device selection. You can specify one of the existing selections.

For example, you may want to use this option to run a task on devices with a specific operating system version.

- **Assign task to an administration group**

The task is assigned to devices included in an administration group. You can specify one of the existing groups or create a new one.

For example, you may want to use this option to run a task of sending a message to users if the message is specific for devices included in a specific administration group.

2. On the **Configure task schedule** page of the Wizard, you can create a schedule for task start. If necessary, specify the following settings:

- **Scheduled start:**

Select the schedule according to which the task runs, and configure the selected schedule.

- **Every N hours**

The task runs regularly, with the specified interval in hours, starting from the specified date and time.

By default, the task runs every six hours, starting from the current system date and time.

- **Every N days**

The task runs regularly, with the specified interval in days. Additionally, you can specify a date and time of the first task run. These additional options become available, if they are supported by the application for which you create the task.

By default, the task runs every day, starting from the current system date and time.

- **Every N weeks**

The task runs regularly, with the specified interval in weeks, on the specified day of week and at the specified time.

By default, the task runs every Monday at the current system time.

- **Every N minutes**

The task runs regularly, with the specified interval in minutes, starting from the specified time on the day that the task is created.

By default, the task runs every 30 minutes, starting from the current system time.

- **Daily (daylight saving time is not supported)**

The task runs regularly, with the specified interval in days. This schedule does not support observance of daylight saving time (DST). It means that when clocks jump one hour forward or backward at the beginning or ending of DST, the actual task start time does not change.

We do not recommend that you use this schedule. It is needed for backward compatibility of Kaspersky Security Center.

By default, the task starts every day at the current system time.

- **Weekly**

The task runs every week on the specified day and at the specified time.

- **By days of week**

The task runs regularly, on the specified days of week, at the specified time.

By default, the task runs every Friday at 6:00:00 P.M.
- **Monthly**

The task runs regularly, on the specified day of the month, at the specified time.

In months that lack the specified day, the task runs on the last day.

By default, the task runs on the first day of each month, at the current system time.
- **Manually** (selected by default)

The task does not run automatically. You can only start it manually.
- **Every month on specified days of selected weeks**

The task runs regularly, on the specified days of each month, at the specified time.

By default, no days of month are selected; the default start time is 6:00:00 P.M.
- **On virus outbreak**

The task runs after a *Virus outbreak* event occurs. Select application types that will monitor virus outbreaks. The following application types are available:

 - Anti-virus for workstations and file servers
 - Anti-virus for perimeter defense
 - Anti-virus for mail systems

By default, all application types are selected.

You may want to run different tasks depending on the anti-virus application type that reports a virus outbreak. In this case, remove the selection of the application types that you do not need.
- **On completing another task**

The current task starts after another task completes. You can select how the previous task must complete (successfully or with error) to trigger the start of the current task. For example, you may want to run the Manage devices task with the **Turn on the device** option and, after it completes, run the Virus scan task.
- **Run missed tasks**

This option determines the behavior of a task if a client device is not visible on the network when the task is about to start.

If this option is enabled, the system attempts to start the task the next time the Kaspersky application is run on the client device. If the task schedule is **Manually**, **Once** or **Immediately**, the task is started immediately after the device becomes visible on the network or immediately after the device is included in the task scope.

If this option is disabled, only scheduled tasks run on client devices; for **Manually**, **Once** and **Immediately**, tasks run only on those client devices that are visible on the network. For example, you may want to disable this option for a resource-consuming task that you want to run only outside of business hours.

By default, this option is enabled.
- **Use automatically randomized delay for task starts**

If this option is enabled, the task is started on client devices randomly within a specified

time interval, that is, *distributed task start*. A distributed task start helps to avoid a large number of simultaneous requests by client devices to the Administration Server when a scheduled task is running.

The distributed start time is calculated automatically when a task is created, depending on the number of client devices to which the task is assigned. Later, the task is always started on the calculated start time. However when task settings are edited or the task is started manually, the calculated value of the task start time changes.

If this option is disabled, the task starts on client devices according to the schedule.

- **Use randomized delay for task starts within an interval of (min)**

If this option is enabled, the task is started on client devices randomly within the specified time interval. A distributed task start helps to avoid a large number of simultaneous requests by client devices to the Administration Server when a scheduled task is running.

If this option is disabled, the task starts on client devices according to the schedule.

By default, this option is disabled. The default time interval is one minute.

1. On the **Define the task name** page of the Wizard, specify the name for the task that you are creating. A task name cannot be more than 100 characters long and cannot include any special characters ("*<>?\":|).
2. On the **Finish task creation** page of the Wizard, click the **Finish** button to close the Wizard.

If you want the task to start as soon as the Wizard finishes, select the **Run the task after the Wizard finishes** check box.

When the Wizard completes, the **Install required updates and fix vulnerabilities** task is created and displayed in the **Tasks** folder.

In addition to the settings that you specify during task creation, you can change other properties of a created task.

Fixing a vulnerability by adding a rule to an existing vulnerability fix task

► *To fix a vulnerability by adding a rule to an existing vulnerability fix task:*

1. In the **Advanced** → **Application management** folder in the console tree, select the **Software vulnerabilities** subfolder.
2. Select the vulnerability that you want to fix.
3. Click the **Run Vulnerability Fix Wizard** button.

The Vulnerability Fix Wizard starts.

The Vulnerability Fix Wizard features are only available under the Vulnerability and Patch Management license.

Proceed through the Wizard by using the **Next** button.

4. In the **Search for existing vulnerability fix tasks** window, specify the following parameters:
 - **Show only tasks that fix this vulnerability**

If this option is enabled, the Vulnerability Fix Wizard searches for existing tasks that fix the selected vulnerability.

If this option is disabled or if the search yields no applicable tasks, the Vulnerability Fix Wizard prompts you to create a rule or task for fixing the vulnerability.

By default, this option is enabled.

- **Approve updates that fix this vulnerability**

Updates that fix a vulnerability will be approved for installation. Enable this option if some applied rules of update installation only allow the installation of approved updates.

By default, this option is disabled.

1. If you choose to search for existing vulnerability fix tasks and if the search retrieves some tasks, you can view properties of these tasks or start them manually. No further actions are required.
Otherwise, click the **Add vulnerability fix rule to existing task** button.
2. Select the task to which you want to add a rule, and then click the **Add rule** button.
Also, you can view properties of the existing tasks, start them manually, or create a new task.
3. Select the type of rule to be added to the selected task, and then click the **Finish** button.
4. Make your choice in the displayed prompt about installing all previous application updates. Click **Yes** if you agree to the installation of successive application versions incrementally if this is required for installing the selected updates. Click **No** if you want to update applications in a straightforward fashion, without installing successive versions. If installing the selected updates is not possible without installing previous versions of applications, the updating of the application fails.

A new rule for fixing the vulnerability is added to the existing **Install required updates and fix vulnerabilities** task.

See also:

Scenario: Updating third-party software..... [1208](#)

Ignoring software vulnerabilities

You can ignore software vulnerabilities to be fixed. The reasons to ignore software vulnerabilities might be, for example, the following:

- You do not consider the software vulnerability critical to your organization.
- You understand that the software vulnerability fix can damage data related to the software that required the vulnerability fix.
- You are sure that the software vulnerability is not dangerous for your organization's network because you use other measures to protect your managed devices.

You can ignore a software vulnerability on all managed devices or only on selected managed devices.

► *To ignore a software vulnerability on all managed devices:*

1. In the **Advanced** → **Application management** folder in the console tree, select the **Software vulnerabilities** subfolder.

The workspace of the folder displays the list of vulnerabilities in applications detected on devices by the Network Agent installed on them.

2. Select the vulnerability you want to ignore.
3. Select **Properties** from the context menu of the vulnerability.

The vulnerability properties window opens.

4. On the **General** section, select the **Ignore vulnerability** option.
5. Click **OK**.

The software vulnerability properties window is closed.

The software vulnerability is ignored on all managed devices.

► *To ignore a software vulnerability on the selected managed device:*

1. Open the properties window of the selected managed device (see section "Settings of a managed device" on page [658](#)) and select the **Software vulnerabilities** section.
2. Select a software vulnerability.
3. Ignore selected vulnerability.

The software vulnerability is ignored on the selected device.

The ignored software vulnerability will not be fixed after completion of the *Fix vulnerabilities* task or *Install required updates and fix vulnerabilities* task. You can exclude ignored software vulnerabilities from the list of vulnerabilities by means of the filter.

Selecting user fixes for vulnerabilities in third-party software

To use the *Fix vulnerabilities* task, you must manually specify the software updates to fix the vulnerabilities in third-party software listed in the task settings. The *Fix vulnerabilities* task uses recommended fixes for Microsoft software and user fixes for other third-party software. *User fixes* are software updates to fix vulnerabilities that the administrator manually specifies for installation.

► *To select user fixes for vulnerabilities in third-party software:*

1. In the **Advanced** → **Application management** folder in the console tree, select the **Software vulnerabilities** subfolder.

The workspace of the folder displays a list of vulnerabilities in applications detected on devices by the Network Agent installed on them.

2. Select the vulnerability for which you want to specify a user fix.
3. Select **Properties** from the context menu of the vulnerability.

The vulnerability properties window opens.

4. In the **User fixes and other fixes** section, click the **Add** button.

The list of available installation packages is displayed. The list of displayed installation packages corresponds to the **Remote installation** → **Installation packages** list. If you have not created an installation package containing a user fix for selected vulnerability, you can create the package now by starting the New Package Wizard.

5. Select an installation package (or packages) containing a user fix (or user fixes) for the vulnerability in third-party software.
6. Click **OK**.

The installation packages containing user fixes for the software vulnerability are specified. When the *Fix vulnerabilities* task is started, the installation package will be installed, and the software vulnerability will be fixed.

See also:

About finding and fixing software vulnerabilities [462](#)

Rules for update installation

When fixing vulnerabilities in applications (on page [469](#)), you must specify rules for update installation. These rules determine updates to install and vulnerabilities to fix.

The exact settings depend on whether you create a rule for updates of Microsoft applications, of third-party applications (applications made by software vendors other than Kaspersky and Microsoft), or of all applications. When creating a rule for Microsoft applications or third-party applications, you can select specific applications and application versions for which you want to install updates. When creating a rule for all applications, you can select specific updates that you want to install and vulnerabilities that you want to fix by means of installing updates.

► To create a new rule for updates of all applications:

1. On the **Settings** page of the New Task Wizard, click the **Add** button.

The Rule Creation Wizard starts. Proceed through the Wizard by using the **Next** button.

2. On the **Rule type** page, select **Rule for all updates**.

3. On the **General criteria** page, use the drop-down lists to specify the following settings:

- **Set of updates to install**

Select the updates that must be installed on client devices:

- **Install approved updates only.** This installs only approved updates.
- **Install all updates (except declined).** This installs updates with the *Approved* or *Undefined* approval status.
- **Install all updates (including declined).** This installs all updates, regardless of their approval status. Select this option with caution. For example, use this option if you want to check installation of some declined updates in a test infrastructure.

- **Fix vulnerabilities with a severity level equal to or higher than**

Sometimes software updates may impair the user experience with the software. In such cases, you may decide to install only those updates that are critical for the software operation and to skip other updates.

If this option is enabled, the updates fix only those vulnerabilities for which the severity level set by Kaspersky is equal to or higher than the value selected in the list (**Medium**, **High**, or **Critical**). Vulnerabilities with a severity level lower than the selected value are not fixed.

If this option is disabled, the updates fix all vulnerabilities regardless of their severity level.

By default, this option is disabled.

1. On the **Updates** page, select the updates to be installed:

- **Install all suitable updates**

Install all software updates that meet the criteria specified on the **General criteria** page of the Wizard. Selected by default.

- **Install only updates from the list**

Install only software updates that you select manually from the list. This list contains all available software updates.

For example, you may want to select specific updates in the following cases: to check their installation in a test environment, to update only critical applications, or to update only specific applications.

- **Automatically install all previous application updates that are required to install the selected updates**

Keep this option enabled if you agree with the installation of interim application versions when this is required for installing the selected updates.

If this option is disabled, only the selected versions of applications are installed. Disable this option if you want to update applications in a straightforward manner, without attempting to install successive versions incrementally. If installing the selected updates is not possible without installing previous versions of applications, the updating of the application fails.

For example, you have version 3 of an application installed on a device and you want to update it to version 5, but version 5 of this application can be installed only over version 4. If this option is enabled, the software first installs version 4, and then installs version 5. If this option is disabled, the software fails to update the application.

By default, this option is enabled.

1. On the **Vulnerabilities** page, select vulnerabilities that will be fixed by installing the selected updates:

- **Fix all vulnerabilities that match other criteria**

Fix all vulnerabilities that meet the criteria specified on the **General criteria** page of the Wizard. Selected by default.

- **Fix only vulnerabilities from the list**

Fix only vulnerabilities that you select manually from the list. This list contains all detected vulnerabilities.

For example, you may want to select specific vulnerabilities in the following cases: to check their fix in a test environment, to fix vulnerabilities only in critical applications, or to fix vulnerabilities only in specific applications.

1. On the **Name** page, specify the name for the rule that you are creating. You can later change this name in the **Settings** section of the properties window of the created task.

After the Rule Creation Wizard completes its operation, the new rule is created and displayed in the **Specify rules for installing updates** field of the New Task Wizard.

► To create a new rule for updates of Microsoft applications:

1. On the **Settings** page of the New Task Wizard, click the **Add** button.

The Rule Creation Wizard starts. Proceed through the Wizard by using the **Next** button.

2. On the **Rule type** page, select **Rule for Windows Update**.
3. On the **General criteria** page, specify the following settings:

- Set of updates to install

Select the updates that must be installed on client devices:

- **Install approved updates only**. This installs only approved updates.
- **Install all updates (except declined)**. This installs updates with the *Approved* or *Undefined* approval status.
- **Install all updates (including declined)**. This installs all updates, regardless of their

approval status. Select this option with caution. For example, use this option if you want to check installation of some declined updates in a test infrastructure.

- **Fix vulnerabilities with a severity level equal to or higher than**

Sometimes software updates may impair the user experience with the software. In such cases, you may decide to install only those updates that are critical for the software operation and to skip other updates.

If this option is enabled, the updates fix only those vulnerabilities for which the severity level set by Kaspersky is equal to or higher than the value selected in the list (**Medium**, **High**, or **Critical**). Vulnerabilities with a severity level lower than the selected value are not fixed.

If this option is disabled, the updates fix all vulnerabilities regardless of their severity level.

By default, this option is disabled.

- **Fix vulnerabilities with an MSRC severity level equal to or higher than**

Sometimes, software updates may impair the user experience with the software. In such cases, you may decide to install only those updates that are critical for the software operation and to skip other updates.

If this option is enabled, the updates fix only those vulnerabilities for which the severity level set by Microsoft Security Response Center (MSRC) is equal to or higher than the value selected in the list (**Low**, **Medium**, **High**, or **Critical**). Vulnerabilities with a severity level lower than the selected value are not fixed.

If this option is disabled, the updates fix all vulnerabilities regardless of their severity level.

By default, this option is disabled.

1. On the **Applications** page, select the applications and application versions for which you want to install updates. By default, all applications are selected.
2. On the **Categories of updates** page, select the categories of updates to be installed. These categories are the same as in Microsoft Update Catalog. By default, all categories are selected.
3. On the **Name** page, specify the name for the rule that you are creating. You can later change this name in the **Settings** section of the properties window of the created task.

After the Wizard completes its operation, the new rule is created and displayed in the **Specify rules for installing updates** field of the New Task Wizard.

► To create a new rule for updates of third-party applications:

1. On the **Settings** page of the New Task Wizard, click the **Add** button.

The Rule Creation Wizard starts. Proceed through the Wizard by using the **Next** button.

2. On the **Rule type** page, select **Rule for third-party updates**.
3. On the **General criteria** page, specify the following settings:
 - Set of updates to install

Select the updates that must be installed on client devices:

- **Install approved updates only**. This installs only approved updates.
- **Install all updates (except declined)**. This installs updates with the *Approved* or *Undefined* approval status.
- **Install all updates (including declined)**. This installs all updates, regardless of their

approval status. Select this option with caution. For example, use this option if you want to check installation of some declined updates in a test infrastructure.

- **Fix vulnerabilities with a severity level equal to or higher than**

Sometimes software updates may impair the user experience with the software. In such cases, you may decide to install only those updates that are critical for the software operation and to skip other updates.

If this option is enabled, the updates fix only those vulnerabilities for which the severity level set by Kaspersky is equal to or higher than the value selected in the list (**Medium**, **High**, or **Critical**). Vulnerabilities with a severity level lower than the selected value are not fixed.

If this option is disabled, the updates fix all vulnerabilities regardless of their severity level.

By default, this option is disabled.

1. On the **Applications** page, select the applications and application versions for which you want to install updates. By default, all applications are selected.
2. On the **Name** page, specify the name for the rule that you are creating. You can later change this name in the **Settings** section of the properties window of the created task.

After the Wizard completes its operation, the new rule is created and displayed in the **Specify rules for installing updates** field of the New Task Wizard.

See also:

| Approving and declining software updates [435](#)

Groups of applications

This section describes how to manage groups of applications installed on devices.

Creating application categories

Kaspersky Security Center allows you to create categories of applications installed on devices.

Application categories can be created in one of the following ways:

- The administrator specifies a folder in which executable files have been included in the selected category.
- The administrator specifies a device from which executable files are to be included in the selected category.
- The administrator sets criteria to be used to include applications in the selected category.

When an application category is created, the administrator can set rules for the application category. Rules define the behavior of applications included in the specified category. For example, you can block or allow startup of applications included in the category.

Managing applications run on devices

Kaspersky Security Center allows you to manage startup of applications on devices in Allowlist mode. For detailed description see Kaspersky Endpoint Security for Windows Online Help <https://support.kaspersky.com/KESWin/11.6.0/en-US/127971.htm>. While in Allowlist mode, on selected devices you

can only start applications included in the specified categories. The administrator can view results of static analysis applied to rules of applications run on devices for each user.

Inventory of software installed on devices

Kaspersky Security Center allows you to perform inventory of software on devices running Windows. Network Agent retrieves information about all applications installed on devices. Information retrieved during inventory is displayed in the workspace of the **Applications registry** folder. The administrator can view detailed information about any application, including its version and manufacturer.

The number of executable files received from a single device cannot exceed 150 000. Having reached this limit, Kaspersky Security Center cannot receive any new files.

Licensed applications group management

Kaspersky Security Center allows you to create licensed applications groups. A licensed applications group includes applications that meet criteria set by the administrator. The administrator can specify the following criteria for licensed applications groups:

- Application name
- Application version
- Manufacturer
- Application tag

Applications that meet one or several criteria are automatically included in a group. To create a licensed applications group, you must set at least one criterion for including applications in this group.

Each licensed applications group has its own license key. The license key of a licensed applications group defines the maximum allowed number of installations for applications included in this group. If the number of installations has exceeded the limit set by the license key, an informational event is logged on Administration Server. The administrator can specify an expiration date for the license key. When this date arrives, an informational event is logged on Administration Server.

Viewing information about executable files

Kaspersky Security Center retrieves all information about executable files that have been run on devices since the operating system was installed on them. Information about executable files is displayed in the main application window, in the workspace of the **Executable files** folder.

In this section

Creating application categories for Kaspersky Endpoint Security for Windows policies.....	487
Creating an application category with content added manually	489
Creating an application category with content added automatically	491
Adding event-related executable files to the application category	493
Configuring application startup management on client devices	494
Viewing the results of static analysis of startup rules applied to executable files	495
Viewing the applications registry	496
Changing the software inventory start time	497
About license key management of third-party applications	498
Creating licensed applications groups.....	499
Managing license keys for licensed applications groups.....	499
Inventory of executable files	500
Viewing information about executable files	501

Creating application categories for Kaspersky Endpoint Security for Windows policies

You can create application categories for Kaspersky Endpoint Security for Windows policies from the **Application categories** folder and from the **Properties** window of a Kaspersky Endpoint Security for Windows policy.

► *To create an application category for a Kaspersky Endpoint Security policy from the **Application categories** folder:*

1. In the console tree, select **Advanced** → **Application management** → **Application categories**.
2. In the workspace of the **Application categories** folder, click the **New category** button.
The New Category Wizard starts.
3. On the **Category type** page, select the type of user category:
 - **Category with content added manually.** Specify the criteria that will be used to assign executable files to the category that is being created.
 - **Category with content added automatically.** Specify the folder from which executable files will be automatically assigned to the created category.

When you create a category with content added automatically, the application inventories the following file types: EXE, COM, DLL, SYS, BAT, PS1, CMD, JS, VBS, REG, MSI, MSC, CPL, HTML, HTM, DRV, OCX, and SCR.

- **Category, which includes executable files from the selected devices.** Specify a device whose executable files must be automatically assigned to the category.
4. Follow the instructions of the Wizard.

When the Wizard finishes, a custom application category is created. You can view newly created categories by using the list of categories in the workspace of the **Application categories** folder.

You can also create an application category from the **Policies** folder.

► *To create an application category from the **Properties** window of a Kaspersky Endpoint Security for Windows policy:*

1. In the console tree, select the **Policies** folder.
2. In the workspace of the **Policies** folder, select a Kaspersky Endpoint Security policy for which you want to create a category.
3. Right-click and select **Properties**.
4. In the **Properties** window that opens, in the left **Sections** pane select **Security Controls** → **Application control**.
5. In the **Application control** section, in the **Control mode** and **Action** drop-down lists make selections for the Allowlist or Denylist, and then click the **Add** button.

The **Application Control rule** window containing a list of categories opens.

6. Click the **Create new** button.
7. Enter the name of the new category and click **OK**.

The New Category Wizard starts.

8. On the **Category type** page, select the type of user category:
 - **Category with content added manually.** Specify the criteria that will be used to assign executable files to the category that is being created.
 - **Category with content added automatically.** Specify the folder from which executable files will be automatically assigned to the created category.

When you create a category with content added automatically, the application inventories the following file types: EXE, COM, DLL, SYS, BAT, PS1, CMD, JS, VBS, REG, MSI, MSC, CPL, HTML, HTM, DRV, OCX, and SCR.

- **Category, which includes executable files from the selected devices.** Specify a device whose executable files must be automatically assigned to the category.
9. Follow the instructions of the Wizard.

When the Wizard finishes, a custom application category is created. You can view newly created categories in the list of categories.

Application categories are used by the Application Control component included in Kaspersky Endpoint Security for Windows. Application Control allows the administrator to impose restrictions on the startup of applications on client devices—for example, restricting the startups to applications in a specified category.

See also:

Creating an application category with content added automatically	491
Creating an application category with content added manually	489
Scenario: Application Management.....	1258

Creating an application category with content added manually

► *To create an application category with content added manually:*

1. In the console tree, in the **Advanced** → **Application management** folder select the **Application categories** subfolder.
2. Click the **New category** button.
The New Category Wizard starts.
3. On the Wizard page, select **Category with content added manually** as the user category type.
4. On the **Configuring conditions for inclusion of applications in categories** page, click the **Add** button.
5. In the drop-down list, specify the relevant settings:
 - **From the list of executable files**
If this option is selected, you can use the list of executable files on the client device to select and add applications to the category.
 - **From file properties**
If this option is selected, you can specify the detailed data for the executable files that will be added to the user application category.
 - **Metadata from files in folder**
Specify a folder on the client device that contains executable files. The metadata in the executable files that are included in the specified folder will be sent to Administration Server. Executable files that contain the same metadata will be added to the user application category.
 - **Checksums of the files in the folder**
If this option is selected, you can select or create a folder on the client device. The MD5 hash of the files in a specified folder will be sent to Administration Server. The applications that have the same hash as the files in the specified folder are added to the user application category.
 - **Certificates for the files from the folder**
If this option is selected, you can specify the folder on the client device, which contains executable files signed with certificates. Certificates of executable files are read and added to the category's conditions. Executable files that have been signed in accordance with the specified certificates will be added to the user category.
 - **MSI installer files metadata**
If this option is selected, you can specify an MSI installer file as the condition of adding

applications to the user category. The application installer metadata will be sent to Administration Server. The applications for which the installer metadata is the same as for the specified MSI installer are added to the user application category.

- **Checksums of the files from the MSI installer of the application**

If this option is selected, you can specify an MSI installer file as the condition of adding applications to the user category. The hash of the application installer files will be sent to Administration Server. The applications for which the hash of MSI installer files is identical to the specified hash are added to the user application category.

- **From KL category**

If this option is selected, you can specify a Kaspersky application category as the condition of adding applications to the user category. The applications from the specified Kaspersky category will be added to the user application category.

- **Application folder**

If this option is selected, you can specify the path to the folder on the client device containing the executable files that are to be added to the user application category.

- **Select certificate from repository**

If this option is selected, you can specify certificates from the storage. Executable files that have been signed in accordance with the specified certificates will be added to the user category.

- **Drive type**

If this option is selected, you can specify the type of the medium (any drive or removable drive) on which the application is run. Applications that have been run on the selected drive type are added to the user application category.

6. Follow the instructions of the Wizard.

Kaspersky Security Center only handles metadata from digitally signed files. No category can be created on the basis of metadata from files that do not contain a digital signature.

When the Wizard has completed, a user application category is created, with content added manually. You can view the newly created category using the list of categories in the workspace of the **Application categories** folder.

See also:

Scenario: Application Management [1258](#)

Creating an application category with content added automatically

► *To create an application category with content added automatically:*

1. In the console tree, in the **Advanced** → **Application management** folder select the **Application categories** subfolder.
2. Click the **New category** button to start the New Category Wizard.
In the Wizard window, select **Category with content added automatically** as the user category type.
3. In the **Repository folder** window, specify the relevant settings:

- **Path to folder for automatic category content addition**

In this field, specify the path to the folder in which Administration Server will regularly search for executable files. The path to this folder is specified when the category is created. The path to this folder cannot be changed.

- **Include dynamic-link libraries (DLL) in this category**

The application category includes dynamic-link libraries (files in DLL format), and the Application Control component logs the actions of such libraries running in the system. Including DLL files in the category may lower the performance of Kaspersky Security Center.

By default, this check box is cleared.

- **Include script data in this category**

The application category includes data on scripts, and scripts are not blocked by Web Threat Protection. Including the script data in the category may lower the performance of Kaspersky Security Center.

By default, this check box is cleared.

- **Hash value computing algorithm**

Depending on the version of the security application installed on devices on your network, you must select an algorithm for hash value computing by Kaspersky Security Center for files in this category. Information about computed hash values is stored in the Administration Server database. Storage of hash values does not increase the database size significantly.

SHA-256 is a cryptographic hash function: no vulnerabilities have been found in its algorithm, and so it is considered the most reliable cryptographic function nowadays. Kaspersky Endpoint Security 10 Service Pack 2 for Windows and later versions support SHA-256 computing. Computing of the MD5 hash function is supported by all versions earlier than Kaspersky Endpoint Security 10 Service Pack 2 for Windows.

Select either of the options of hash value computing by Kaspersky Security Center for files in the category:

- If all instances of security applications installed on your network are Kaspersky Endpoint Security 10 Service Pack 2 for Windows or later versions, select the **Calculate SHA-256 for files in this category (supported by Kaspersky Endpoint Security 10 Service Pack 2 for Windows and any later versions)** check box. We do not recommend that you add any categories created according to the criterion of the SHA-256 hash of an executable file for versions earlier than Kaspersky Endpoint Security 10 Service Pack 2 for Windows. This may result in failures in the security application operation. In this case, you can use the MD5 cryptographic hash function

for files of the category.

- If any versions earlier than Kaspersky Endpoint Security 10 Service Pack 2 for Windows are installed on your network, select the **Calculate MD5 for files in this category (supported by versions earlier than Kaspersky Endpoint Security 10 Service Pack 2 for Windows)**. You cannot add a category that was created based on the criterion of the MD5 hash sum of an executable file for Kaspersky Endpoint Security 10 Service Pack 2 for Windows or later versions. In this case, you can use the SHA-256 cryptographic hash function for files of the category.

If different devices on your network use both earlier and later versions of Kaspersky Endpoint Security 10, select both the **Calculate SHA-256 for files in this category** check box and the **Calculate MD5 for files in this category** check box.

The **Calculate SHA-256 for files in this category (supported by Kaspersky Endpoint Security 10 Service Pack 2 for Windows and any later versions)** check box is selected by default.

The **Calculate MD5 for files in this category (supported by versions earlier than Kaspersky Endpoint Security 10 Service Pack 2 for Windows)** is cleared by default.

- **Force folder scan for changes**

If this check box is selected, the application regularly checks the folder of category content addition for changes. You can specify the frequency of checks (in hours) in the entry field next to the check box. By default, the time interval between forced checks is 24 hours.

If this check box is cleared, the application does not force any checks of the folder. The Server attempts to access files if they have been modified, added, or deleted.

By default, this check box is cleared.

- **Force folder scan for changes**

In this field, you can specify the time interval (in hours) after which the application starts a forced check for changes to the folder of automatic category content addition. By default, the time interval between forced checks is 24 hours. This field is available if the **Force folder scan for changes** check box is selected.

By default, this check box is cleared.

4. Follow the instructions of the Wizard.

When the Wizard completes, an application category with content added automatically is created. You can view the newly created category using the list of categories in the workspace of the **Application categories** folder.

See also:

Scenario: Application Management [1258](#)

Adding event-related executable files to the application category

You can add executable files related to the **Application startup prohibited** and **Application startup prohibited in test mode** events to an existing application category with content added manually or to a new application category.

► *To add executable files related to Application Control events to the application category:*

1. In the console tree, select the node with the name of the required Administration Server.
2. In the workspace of the node, select the **Events** tab.
3. On the **Events** tab, select the required events.
4. In the context menu of one of the selected events, select **Add to category**.
5. In the **Action on executable file related to the event** window that opens, specify the relevant settings:

Select one of the following:

- **Add to a new application category**

Select this option if you want to create a new application category.

Click the **OK** button to start the Create User Category Wizard. When the Wizard completes, the category with the specified settings is created.

By default, this option is not selected.

- **Add to an existing application category**

Select this option if you have to add rules to an existing application category. Select the relevant category in the list of application categories.

This option is selected by default.

In the **Rule type** section, select one of the following settings:

- **Add to category**

Select this option if you have to add rules to the conditions of the application category.

This option is selected by default.

- **Rules for adding to exclusions**

Select this option if you want to add rules to the exclusions of the application category.

In the **File info type** section, select one of the following settings:

- **Certificate details (or SHA-256 hashes for files without certificate)**

Files may be signed with a certificate. Multiple files may be signed with the same certificate. For example, different versions of the same application may be signed with the same certificate, or several different applications from the same vendor may be signed with the same certificate. When you select a certificate, several versions of an application or several applications from the same vendor may end up in the category.

Each file has its own unique SHA-256 hash function. When you select an SHA-256 hash function, only one corresponding file, for example, the defined application version, ends up in the category.

Select this option if you want to add to the category rules the certificate details of an executable file (or the SHA-256 hash function for files without a certificate).

By default, this option is selected.

- **Certificate details (files without a certificate will be skipped)**

Files may be signed with a certificate. Multiple files may be signed with the same certificate. For example, different versions of the same application may be signed with the same certificate, or several different applications from the same vendor may be signed with the same certificate. When you select a certificate, several versions of an application or several applications from the same vendor may end up in the category.

Select this option if you want to add the certificate details of an executable file to the category rules. If the executable file has no certificate, this file will be skipped. No information about this file will be added to the category.

- **Only SHA-256 (files without hash will be skipped)**

Each file has its own unique SHA-256 hash function. When you select an SHA-256 hash function, only one corresponding file, for example, the defined application version, ends up in the category.

Select this option if you want to add only the details of the SHA-256 hash function of the executable file.

- **Only MD5 (discontinued mode, only for Kaspersky Endpoint Security 10 Service Pack 1 version)**

Each file has its own unique MD5 hash function. When you select an MD5 hash function, only one corresponding file, for example, the defined application version, ends up in the category.

Select this option if you want to add only the details of the MD5 hash function of the executable file. Computing of the MD5 hash function is supported by Kaspersky Endpoint Security 10 Service Pack 1 for Windows and all earlier versions.

6. Click **OK**.

See also:

Scenario: Application Management.....[1258](#)

Configuring application startup management on client devices

Categorization of applications allows you to optimize management of application runs on devices. You can create an application category and configure Application Control for a policy so only applications from the specified category will be started on devices to which that policy is applied. For example, you have created a category that includes applications named *Application_1* and *Application_2*. After you add this category to a policy, only two applications are allowed to start on devices to which that policy is applied: *Application_1* and *Application_2*. If a user attempts to start an application that has not been included in that category, for example, *Application_3*, this application is blocked from being started. The user is shown a notification stating that *Application_3* is blocked from starting, in accordance with an Application Control rule. You can create a category with content added automatically based on various criteria from a specific folder. In this case, files are automatically added to the category from the specified folder. Executable files of applications are copied to the specified folder and processed automatically; their metrics are added to the category.

► *To configure the applications run management on client devices:*

1. In the **Advanced** → **Application management** folder in the console tree, select the **Application categories** subfolder.

2. In the workspace of the **Application categories** folder, create a category of applications (see section "Creating application categories for Kaspersky Endpoint Security for Windows policies" on page [487](#)) that you want to manage while they are being started.
3. In the **Managed devices** folder, on the **Policies** tab click the **New policy** button to create a new policy (see section "Creating a policy" on page [388](#)) for Kaspersky Endpoint Security for Windows, and follow the instructions of the Wizard.

If such a policy already exists, you can skip this step. You can configure management of the startup of applications in a specified category through the settings of this policy. The newly created policy is displayed in the **Managed devices** folder on the **Policies** tab.

4. Select **Properties** from the context menu of the policy for Kaspersky Endpoint Security for Windows.
The properties window of the policy for Kaspersky Endpoint Security for Windows opens.
5. In the properties window of the Kaspersky Endpoint Security for Windows policy, in the **Security Controls** → **Application Control** section select the **Application Control** check box.
6. Click the **Add** button.

The **Application Control rule** window opens.

7. In the **Application Control rule** window, in the **Category** drop-down list select the application category that the startup rule will cover. Configure the startup rule for the selected application category.

For Kaspersky Endpoint Security 10 Service Pack 2 and later, no categories are displayed if they were created upon the criterion of the MD5 hash of an executable file.

We do not recommend that you add any categories created according to the criterion of the SHA-256 hash of an executable file for versions earlier than Kaspersky Endpoint Security 10 Service Pack 2. This may result in application failures.

Detailed instructions on configuring control rules are provided in the Kaspersky Endpoint Security for Windows Online Help <https://support.kaspersky.com/KESWin/11.6.0/en-US/127971.htm>.

8. Click **OK**.

Applications will be run on devices included in the specified category according to the rule that you created. The newly created rule is displayed in the properties window of the Kaspersky Endpoint Security for Windows policy, in the **Application Control** section.

See also:

Scenario: Application Management [1258](#)

Viewing the results of static analysis of startup rules applied to executable files

► *To view information about which executable files are prohibited for users to run:*

1. In the **Managed devices** folder in the console tree, select the **Policies** tab.
2. Select **Properties** from the context menu of the policy for Kaspersky Endpoint Security for Windows.
The properties window of the application policy opens.
3. In the **Sections** pane, select **Security Controls** and then select the **Application Control** subsection.
4. Click the **Static analysis** button.

The **Analysis of the access rights list** window opens. In the left part of the window a user list based on Active Directory data is displayed.

5. Select a user from the list.

The right part of the window displays categories of applications assigned to this user.

6. To view executable files that the user is not allowed to run, in the **Analysis of the access rights list** window click the **View files** button.

A window opens, displaying a list of prohibited executable files.

7. To view a list of executable files included in a category, select the application category and click the **View files in category** button.

A window opens, displaying a list of executable files included in the application category.

Viewing the applications registry

Kaspersky Security Center inventories all software installed on managed devices.

Network Agent compiles a list of applications installed on a device, and then transmits this list to Administration Server. Network Agent automatically receives information about installed applications from the Windows registry.

Retrieval of information about installed applications is only available for devices running Microsoft Windows.

- *To view the registry of applications installed on client devices,*

In the **Advanced** → **Application management** folder in the console tree, select the **Applications registry** subfolder.

The workspace of the **Applications registry** folder displays a list of applications installed on client devices and the Administration Server.

You can view the details of any application by opening its context menu and selecting **Properties**. The application properties window displays the application details and information about its executable files, as well as a list of devices on which the application is installed.

In the context menu of any application in the list you can:

- Add this application to an application category.
- Assign a tag to the application.
- Export the list of applications to a CSV file or TXT file.
- View the application properties, for example, vendor name, version number, list of executable files, list of devices on which the application is installed, list of available software updates, or list of detected software vulnerabilities.

To view applications that meet specific criteria, you can use filtering fields in the workspace of the **Applications registry** folder.

In the properties window of the selected device (see section "Settings of a managed device" on page [658](#)), in the **Applications registry** section, you can view the list of applications installed on the device.

Generating a report on installed applications

In the **Applications registry** workspace, you can also click the **View report on installed applications** button to generate a report containing detailed statistics on the installed applications, including the number of devices on which each application is installed. This report, which opens on the **Report on Installed applications** page, contains information about both the Kaspersky applications and third-party software. If you want information only on Kaspersky applications installed on client devices, in the **Summary** list, select AO Kaspersky Lab.

Information about Kaspersky applications and third-party software installed on devices that are connected to secondary and virtual Administration Servers is also stored in the applications registry of the primary Administration Server. After you add data from secondary and virtual Administration Servers, click the **View report on installed applications** button, and on the **Report on installed applications** page that opens, you can view this information.

► *To add information from secondary and virtual Administration Servers to the report on installed applications:*

1. In the console tree, select the node with the name of the required Administration Server.
2. In the workspace of the node, select the **Reports** tab.
3. On the **Reports** tab, select **Report on installed applications**.
4. Select **Properties** from the context menu of the report.
The **Properties: Report on installed applications** window opens.
5. In the **Hierarchy of Administration Servers** section select the **Include data from secondary and virtual Administration Servers** check box.
6. Click **OK**.

Information from secondary and virtual Administration Servers will be included in the **Report on installed applications**.

See also:

Monitoring of applications installation and uninstallation	535
Scenario: Application Management	1258

Changing the software inventory start time

Kaspersky Security Center inventories all software installed on managed client devices running Windows.

Network Agent compiles a list of applications installed on a device, and then transmits this list to Administration Server. Network Agent automatically receives information about installed applications from the Windows registry.

To save the device resources, Network Agent by default starts receiving information about installed applications 10 minutes after the Network Agent service starts.

► *To change the software inventory start time, which elapses after the Network Agent service runs on a device:*

1. Open the system registry of the device on which Network Agent is installed (for example, locally, using the regedit command in the **Start** → **Run** menu).
2. Go to the following hive:
 - For a 64-bit system:
HKEY_LOCAL_MACHINE\SOFTWAREWow6432Node\KasperskyLab\Components\34\1103\1.0.0.0\NagentFlags
 - For a 32-bit system:
HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1103\1.0.0.0\NagentFlags
3. For the KLINV_INV_COLLECTOR_START_DELAY_SEC key, set the required value in seconds.
The default value is 600 seconds.
4. Restart the Network Agent service.

The software inventory start time, which elapses after the Network Agent service runs, is changed.

About license key management of third-party applications

Kaspersky Security Center allows you to track license key usage for third-party applications installed on the managed devices. The list of applications for which you can track license key usage is taken from the applications registry (see section "Viewing the applications registry" on page [496](#)). For each license key, you can specify and track violation of the following restrictions:

- Maximum number of devices on which the application using this license key can be installed
- Expiration date of the license key

Kaspersky Security Center does not check whether or not you specify a real license key. You can only track the restrictions that you specify. If one of the restrictions that you impose on a license key is violated, Administration Server registers an informational (see section "Administration Server informational events" on page [566](#)), warning (see section "Administration Server warning events" on page [552](#)), or functional failure (see section "Administration Server functional failure events" on page [543](#)) event.

License keys are bound to applications groups. An applications group is a group of third-party applications that you combine on a basis of a criterion or several criteria. You can define applications by the name of the application, its version, vendor, and tag. An application is added to the group if at least one of the criteria is met. To each applications group, you can bind several license keys, but each license key can be bound to a single applications group only.

One more tool that you can use to track license key usage is Report on status of licensed applications groups. This report provides information about the current status of licensed applications groups, including:

- Number of installations of license keys on each applications group
- Number of license keys in use and vacant license keys

- Detailed list of licensed applications installed on managed devices

The tools for license key management of third-party applications are located in the **Third-party licenses usage** subfolder (**Advanced** → **Application management** → **Third-party licenses usage**). In this subfolder, you can create applications groups (see section "Creating licensed applications groups" on page [499](#)), add license keys (see section "Managing license keys for licensed applications groups" on page [499](#)), and generate the Report on statuses on licensed application groups.

Creating licensed applications groups

► *To create a licensed applications group:*

1. In the **Advanced** → **Application management** folder in the console tree, select the **Third-party licenses usage** subfolder.
2. Click the **Add a licensed applications group** button to run Licensed Application Group Addition Wizard. Licensed Application Group Addition Wizard starts.
3. On the **Details of licensed applications group** step, specify which applications you want to include into the applications group:
 - **Name of licensed applications group**
 - **Track violated restrictions**
 - **Criteria for adding detected applications to this licensed applications group**
4. On the **Enter data about existing license keys** step, specify the license keys that you want to track. Select the **Control if license limit is exceeded** option, and then add the license keys:
 - a. Click the **Add** button.
 - b. Select the license key that you want to add, and then click the **OK** button. If the required license key is not listed, click the **Add** button, and then specify the license key properties (see section "Managing license keys for licensed applications groups" on page [499](#)).
5. On the **Add licensed applications group** step, click the **Finish** button.

A licensed applications group is created and displayed in the **Third-party licenses usage** folder.

Managing license keys for licensed applications groups

► *To create a license key for a licensed applications group:*

1. In the **Advanced** → **Application management** folder in the console tree, select the **Third-party licenses usage** subfolder.
2. In the workspace of the **Third-party licenses usage** folder, click the **Manage license keys of licensed applications** button.

The **License Key Management in licensed applications** window opens.
3. In the **License Key Management in licensed applications** window, click the **Add** button.

The **License key** window opens.
4. In the **License key** window, specify the properties of the license key and restrictions that the license key imposes on the licensed applications group.
 - **Name.** The name of the license key.

- **Comment.** Notes on the selected license key.
- **Restriction.** The number of devices on which the application using this license key can be installed.
- **Expires.** The expiration date of the license key.

Created license keys are displayed in the **License Key Management in licensed applications** window.

► *To apply a license key to a licensed applications group:*

1. In the **Advanced** → **Application management** folder in the console tree, select the **Third-party licenses usage** subfolder.
2. In the **Third-party licenses usage** folder, select a licensed applications group to which you want to apply a license key.
3. Select **Properties** from the context menu of the licensed applications group.
This opens the properties window of the licensed applications group.
4. In the properties window of the licensed applications group, in the **License keys** section, select **Control if license limit is exceeded**.
5. Click the **Add** button.
The **Selecting a license key** window opens.
6. In the **Selecting a license key** window, select a license key that you want to apply to a licensed applications group.
7. Click **OK**.

Restrictions imposed on a licensed applications group and specified in the license key will also apply to the selected licensed applications group.

Inventory of executable files

You can use an inventory task to inventory executable files on client devices. Kaspersky Endpoint Security 10 for Windows and later versions provide the feature of inventorying executable files.

The number of executable files received from a single device cannot exceed 150 000. Having reached this limit, Kaspersky Security Center cannot receive any new files.

► *To create an inventory task for executable files on client devices:*

1. In the console tree, select the **Tasks** folder.
2. By clicking the **New task** button in the workspace of the **Tasks** folder.
The New Task Wizard starts.
3. In the **Select the task type** window of the Wizard, select **Kaspersky Endpoint Security** as the task type, and then select **Inventory** as the task subtype, and click **Next**.
4. Follow the rest of the Wizard instructions.

After the Wizard is done, an inventory task for Kaspersky Endpoint Security is created. The newly created task is displayed in the list of tasks in the workspace of the **Tasks** folder.

A list of executable files that have been detected on devices during inventory is displayed in the workspace of the **Executable files** folder.

During inventory, the application detects executable files of the following formats: MZ, COM, PE, NE, SYS, CMD, BAT, PS1, JS, VBS, REG, MSI, CPL, DLL, JAR, and HTML files.

See also:

Scenario: Application Management.....[1258](#)

Viewing information about executable files

- ▶ *To view a list of all executable files detected on client devices,*

In the **Application management** folder of the console tree, select the **Executable files** subfolder.

The workspace of the **Executable files** folder displays a list of executable files that have been run on devices since the installation of the operating system or have been detected while running the inventory task of Kaspersky Endpoint Security for Windows.

To view details of executable files that match specific criteria, you can use filtering.

- ▶ *To view the properties of an executable file,*

From the context menu of the file, select **Properties**.

A window opens displaying information about the executable file and a list of devices on which this executable file can be found.

Monitoring and reporting

This section describes the monitoring and reporting capabilities of Kaspersky Security Center. These capabilities give you an overview of your infrastructure, protection statuses, and statistics.

After Kaspersky Security Center deployment or during the operation, you can configure the monitoring and reporting features to best suit your needs.

- Traffic lights

Administration Console allows you to quickly assess the current status of Kaspersky Security Center and managed devices by checking traffic lights.

- Statistics

Statistics on the status of the protection system and managed devices are displayed in information panels that can be customized.

- Reports

The Reports feature allows you to get detailed numerical information about the security of your organization's network, save this information to a file, send it by email, and print it.

- Events

Event selections provide an onscreen view of named sets of events that are selected from the Administration Server database. These sets of events are grouped according to the following categories:

- By importance level—**Critical events**, **Functional failures**, **Warnings**, and **Info events**
- By time—**Recent events**
- By type—**User requests** and **Audit events**

You can create and view user-defined event selections based on the settings available, in the Kaspersky Security Center 13 Web Console interface, for configuration.

In this chapter

Traffic lights in Administration Console	503
Working with reports, statistics, and notifications.....	503
Monitoring of applications installation and uninstallation.....	535
Event types	535
Blocking frequent events	582
Controlling changes in the status of virtual machines	584
Monitoring the anti-virus protection status using information from the system registry	584
Viewing and configuring the actions when devices show inactivity.....	586

Traffic lights in Administration Console

Administration Console allows you to quickly assess the current status of Kaspersky Security Center and managed devices by checking traffic lights. The traffic lights are shown in the workspace of the **Administration Server** node, on the **Monitoring** tab. The tab provides six information panels with traffic lights. A traffic light is a colored vertical bar on the left side of a panel. Each panel with a traffic light corresponds to a specific functional scope of Kaspersky Security Center (see the table below).

Table 46. Scopes covered by traffic lights in Administration Console

Panel name	Traffic light scope
Deployment	Installing Network Agent and security applications on devices on an organization's network
Management scheme	Structure of administration groups. Network scanning. Device moving rules
Protection settings	Security application functionality: protection status, virus scanning
Update	Updates and patches
Monitoring	Protection status
Administration Server	Administration Server features and properties

Each traffic light can be any of these five colors (see the table below). The color of a traffic light depends on the current status of Kaspersky Security Center and on events that were logged.

Table 47. Color codes of traffic lights

Status	Traffic light color	Traffic light color meaning
Informational	Green	Administrator's intervention is not required.
Warning	Yellow	Administrator's intervention is required.
Critical	Red	Serious problems have been encountered. Administrator's intervention is required to solve them.
Informational	Light blue	Events have been logged that are unrelated to potential or actual threats to the security of managed devices.
Informational	Gray	The details of events are not available or have not yet been retrieved.

The administrator's goal is to keep traffic lights on all of the information panels on the **Monitoring** tab green.

Working with reports, statistics, and notifications

This section provides information about how to work with reports, statistics, and selections of events and devices in Kaspersky Security Center, as well as how to configure Administration Server notifications.

In this section

Working with reports	504
Managing statistics	515
Configuring event notification	515
Creating a certificate for an SMTP server	518
Event selections.....	518
Configuring event export to a SIEM system	521
Device selections	521

Working with reports

Reports in Kaspersky Security Center contain information about the status of managed devices. Reports are generated based on information stored on Administration Server. You can create reports for the following types of objects:

- For device selections created according to specific settings.
- For administration groups.
- For specific devices from different administration groups.
- For all devices on the network (in the deployment report).

The application has a selection of standard report templates. It is also possible to create custom report templates. Reports are displayed in the main application window, in the **Administration Server** folder in the console tree.

See also:

Scenario: Deployment for cloud environment.....	821
Creating a report template	504
Viewing and editing report template properties	505
Extended filter format in report templates.....	507
Creating and viewing a report.....	509
Saving a report	510
Creating a report delivery task.....	510

Creating a report template

► *To create a report template:*

1. In the console tree, select the node with the name of the required Administration Server.
2. In the workspace of the node, select the **Reports** tab.

3. Click the **New report template** button.

The New Report Template Wizard starts. Follow the instructions of the Wizard.

After the Wizard finishes its operation, the newly created report template is added to the selected **Administration Server** folder in the console tree. You can use this template for generating and viewing reports.

Viewing and editing report template properties

You can view and edit basic properties of a report template, for example, the report template name or the fields displayed in the report.

► *To view and edit properties of a report template:*

1. In the console tree, select the node with the name of the required Administration Server.
2. In the workspace of the node, select the **Reports** tab.
3. In the list of report templates, select the required report template.
4. In the context menu of the selected report template, select **Properties**.

As an alternative, you can first generate the report, and then click either the **Open report template properties** button or the **Configure report columns** button.

5. In the window that opens, edit the report template properties. Properties of each report may contain only some of the sections described below.
 - **General** section
 - Report template name
 - **Maximum number of entries to display**

If this option is enabled, the number of entries displayed in the table with detailed report data does not exceed the specified value.

Report entries are first sorted according to the rules specified in the **Fields** → **Details fields** section of the report template properties, and then only the first of the resulting entries are kept. The heading of the table with detailed report data shows the displayed number of entries and the total available number of entries that match other report template settings.

If this option is disabled, the table with detailed report data displays all available entries. We do not recommend that you disable this option. Limiting the number of displayed report entries reduces the load on the database management system (DBMS) and reduces the time required for generating and exporting the report. Some of the reports contain too many entries. If this is the case, you may find it difficult to read and analyze them all. Also, your device may run out of memory while generating such a report and, consequently, you will not be able to view the report.

By default, this option is enabled. The default value is 1000.

- **Print version**

The report output is optimized for printing: space characters are added between some values for better visibility.

By default, this option is enabled.

- **Fields** section

Select the fields that will be displayed in the report, and the order of these fields, and configure whether the information in the report must be sorted and filtered by each of the fields.

- **Time interval** section

Modify the report period. Available values are as follows:

- Between the two specified dates
- From the specified date to the report creation date
- From the report creation date, minus the specified number of days, to the report creation date

- **Group, Device selection, or Devices** section

Change the set of client devices for which the report creates. Only one of these sections may be present, depending on the settings specified during the report template creation.

- **Settings** section

Change the settings of the report. The exact set of settings depends on the specific report.

- **Security** section

- **Inherit settings from Administration Server**

If this option is enabled, security settings of the report are inherited from the Administration Server.

If this option is disabled, you can configure security settings for the report. You can assign a role to a user or a group of users (see section "Assigning a role to a user or a user group" on page [707](#)) or assign permissions to a user or a group of users (see section "Assigning permissions to users and groups" on page [707](#)), as applied to the report.

By default, this option is enabled.

The **Security** section is available if the **Display security settings sections** (see section "**Adjusting the general settings of Administration Server**" on page [609](#)) check box is selected in the interface settings window.

- **Hierarchy of Administration Servers** section

- **Include data from secondary and virtual Administration Servers**

If this option is enabled, the report includes the information from the secondary and virtual Administration Servers that are subordinate to the Administration Server for which the report template is created.

Disable this option if you want to view data only from the current Administration Server.

By default, this option is enabled.

- **Up to nesting level**

The report includes data from secondary and virtual Administration Servers that are located under the current Administration Server on a nesting level that is less than or equal to the specified value.

The default value is 1. You may want to change this value if you have to retrieve information from secondary Administration Servers located at lower levels in the tree.

- **Data wait interval (min)**

Before generating the report, the Administration Server for which the report template is

created waits for data from secondary Administration Servers during the specified number of minutes. If no data is received from a secondary Administration Server at the end of this period, the report runs anyway. Instead of the actual data, the report shows data taken from the cache (if the **Cache data from secondary Administration Servers** option is enabled), or **N/A** (not available) otherwise.

The default value is 5 (minutes).

- **Cache data from secondary Administration Servers**

Secondary Administration Servers regularly transfer data to the Administration Server for which the report template is created. There, the transferred data is stored in the cache.

If the current Administration Server cannot receive data from a secondary Administration Server while generating the report, the report shows data taken from the cache. The date when the data was transferred to the cache is also displayed.

Enabling this option allows you to view the information from secondary Administration Servers even if the up-to-date data cannot be retrieved. However, the displayed data can be obsolete.

By default, this option is disabled.

- **Cache update frequency (h)**

Secondary Administration Servers at regular intervals transfer data to the Administration Server for which the report template is created. You can specify this period in hours. If you specify 0 hours, data is transferred only when the report is generated.

The default value is 0.

- **Transfer detailed information from secondary Administration Servers**

In the generated report, the table with detailed report data includes data from secondary Administration Servers of the Administration Server for which the report template is created.

Enabling this option slows the report generation and increases traffic between Administration Servers. However, you can view all data in one report.

Instead of enabling this option, you may want to analyze detailed report data to detect a faulty secondary Administration Server, and then generate the same report only for that faulty Administration Server.

By default, this option is disabled.

Extended filter format in report templates

In Kaspersky Security Center 13, you can apply the extended filter format to a report template. The extended filter format provides more flexibility in comparison with the default format. You can create complex filtering conditions by using a set of filters, which will be applied to the report by means of the OR logical operator during report creation, as shown below:

```
Filter[1](Field[1] AND Field[2]... AND Field[n]) OR Filter[2](Field[1] AND Field[2]... AND Field[n]) OR...  
Filter[n](Field[1] AND Field[2]... AND Field[n])
```

Additionally, with the extended filter format you can set a time interval value in a relative time format (for example, by using a "For last N days" condition) for specific fields in a filter. The availability and the set of time interval conditions depend on the type of the report template.

In this section

Converting the filter into the extended format.....	508
Configuring the extended filter.....	508

Converting the filter into the extended format

The extended filter format for report templates is supported only in Kaspersky Security Center 12 and later versions. After conversion of the default filter into the extended format, the report template becomes incompatible with Administration Servers on your network that have earlier versions of Kaspersky Security Center installed. Information from these Administration Servers will not be received for the report.

► To convert the report template default filter into the extended format:

1. In the console tree, select the node with the name of the required Administration Server.
2. In the workspace of the node, select the **Reports** tab.
3. In the list of report templates, select the required report template.
4. In the context menu of the selected report template, select **Properties**.
5. In the properties window that opens, select the **Fields** section.
6. In the **Details fields** tab click the **Convert filter** link.
7. In the window that opens, click the **OK** button.

Conversion into the extended filter format is irreversible for the report template to which it is applied. If you clicked the **Convert filter** link accidentally, you can cancel the changes by clicking the **Cancel** button in the report template properties window.

8. To apply the changes, close the report template properties window by clicking the **OK** button. When the report template properties window opens again, the newly available **Filters** section is displayed. In this section you can configure the extended filter (see section "Configuring the extended filter" on page [508](#)).

Configuring the extended filter

► To configure the extended filter in the report template properties:

1. In the console tree, select the node with the name of the required Administration Server.
2. In the workspace of the node, select the **Reports** tab.
3. In the list of report templates, select the report template that was previously converted to extended filter format (see section "Converting the filter into the extended format" on page [508](#)).
4. In the context menu of the selected report template, select **Properties**.

5. In the properties window that opens, select the **Filters** section.

The **Filters** section is not displayed if the report template was not previously converted to extended filter format (see section "Converting the filter into the extended format" on page [508](#)).

In the **Filters** section of the report template properties window you can review and modify the list of filters applied to the report. Each filter in the list has a unique name and represents a set of filters for corresponding fields in the report.

6. Open the filter settings window in one of the following ways:

- To create a new filter, click the **Add** button.
- To modify the existing filter, select the required filter and click the **Modify** button.

7. In the window that opens, select and specify the values of the required fields of the filter.

8. Click the **OK** button to save changes and close the window.

If you are creating a new filter, the filter name must be specified in the **Filter name** field before clicking the **OK** button.

9. Close the report template properties window by clicking the **OK** button.

The extended filter in the report template is configured. Now you can create reports (see section "Creating and viewing a report" on page [509](#)) by using this report template.

Creating and viewing a report

► *To create and view a report:*

1. In the console tree, select the node with the name of the required Administration Server.
2. In the workspace of the node, select the **Reports** tab.
3. In the list of report templates, double-click the report template that you need.

A report for the selected template is displayed.

The report displays the following data:

- The name and type of report, a brief description and the reporting period, as well as information about the group of devices for which the report is generated.
- Graph chart showing the most representative report data.
- Consolidated table with calculated report indicators.
- Table with detailed report data.

See also:

Scenario: Updating third-party software[1208](#)

Saving a report

► *To save a created report:*

1. In the console tree, select the node with the name of the required Administration Server.
2. In the workspace of the node, select the **Reports** tab.
3. In the list of report templates, select the report template that you need.
4. In the context menu of the selected report template, select **Save**.

The Report Saving Wizard starts. Follow the instructions of the Wizard.

After the Wizard finishes, the folder opens to which you have saved the report file.

Creating a report delivery task

Reports can be emailed. Delivery of reports in Kaspersky Security Center is carried out using the report delivery task.

► *To create a delivery task for a single report:*

1. In the console tree, select the node with the name of the required Administration Server.
2. In the workspace of the node, select the **Reports** tab.
3. In the list of report templates, select the report template that you need.
4. In the context menu of the selected report template, select **Deliver reports**.

The Report Delivery Task Creation Wizard starts. Follow the instructions of the Wizard.

► *To create a delivery task for multiple reports:*

1. In the console tree, under the node with the name of the required Administration Server, select the **Tasks** folder.
2. In the workspace of the **Tasks** folder, click the **Create a task** button.

The New Task Wizard starts. Follow the instructions of the Wizard.

The newly created report delivery task is displayed in the **Tasks** folder in the console tree.

The report delivery task is created automatically if the email settings (see section "Administration Server Quick Start Wizard" on page [265](#)) were specified during Kaspersky Security Center installation.

In this section

Step 1. Selecting the task type	511
Step 2. Selecting the report type	511
Step 3. Actions on a report	511
Step 4. Selecting the account to start the task	512
Step 5. Configuring a task schedule	512
Step 6. Defining the task name	515
Step 7. Completing creation of the task.....	515

Step 1. Selecting the task type

In the **Select the task type** window, in the list of tasks select **Deliver reports** as the task type.

Click **Next** to proceed to the next step.

Step 2. Selecting the report type

In the **Select report type** window, in the list of task creation templates, select the type of report.

Click **Next** to proceed to the next step.

Step 3. Actions on a report

In the **Action to apply to reports** window, specify the following settings:

- **Send reports by email**

If this check box is selected, the application sends generated reports by email.

You can configure the report sending by email by clicking the **Email notification settings** link. The link is available if this check box is selected.

If this check box is cleared, the application saves reports in the specified folder to store them.

By default, this check box is cleared.

- **Save reports to shared folder**

If this check box is selected, the application saves reports to the folder that is specified in the field under the check box. To save reports to a shared folder, specify the UNC path to the folder. In this case, in the **Selecting an account to run the task** window, you must specify the user account and password for accessing this folder.

If this check box is cleared, the application does not save reports to the folder and sends them by email instead.

By default, this check box is cleared.

- **Overwrite older reports of the same type**

If this check box is selected, the new report file at each task startup overwrites the file that was saved in the reports folder at the previous task startup.

If this check box is cleared, report files will not be overwritten. A new report file is stored in the reports folder at each task run.

This check box is available, if the **Save report to folder** is selected.

By default, this check box is cleared.

- **Specify account for access to shared folder**

If this check box is selected, you can specify the account under which the report will be saved to the folder. If a UNC path to a shared folder is specified as the **Save report to folder** setting in the **Action to be applied to report** window, you must specify the user account and password for accessing this folder.

If this check box is cleared, the report is saved to the folder under the account of Administration Server.

This check box is available, if the **Save report to folder** is selected.

By default, this check box is cleared.

Click **Next** to proceed to the next step.

Step 4. Selecting the account to start the task

In the **Selecting an account to run the task** window, you can specify which account to use when running the task. Select one of the following options:

- **Default account**

The task will be run under the same account as the application that performs this task.

By default, this option is selected.

- **Specify account**

Fill in the **Account** and **Password** fields to specify the details of an account under which the task is run. The account must have sufficient rights for this task.

- **Account**

Account under which the task is run.

- **Password**

Password of the account under which the task will be run.

Click **Next** to proceed to the next step.

Step 5. Configuring a task schedule

On the **Configure task schedule** wizard page, you can create a schedule for task start. If necessary, configure the following settings:

- **Scheduled start:**

Select the schedule according to which the task runs, and configure the selected schedule.

- **Every N hours**

The task runs regularly, with the specified interval in hours, starting from the specified date and time.

By default, the task runs every six hours, starting from the current system date and time.

- **Every N days**

The task runs regularly, with the specified interval in days. Additionally, you can specify a date and time of the first task run. These additional options become available, if they are supported by the application for which you create the task.

By default, the task runs every day, starting from the current system date and time.

- **Every N weeks**

The task runs regularly, with the specified interval in weeks, on the specified day of week and at the specified time.

By default, the task runs every Monday at the current system time.

- **Every N minutes**

The task runs regularly, with the specified interval in minutes, starting from the specified time on the day that the task is created.

By default, the task runs every 30 minutes, starting from the current system time.

- **Daily (daylight saving time is not supported)**

The task runs regularly, with the specified interval in days. This schedule does not support observance of daylight saving time (DST). It means that when clocks jump one hour forward or backward at the beginning or ending of DST, the actual task start time does not change.

We do not recommend that you use this schedule. It is needed for backward compatibility of Kaspersky Security Center.

By default, the task starts every day at the current system time.

- **Weekly**

The task runs every week on the specified day and at the specified time.

- **By days of week**

The task runs regularly, on the specified days of week, at the specified time.

By default, the task runs every Friday at 6:00:00 P.M.

- **Monthly**

The task runs regularly, on the specified day of the month, at the specified time.

In months that lack the specified day, the task runs on the last day.

By default, the task runs on the first day of each month, at the current system time.

- **Manually**

The task does not run automatically. You can only start it manually.

- **Every month on specified days of selected weeks**

The task runs regularly, on the specified days of each month, at the specified time.

By default, no days of month are selected; the default start time is 6:00:00 P.M.

- **On virus outbreak**

The task runs after a *Virus outbreak* event occurs. Select application types that will monitor virus outbreaks. The following application types are available:

- Anti-virus for workstations and file servers
- Anti-virus for perimeter defense
- Anti-virus for mail systems

By default, all application types are selected.

You may want to run different tasks depending on the anti-virus application type that reports a virus outbreak. In this case, remove the selection of the application types that you do not need.

- **On completing another task**

The current task starts after another task completes. You can select how the previous task must complete (successfully or with error) to trigger the start of the current task. For example, you may want to run the Manage devices task with the **Turn on the device** option and, after it completes, run the Virus scan task.

- **Run missed tasks**

This option determines the behavior of a task if a client device is not visible on the network when the task is about to start.

If this option is enabled, the system attempts to start the task the next time the Kaspersky application is run on the client device. If the task schedule is **Manually, Once** or **Immediately**, the task is started immediately after the device becomes visible on the network or immediately after the device is included in the task scope.

If this option is disabled, only scheduled tasks run on client devices; for **Manually, Once** and **Immediately**, tasks run only on those client devices that are visible on the network. For example, you may want to disable this option for a resource-consuming task that you want to run only outside of business hours.

By default, this option is enabled.

- **Use automatically randomized delay for task starts**

If this option is enabled, the task is started on client devices randomly within a specified time interval, that is, *distributed task start*. A distributed task start helps to avoid a large number of simultaneous requests by client devices to the Administration Server when a scheduled task is running.

The distributed start time is calculated automatically when a task is created, depending on the number of client devices to which the task is assigned. Later, the task is always started on the calculated start time. However when task settings are edited or the task is started manually, the calculated value of the task start time changes.

If this option is disabled, the task starts on client devices according to the schedule.

- **Use randomized delay for task starts within an interval of (min)**

If this option is enabled, the task is started on client devices randomly within the specified time interval. A distributed task start helps to avoid a large number of simultaneous requests by client devices to the Administration Server when a scheduled task is running.

If this option is disabled, the task starts on client devices according to the schedule.

By default, this option is disabled. The default time interval is one minute.

Step 6. Defining the task name

In the **Define the task name** window, specify the name for the task that you are creating. A task name cannot be more than 100 characters long and cannot include any special characters (" * < > ? \ : |).

Click **Next** to proceed to the next step.

Step 7. Completing creation of the task

In the **Finish task creation** window, click the **Finish** button to finish the Wizard.

If you want the task to start as soon as the Wizard finishes, select the **Run the task after the Wizard finishes** check box.

Managing statistics

Statistics on the status of the protection system and managed devices are displayed in information panels that can be customized. Statistics are displayed in the workspace of the **Administration Server** node on the **Statistics** tab. The tab contains some second-level tabs (pages). Each tabbed page displays information panels with statistics, as well as links to corporate news and other materials from Kaspersky. The statistical information is displayed in information panels as a table or chart (pie or bar). The data in the information panels is updated while the application is running and reflects the current state of the protection application.

You can modify the set of second-level tabs on the **Statistics** tab, the number of information panels on each tabbed page, and the data display mode in information panels.

► *To add a new second-level tab with information panels on the **Statistics** tab:*

1. Click the **Customize view** button in the upper right corner of the **Statistics** tab.

The statistics properties window opens. This window contains a list of tabbed pages that are currently shown on the **Statistics** tab. In this window, you can change the display order for the pages on the tab, add and remove pages, and proceed to configuration of page properties by clicking the **Properties** button.

2. Click the **Add** button.


This opens the properties window of a new page.

3. Configure the new page:

- In the **General** section, specify the page name.
- In the **Information panels** section, click the **Add** button to add information panels that must be displayed on the page.

Click the **Properties** button in the **Information panels** section to set up the properties of information panels that you added: name, type, and appearance of the chart in the panel, as well as data required to plot the chart.

4. Click **OK**.

The tabbed page with information panels that you have added appears on the **Statistics** tab. Click the **Settings** icon () to proceed instantly to configuration of the page or a selected information panel on that page.

Configuring event notification

Kaspersky Security Center allows you to select a method of notifying the administrator of events on client devices

and to configure notification.

- **Email.** When an event occurs, the application sends a notification to email addresses specified. You can edit the text of the notification.
- **SMS.** When an event occurs, the application sends a notification to the phone numbers specified. You can configure SMS notifications to be sent through the mail gateway.
- **Executable file.** When an event occurs on a device, the executable file is started on the administrator's workstation. Using the executable file, the administrator can receive the parameters of any event that has occurred (see section "Event notifications displayed by running an executable file" on page [300](#)).

► *To configure notification of events occurring on client devices:*

1. In the console tree, select the node with the name of the required Administration Server.
2. In the workspace of the node, select the **Events** tab.
3. Click the **Configure notifications and event export** link and select the **Configure notifications** value in the drop-down list.

This opens the **Properties: Events** window.

4. In the **Notification** section, select a notification method (by email, by SMS, or by running an executable file) and define the notification settings:

- **Email**

The **Email** tab allows you to configure event notification by email.

In the **Recipients (email addresses)** field, specify the email addresses to which the application will send notifications. You can specify multiple addresses in this field, separating them with semicolons.

In the **SMTP servers** field, specify mail server addresses, separating them with semicolons. You can use the IP address or the Windows network name (NetBIOS name) of the device as the address.

In the **SMTP server port** field, specify the number of an SMTP server communication port. The default port number is 25.

Click the **Settings** link to define additional notification settings (for example, specify a message subject).

The **Notification message** field contains standard text with information about the event that the application sends when an event occurs. This text includes substitute parameters, such as event name, device name, and domain name. You can edit the message text by adding some other substitute parameters with more relevant details of the event. The list of substitute parameters is available by clicking the button to the right of the field.

If the notification text contains a percent sign (%), you have to type it twice in a row to allow message sending. For example, "CPU load is 100%%".

Clicking the **Configure numeric limit of notifications** link allows you to specify the maximum number of notifications that the application can send over the specified time interval.

Clicking the **Send test message** button allows you to check if you have configured notifications properly: the application sends a test notification to the email addresses that you have specified.

- **SMS**

The **SMS** tab allows you to configure the transmission of SMS notifications of various events to a cell phone. SMS messages will be sent through a mail gateway.

In the **Recipients (email addresses)** field, specify the email addresses to which the application will send notifications. You can specify multiple addresses in this field, separating them with semicolons. The notifications will be delivered to the phone numbers associated with the specified email addresses.

In the **SMTP servers** field, specify mail server addresses, separating them with semicolons. You can use the IP address or the Windows network name (NetBIOS name) of the device as the address.

In the **SMTP server port** field, specify the number of an SMTP server communication port. The default port number is 25.

Click the **Settings** link to define additional notification settings (for example, specify a message subject).

The **Notification message** field contains standard text with information about the event that the application sends when an event occurs. This text includes substitute parameters, such as event name, device name, and domain name. You can edit the message text by adding some other substitute parameters with more relevant details of the event. The list of substitute parameters is available by clicking the button to the right of the field.

If the notification text contains a percent sign (%), you have to type it twice in a row to allow message sending. For example, "CPU load is 100%%".

Clicking the **Configure numeric limit of notifications** link allows you to specify the maximum number of notifications that the application can send during the specified time interval.

Clicking the **Send test message** allows you to check whether you configured notifications properly: the application sends a test notification to the recipient that you specified.

- **Executable file to be run**

If this notification method is selected, in the entry field you can specify the application that will start when an event occurs.

Clicking the **Configure numeric limit of notifications** link allows you to specify the maximum number of notifications that the application can send during the specified time interval.

Clicking the **Send test message** button allows you to check whether you configured notifications properly: the application sends a test notification to the email addresses that you specified.

1. In the **Notification message** field, enter the text that the application will send when an event occurs.

You can use the drop-down list to the right of the text field to add substitution settings with event details (for example, event description, or time of occurrence).

If the notification text contains a percent (%), you must specify it twice in succession to allow message sending. For example, "CPU load is 100%%".

2. Click the **Send test message** button to check whether notification has been configured correctly.

The application sends a test notification to the specified user.

3. Click **OK** to save the changes.

The re-adjusted notification settings are applied to all events that occur on client devices.

You can override notification settings for certain events in the **Event configuration** section of the Administration Server settings, of a policy settings (see section "General policy settings" on page [663](#)), or of an application settings (see section "Selecting events for an application" on page [798](#)).

See also:

Event processing and storage on the Administration Server[610](#)

Creating a certificate for an SMTP server

► *To create a certificate for an SMTP server:*

1. In the console tree, select the node with the name of the required Administration Server.
2. In the workspace of the node, select the **Events** tab.
3. Click the **Configure notifications and event export** link and select the **Configure notifications** value in the drop-down list.

The event properties window opens.

4. On the **Email** tab, click the **Settings** link to open the **Settings** window.
5. In the **Settings** window click the **Specify certificate** link to open the **Certificate for signing** window.
6. In the **Certificate for signing** window, click the **Browse** button.

The **Certificate** window opens.

7. In the **Certificate type** drop-down list, specify the public or private type of certificate:
 - If the private type of certificate (**PKCS #12 container**) is selected, specify the certificate file and the password.
 - If the public type of certificate (**X.509 certificate**) is selected:
 - a. Specify the private key file (one with the *.prk or *.pem extension).
 - b. Specify the private key password.
 - c. Specify the public key file (one with the *.cer extension).
8. Click **OK**.

The certificate for the SMTP server is issued.

Event selections

Information about events in the operation of Kaspersky Security Center and managed applications is saved both in the Administration Server database and in the Microsoft Windows system log. You can view information from the Administration Server database in the workspace of the **Administration Server** node, on the **Events** tab.

Information on the **Events** tab is represented as a list of event selections. Each selection includes events of a specific type only. For example, the "Device status is Critical" selection contains only records about changes of device statuses to "Critical". After application installation, the **Events** tab contains some standard event selections. You can create additional (custom) event selections or export event information to a file.

In this section

Viewing an event selection	519
Customizing an event selection	519
Creating an event selection	519
Exporting an event selection to a text file	520
Deleting events from a selection	520
Adding applications to exclusions by user requests	520

Viewing an event selection

► *To view the event selection:*

1. In the console tree, select the node with the name of the required Administration Server.
2. In the workspace of the node, select the **Events** tab.
3. In the **Event selections** drop-down list, select the relevant event selection.

If you want events from this selection to be continuously displayed in the workspace, click the ☆ button next to the selection.

The workspace will display a list of events, stored on the Administration Server, of the selected type.

You can sort information in the list of events in ascending or descending order in any column.

Customizing an event selection

► *To customize an event selection:*

1. In the console tree, select the node with the name of the required Administration Server.
2. In the workspace of the node, select the **Events** tab.
3. Open the relevant event selection on the **Events** tab.
4. Click the **Selection properties** button.

In the event selection properties window that opens you can configure the event selection.

Creating an event selection

► *To create an event selection:*

1. In the console tree, select the node with the name of the required Administration Server.
2. In the workspace of the node, select the **Events** tab.
3. Click the **Create a selection** button.
4. In the **New event selection** window that opens, enter the name of the new selection and click **OK**.

A selection with the name that you specified is created in the **Event selections** drop-down list.

By default, a created event selection contains all events stored on the Administration Server. To cause a selection to display only the events you want, you must customize the selection.

Exporting an event selection to a text file

► *To export an event selection to a text file:*

1. In the console tree, select the node with the name of the required Administration Server.
2. In the workspace of the node, select the **Events** tab.
3. Click the **Import/Export** button.
4. In the drop-down list, select **Export events to file**.

The Events Export Wizard starts. Follow the instructions of the Wizard.

Deleting events from a selection

► *To delete events from a selection:*

1. In the console tree, select the node with the name of the relevant Administration Server.
2. In the workspace of the node, select the **Events** tab.
3. Select the events that you want to delete by using a mouse, the **SHIFT** key, or the **CTRL** key.
4. Delete the selected events in one of the following ways:
 - By selecting **Delete** in the context menu of any of the selected events.
If you select the **Delete All** item from the context menu, all displayed events will be deleted from the selection, regardless of your choice of events to delete.
 - By clicking the **Delete event** link (if one event is selected) or the **Delete events** link (if several events are selected) in the information box for these events.

The selected events are deleted.

Adding applications to exclusions by user requests

When you receive user requests to unblock erroneously blocked applications, you can create an exclusion from the Adaptive Security rules for these applications. Consequently, the applications will no longer be blocked on users' devices. You can track the number of user requests on the **Monitoring** tab of Administration Server.

► *To add applications blocked by Kaspersky Endpoint Security to exclusions by user requests:*

1. In the console tree, select the node with the name of the required Administration Server.
2. In the workspace of the node, select the **Events** tab.
3. In the **Event selections** drop-down list, select **User requests**.
4. Right-click the user request (or several user requests) containing applications that you want to add to exclusions, and then select **Add exclusion**.

This starts the **Add Exclusion** Wizard (see section "Adding exclusions from the Adaptive Anomaly Control rules" on page [779](#)). Follow its instructions.

The selected applications will be excluded from the **Triggering of rules in Smart Training state** list (under **Repositories** in the console tree) after the next synchronization of the client device with the Administration Server, and will no longer appear in the list.

Configuring event export to a SIEM system

The application allows you to export events—registered during the operation of Administration Server and other Kaspersky applications that are installed on client devices—to a Security Information and Event Management (SIEM) system.

► *To configure events export to a SIEM system:*

1. In the console tree, select the node with the name of the required Administration Server.
2. In the workspace of the node, select the **Events** tab.
3. Click the **Configure notifications and event export** link and select the **Configure export to SIEM system** value in the drop-down list.

The events properties window opens, displaying the **Exporting events** section.

4. Select the **Automatically export events to SIEM system database** check box.
5. In the **SIEM system** drop-down list, select the system to which you have to export events.
Events can be exported to SIEM systems, such as QRadar® (LEEF format), ArcSight (CEF format), Splunk® (CEF format), and Syslog format (RFC 5424). The ArcSight (CEF format) system is selected by default.
6. Specify the address of a SIEM system server and a port for connection to that server in the corresponding fields.

Clicking the **Export archive** button causes the application to export newly created events to the database of the SIEM system starting from the specified date. By default, the application exports events starting from the current date.

7. Click **OK**.

After you select the **Automatically export events to SIEM system database** check box and configure connection with the server, the application will automatically export all events to the SIEM system when they are registered during the operation of Administration Server and other Kaspersky applications.

For more details of event export, see section "Exporting events to SIEM systems (on page [791](#))".

Device selections

Information about the status of devices is displayed in the **Device selections** folder in the console tree.

Information in the **Device selections** folder is displayed as a list of device selections. Each selection contains devices that meet specific conditions. For example, the **Devices with Critical status** selection contains only devices with the *Critical* status. After application installation, the **Device selections** folder contains some standard selections. You can create additional (custom) device selections, export selection settings to file, or create selections with settings imported from another file.

In this section

Viewing a device selection.....	522
Configuring a device selection.....	522
Exporting the settings of a device selection to a file.....	533
Creating a device selection	534
Creating a device selection according to imported settings	534
Removing devices from administration groups in a selection	534

Viewing a device selection

► *To view a device selection:*

1. In the console tree, select the **Device selections** folder.
2. In the workspace of the folder, in the **Devices in this selection** list, select the relevant device selection.
3. Click the **Run selection** button.
4. Click the **Selection results** tab.

The workspace will display a list of devices that meet the selection criteria.

You can sort the information in the list of devices in ascending or descending order, in any column.

Configuring a device selection

► *To configure a device selection:*

1. In the console tree, select the **Device selections** folder.
2. In the workspace, click the **Selection** tab, and then click the relevant device selection in the list of user selections.
3. Click the **Selection properties** button.
4. In the properties window that opens, specify the following settings:
 - General selection properties.
 - Conditions that must be met for including devices in this selection. You can configure the conditions after selecting a condition name and clicking the **Properties** button.
 - Security settings.
5. Click **OK**.

The settings are applied and saved.

Below are descriptions of the conditions for assigning devices to a selection. Conditions are combined by using the OR logical operator: the selection will contain devices that comply with at least one of the listed conditions.

General

In the **General** section, you can change the name of the selection condition and specify

whether that condition must be inverted:

- **Invert selection condition**

If this check box is selected, the specified selection condition will be inverted. The selection will include all devices that do not meet the condition.

By default, this check box is cleared.

Network

In the **Network** section, you can specify the criteria that will be used to include devices in the selection according to their network data:

- **Device name or IP address**

Name of the device in the Windows network (NetBIOS name).

- **Windows domain**

Displays all devices included in the specified Windows domain.

- **Administration group**

Displays devices included in the specified administration group.

- **Description**

Text in the device properties window: In the **Description** field of the **General** section.

To describe text in the **Description** field, you can use the following characters:

- Within a word:

- *. Replaces any string with any number of characters.

Example:

To describe words such as **Server** or **Server's**, you can enter **Server***.

- ?. Replaces any single character.

Example:

To describe words such as **Window** or **Windows**, you can enter **Windo?**.

Asterisk (*) or question mark (?) cannot be used as the first character in the query.

- To find several words:

- Space. You will see all devices whose descriptions contain any of the listed words.

Example:

To find a phrase that contains **Secondary** or **Virtual** words, you can include **Secondary Virtual** line in your query.

- +. When a plus sign precedes a word, all search results will contain this word.

Example:

To find a phrase that contains both **Secondary** and **Virtual**, enter the **+Secondary+Virtual** query.

- -. When a minus sign precedes a word, no search results will contain this word.

Example:

To find a phrase that contains **Secondary** and does not contain **Virtual**, enter the

+**Secondary-Virtual** query.

- "**<some text>**". Text enclosed in quotation marks must be present in the text.

Example:

To find a phrase that contains **Secondary Server** word combination, you can enter "**Secondary Server**" in the query.

- **IP range**

If this check box is selected, you can enter the initial and final IP addresses of the IP range in which the relevant devices must be included.

By default, this check box is cleared.

Tags

In the **Tags** section, you can configure criteria for including devices into a selection based on key words (tags) that were previously added to the descriptions of managed devices:

- **Apply if at least one specified tag matches**

If this check box is selected, the search results will show devices with descriptions that contain at least one of the selected tags.

If this check box is cleared, the search results will only show devices with descriptions that contain all the selected tags.

By default, this check box is cleared.

- **Tag must be included**

If this option is selected, the search results will display the devices whose descriptions contain the selected tag. To find devices, you can use the asterisk, which stands for any string with any number of characters.

By default, this option is selected.

- **Tag must be excluded**

If this option is selected, the search results will display the devices whose descriptions do not contain the selected tag. To find devices, you can use the asterisk, which stands for any string with any number of characters.

Active Directory

In the **Active Directory** section, you can configure criteria for including devices into a selection based on their Active Directory data:

- **Device is in an Active Directory organizational unit**

If this check box is selected, the selection includes devices from the Active Directory unit specified in the entry field.

By default, this check box is cleared.

- **Include child organizational units**

If this check box is selected, the selection includes devices from all child OUs of the specified Active Directory OU.

By default, this check box is cleared.

- **This device is a member of an Active Directory group**

If this check box is selected, the selection includes devices from the Active Directory group specified in the entry field.

By default, this check box is cleared.

Network activity

In the **Network activity** section, you can specify the criteria that will be used to include devices in the selection according to their network activity:

- **This device is a distribution point**

In the drop-down list, you can set up the criterion for including devices in the selection when performing search:

- **Yes.** The selection includes devices that act as distribution points.
- **No.** Devices that act as distribution points are not included in the selection.
- **No value is selected.** The criterion will not be applied.

- **Do not disconnect from the Administration Server**

In the drop-down list, you can set up the criterion for including devices in the selection when performing search:

- **Enabled.** The selection will include devices on which the **Do not disconnect from the Administration Server** check box is selected.
- **Disabled.** The selection will include devices on which the **Do not disconnect from the Administration Server** check box is cleared.
- **No value is selected.** The criterion will not be applied.

- **Connection profile switched**

In the drop-down list, you can set up the criterion for including devices in the selection when performing search:

- **Yes.** The selection will include devices that connected to the Administration Server after the connection profile was switched.
- **No.** The selection will not include devices that connected to the Administration Server after the connection profile was switched.
- **No value is selected.** The criterion will not be applied.

- **Last connected to Administration Server**

You can use this check box to set a search criterion for devices according to the time they last connected to the Administration Server.

If this check box is selected, in the entry fields you can specify the time interval (date and time) during which the last connection was established between Network Agent installed on the client device and the Administration Server. The selection will include devices that fall within the specified interval.

If this check box is cleared, the criterion will not be applied.

By default, this check box is cleared.

- **New devices detected by network poll**

Searches for new devices that have been detected by network polling over the last few days.

If this check box is selected, the selection only includes new devices that have been

detected by device discovery over the number of days specified in the **Detection period (days)** field.

If this check box is cleared, the selection includes all devices that have been detected by device discovery.

By default, this check box is cleared.

- **Device is visible**

In the drop-down list, you can set up the criterion for including devices in the selection when performing search:

- **Yes.** The application includes in the selection devices that are currently visible in the network.
- **No.** The application includes in the selection devices that are currently invisible in the network.
- **No value is selected.** The criterion will not be applied.

Application

In the **Application** section, you can configure criteria for including devices in a selection based on the selected managed application:

- **Application name**

In the drop-down list, you can set a criterion for including devices in a selection when search is performed by the name of a Kaspersky application.

The list provides only the names of applications with management plug-ins installed on the administrator's workstation.

If no application is selected, the criterion will not be applied.

- **Application version**

In the entry field, you can set a criterion for including devices in a selection when search is performed by the version number of a Kaspersky application.

If no version number is specified, the criterion will not be applied.

- **Critical update name**

In the entry field, you can set a criterion for including devices in a selection when search is performed by application name or by update package number.

If the field is left blank, the criterion will not be applied.

- **Modules last updated**

You can use this setting to set a criterion for searching devices by time of the last update of modules of applications installed on those devices.

If this check box is selected, in the entry fields you can specify the time interval (date and time) during which the last update of modules of applications installed on those devices was performed.

If this check box is cleared, the criterion will not be applied.

By default, this check box is cleared.

- **Device is managed through Kaspersky Security Center 13**

In the drop-down list, you can include in the selection the devices managed through Kaspersky Security Center:

- **Yes.** The application includes in the selection devices managed through Kaspersky Security Center.
 - **No.** The application includes devices in the selection if they are not managed through Kaspersky Security Center.
 - **No value is selected.** The criterion will not be applied.
- **Security application is installed**

In the drop-down list, you can include in the selection all devices with the security application installed:

 - **Yes.** The application includes in the selection all devices with the security application installed.
 - **No.** The application includes in the selection all devices with no security application installed.
 - **No value is selected.** The criterion will not be applied.

Operating system

In the **Operating system** section, you can specify the criteria that will be used to include devices in the selection according to their operating system type.

- **Operating system version**

If the check box is selected, you can select an operating system from the list. Devices with the specified operating systems installed are included in the search results.
- **Operating system bit size**

In the drop-down list, you can select the architecture for the operating system, which will determine how the moving rule is applied to the device (**Unknown**, **x86**, **AMD64**, or **IA64**). By default, no option is selected in the list so that the operating system's architecture is not defined.
- **Operating system service pack version**

In this field, you can specify the package version of the operating system (in X.Y format), which will determine how the moving rule is applied to the device. By default, no version value is specified.
- **Operating system build**

This setting is applicable to Windows operating systems only.

The build number of the operating system. You can specify whether the selected operating system must have an equal, earlier, or later build number. You can also configure searching for all build numbers except the specified one.

- **Operating system release ID**

This setting is applicable to Windows operating systems only.

The release identifier (ID) of the operating system. You can specify whether the selected operating system must have an equal, earlier, or later release ID. You can also configure searching for all release ID numbers except the specified one.

Device status

In the **Device status** section, you can configure criteria for including devices into a selection based on the description of the devices status from a managed application:

- **Device status**

Drop-down list in which you can select one of the device statuses: *OK*, *Critical*, or *Warning*.

- **Device status description**

In this field, you can select the check boxes next to conditions that, if met, assign one of the following statuses to the device: *OK*, *Critical*, or *Warning*.

- **Device status defined by application**

Drop-down list, in which you can select the real-time protection status. Devices with the specified real-time protection status are included in the selection.

Protection components

In the **Protection components** section, you can set up the criteria for including devices in a selection based on their protection status:

- **Databases released**

If this check box is selected, you can search for client devices by anti-virus database release date. In the entry fields you can set the time interval, on the basis of which the search is performed.

By default, this check box is cleared.

- **Last scanned**

If this check box is selected, you can search for client devices by time of the last virus scan. In the entry fields you can specify the time period within which the last virus scan was performed.

By default, this check box is cleared.

- **Total number of threats detected**

If this check box is selected, you can search for client devices by number of viruses detected. In the entry fields you can set the lower and upper threshold values for the number of viruses found.

By default, this check box is cleared.

Applications registry

In the **Applications registry** section, you can set up the criteria to search for devices according to applications installed on them:

- **Application name**

Drop-down list in which you can select an application. Devices on which the specified application is installed, are included in the selection.

- **Application version**

Entry field in which you can specify the version of selected application.

- **Vendor**

Drop-down list in which you can select the manufacturer of an application installed on the device.

- **Application status**

A drop-down list in which you can select the status of an application (*Installed, Not installed*). Devices on which the specified application is installed or not installed, depending on the selected status, will be included in the selection.

- **Find by update**

If this check box is selected, search will be performed using the details of updates for applications installed on the relevant devices. After you select the check box, the **Application name**, **Application version**, and **Application status** fields change to **Update name**, **Update version**, and **Status** respectively.

By default, this check box is cleared.

- **Incompatible security application name**

Drop-down list in which you can select third-party security applications. During the search, devices on which the specified application is installed, are included in the selection.

- **Application tag**

In the drop-down list, you can select the application tag. All devices that have installed applications with the selected tag in the description are included in the device selection.

- **Apply to devices without the specified tags**

If this check box is selected, the selection includes devices with descriptions that contain none of the selected tags.

If this check box is cleared, the criterion is not applied.

By default, this check box is cleared.

Hardware registry

In the **Hardware registry** section, you can configure criteria for including devices into a selection based on their installed hardware:

- **Device**

In the drop-down list, you can select a unit type. All devices with this unit are included in the search results.

The field supports the full-text search.

- **Vendor**

In the drop-down list, you can select the name of a unit manufacturer. All devices with this unit are included in the search results.

The field supports the full-text search.

- **Device name**

Name of the device in the Windows network. The device with the specified name is included in the selection.

- **Description**

Description of the device or hardware unit. Devices with the description specified in this field are included in the selection.

A device's description in any format can be entered in the properties window of that device. The field supports the full-text search.

- **Device vendor**

Name of the device manufacturer. Devices produced by the manufacturer specified in this field are included in the selection.

You can enter the manufacturer's name in the properties window of a device.

- **Serial number**

All hardware units with the serial number specified in this field will be included in the selection.

- **Inventory number**

Equipment with the inventory number specified in this field will be included in the selection.

- **User**

All hardware units of the user specified in this field will be included in the selection.

- **Location**

Location of the device or hardware unit (for example, at the HQ or a branch office). Computers or other devices that are deployed at the location specified in this field will be included in the selection.

You can describe the location of a device in any format in the properties window of that device.

- **CPU frequency, in MHz**

The frequency range of a CPU. Devices with CPUs that match the frequency range in these fields (inclusive) will be included in the selection.

- **Virtual CPU cores**

Range of the number of virtual cores in a CPU. Devices with CPUs that match the range in these fields (inclusive) will be included in the selection.

- **Hard drive volume, in GB**

Range of values for the size of the hard drive on the device. Devices with hard drives that match the range in these entry fields (inclusive) will be included in the selection.

- **RAM size, in MB**

Range of values for the size of the device RAM. Devices with RAMs that match the range in these entry fields (inclusive) will be included in the selection.

Virtual machines

In the **Virtual machines** section, you can set up the criteria to include devices in the selection according to whether these are virtual machines or part of virtual desktop infrastructure (VDI):

- **This is a virtual machine**

In the drop-down list you can select the following options:

- **Not important.**

- **No.** Find devices that are not virtual machines.
 - **Yes.** Find devices that are virtual machines.
- **Virtual machine type**

In the drop-down list, you can select the virtual machine manufacturer.

This drop-down list is available if the **Yes** or **Not important** value is selected in the **This is a virtual machine** drop-down list.
 - **Part of Virtual Desktop Infrastructure**

In the drop-down list you can select the following options:
 - **Not important.**
 - **No.** Find devices that are not part of Virtual Desktop Infrastructure.
 - **Yes.** Find devices that are part of the Virtual Desktop Infrastructure (VDI).

Vulnerabilities and updates

In the **Vulnerabilities and updates** section, you can specify the criteria that will be used to include devices in the selection according to their Windows Update source:

- **WUA is switched to Administration Server**

You can select one of the following search options from the drop-down list:

 - **Yes.** If this option is selected, the search results will include devices that receive updates through Windows Update from the Administration Server.
 - **No.** If this option is selected, the results will include devices that receive updates through Windows Update from another sources.

Users

In the **Users** section, you can set up the criteria to include devices in the selection according to the accounts of users who have logged in to the operating system.

- **Last user who logged in to the system**

If this check box is selected, click the **Browse** button to specify a user account. The search results include devices on which the specified user performed the last login to the system.
- **User who logged in to the system at least once**

If this check box is selected, click the **Browse** button to specify a user account. The search results include devices on which the specified user logged in to the system at least once.

Status-affecting problems in managed applications

In the **Status-affecting problems in managed applications** section, you can specify the criteria that will be used to include devices in the selection according to the list of possible problems detected by a managed application. If at least one problem that you select exists on a device, the device will be included in the selection. When you select a problem listed for several applications, you have the option to select this problem in all of the lists automatically.

- **Device status description**

You can select check boxes for descriptions of statuses from the managed application; upon receipt of these statuses, the devices will be included in the selection. When you

select a status listed for several applications, you have the option to select this status in all of the lists automatically.

Statuses of components in managed applications

In the **Statuses of components in managed applications** section, you can configure criteria for including devices in a selection according to the statuses of components in managed applications:

- **Data Leakage Prevention status**

Search for devices by the status of Data Leakage Prevention (*No data from device, Stopped, Starting, Paused, Running, Failed*).

- **Collaboration servers protection status**

Search for devices by the status of server collaboration protection (*No data from device, Stopped, Starting, Paused, Running, Failed*).

- **Anti-virus protection status of mail servers**

Search for devices by the status of Mail Server protection (*No data from device, Stopped, Starting, Paused, Running, Failed*).

- **Endpoint Sensor status**

Search for devices by the status of the Endpoint Sensor component (*No data from device, Stopped, Starting, Paused, Running, Failed*).

Encryption

- **Encryption algorithm**

Advanced Encryption Standard (AES) symmetrical block cipher algorithm. In the drop-down list, you can select the encryption key size (56-bit, 128-bit, 192-bit, or 256-bit).

Available values: *AES56, AES128, AES192, and AES256*.

Cloud segments

In the **Cloud segments** section, you can configure criteria for including devices in a selection according to their respective cloud segments:

- **Device is in a cloud segment**

If this check box is selected, you can click the **Browse** button to specify the segment to search.

If the **Include child objects** check box is also selected, the search is run on all child objects of the specified segment.

Search results include only devices from the selected segment.

- **Device discovered by using the API**

In the drop-down list, you can select whether a device is detected by API tools.

- **AWS.** The device is discovered by using AWS API, that is, the device definitely is in the AWS cloud environment.
- **Azure.** The device is discovered by using Azure API, that is, the device definitely is in the Azure cloud environment.
- **Google Cloud.** The device is discovered by using Google API, that is, the device definitely is in the Google cloud environment.

- **No.** The device cannot be detected by using AWS, Azure or Google API, that is, it is either outside the cloud environment, or it is in the cloud environment but it cannot be detected by using an API for some reason.
- No value. This criterion cannot be applied.

Application components

This section contains the list of components of those applications that have corresponding management plugins installed in Administration Console.

In the **Application components** section, you can specify criteria for including devices in a selection according to the statuses and version numbers of the components that refer to the application that you select:

- **Status**

Search for devices according to the component status sent by an application to the Administration Server. You can select one of the following statuses: *No data from device*, *Stopped*, *Starting*, *Paused*, *Running*, *Malfunction*, or *Not installed*. If the selected component of the application installed on a managed device has the specified status, the device is included in the device selection.

Statuses sent by applications:

- *Starting*—The component is currently in the process of initialization.
- *Running*—The component is enabled and working properly.
- *Paused*—The component is suspended, for example, after the user has paused protection in the managed application.
- *Malfunction*—An error has occurred during the component operation.
- *Stopped*—The component is disabled and not working at the moment.
- *Not installed*—The user did not select the component for installation when configuring custom installation of the application.

Unlike other statuses, the *No data from device* status is not sent by applications. This option shows that the applications have no information about the selected component status. For example, this can happen when the selected component does not belong to any of the applications installed on the device, or when the device is turned off.

- **Version**

Search for devices according to the version number of the component that you select in the list. You can type a version number, for example *3.4.1.0*, and then specify whether the selected component must have an equal, earlier, or later version. You can also configure searching for all versions except the specified one.

Exporting the settings of a device selection to a file

► *To export the settings of a device selection to a text file:*

1. In the console tree, select the **Device selections** folder.
2. In the workspace, on the **Selection** tab, click the relevant device selection in the list of user selections.

Settings can be exported only from the device selections created by a user.

3. Click the **Run selection** button.
4. On the **Selection results** tab, click the **Export settings** button.
5. In the **Save as** window that opens, specify a name for the selection settings export file, select a folder to save it to, and click the **Save** button.

The settings of the device selection will be saved to the specified file.

Creating a device selection

► *To create a device selection:*

1. In the console tree, select the **Device selections** folder.
2. In the workspace of the folder, click **Advanced** and select the **Create a selection** in the drop-down list.
3. In the **New device selection** window that opens, enter the name of the new selection and click **OK**.

A new folder with the name you entered will appear in the console tree in the **Device selections** folder. By default, the new device selection contains all devices included in administration groups of the Administration Server on which the selection was created. To cause a selection to display only the devices you are particularly interested in, configure the selection by clicking the **Selection properties** button.

Creating a device selection according to imported settings

► *To create a device selection according to imported settings:*

1. In the console tree, select the **Device selections** folder.
2. In the workspace of the folder, click the **Advanced** button and select **Import selection from file** in the drop-down list.
3. In the window that opens, specify the path to the file from which you want to import the selection settings. Click the **Open** button.

A **New selection** entry is created in the **Device selections** folder. The settings of the new selection are imported from the file that you specified.

If a selection named **New selection** already exists in the **Device selections** folder, an index in (<next sequence number>) format is added to the name of the created selection, for example: **(1)**, **(2)**.

Removing devices from administration groups in a selection

When working with a device selection, you can remove devices from administration groups right in this selection, without switching to the administration groups from which these devices must be removed.

► *To remove devices from administration groups:*

1. In the console tree, select the **Device selections** folder.

2. Select the devices that you want to remove by using the **Shift** or **Ctrl** keys.
3. Remove the selected devices from administration groups in one of the following ways:
 - By selecting **Delete** in the context menu of any of the selected devices.
 - By clicking the **Perform action** button and selecting **Remove from group** in the drop-down list.

The selected devices are removed from their respective administration groups.

Monitoring of applications installation and uninstallation

You can monitor installation or uninstallation of specific applications on managed devices, for example, specific browser. To use this function, you can add applications from the Application registry to the list of monitored applications. When a monitored application is installed or uninstalled, Network Agent publishes respective events (see section "Network Agent informational events" on page [572](#))—**Monitored application has been installed** or **Monitored application has been uninstalled**. You can monitor these events using, for example, event selections (on page [518](#)) or reports (see section "Working with reports" on page [504](#)).

You can monitor these events only if they are stored in Administration Server database.

► *To add an application to the list of monitored applications:*

1. In the **Advanced** → **Application management** folder in the console tree, select the **Applications registry** subfolder.
2. Above the list of application, that is displayed, click the **Show applications registry properties window** button.
3. In the **Monitored Applications** window, that is displayed, click the **Add** button.
4. In the **Select application name** window, that is displayed, select the applications from the Application registry whose installation or uninstallation you want to monitor.
5. In the **Select application name** window, click the **OK** button.

After you have configured the list of monitored applications, and a monitored application is installed or uninstalled on managed devices in your organization, you can monitor the respective events, for example using the Recent events event selection.

Event types

Each Kaspersky Security Center component has its own set of event types. This section lists types of events that occur in Kaspersky Security Center Administration Server, Network Agent, iOS MDM Server, and Exchange Mobile Device Server. Types of events that occur in Kaspersky applications are not listed in this section.

In this section

Data structure of event type description	536
Administration Server events.....	536
Network Agent events.....	568
iOS MDM Server events	575
Exchange Mobile Device Server events.....	581

Data structure of event type description

For each event type, its display name, identifier (ID), alphabetic code, description, and the default storage term are provided.

- **Event type display name.** This text is displayed in Kaspersky Security Center when you configure events and when they occur.
- **Event type ID.** This numerical code is used when you process events by using third-party tools for event analysis.
- **Event type** (alphabetic code). This code is used when you browse and process events by using public views that are provided in the Kaspersky Security Center database and when events are exported to a SIEM system.
- **Description.** This text contains the situations when an event occurs and what you can do in such a case.
- **Default storage term.** This is the number of days during which the event is stored in the Administration Server database and is displayed in the list of events on Administration Server. After this period elapses, the event is deleted. If the event storage term value is 0, such events are detected but are not displayed in the list of events on Administration Server. If you configured to save such events to the operating system event log, you can find them there.

You can change the storage term for events:

- Administration Console: Setting the storage term for an event (see section "Event processing and storage on the Administration Server" on page [610](#))
- Kaspersky Security Center 13 Web Console: Setting the storage term for an event (on page [1305](#))

Administration Server events

This section contains information about the events related to the Administration Server.

In this section

Administration Server critical events	538
Administration Server functional failure events	543
Administration Server warning events	552
Administration Server informational events	566

Administration Server critical events

The table below shows the events of Kaspersky Security Center Administration Server that have the **Critical** severity level.

Table 48. Administration Server critical events

Event type display name	Event type ID	Event type	Description	Default storage term
License limit has been exceeded	4099	KLSRV_EV_LICENSE_CHECK_MORE_10	<p>Once a day Kaspersky Security Center checks whether a licensing restriction is exceeded.</p> <p>Events of this type occur when Administration Server detects that some licensing limits are exceeded by Kaspersky applications installed on client devices and if the number of currently used licensing units (see section "About the license certificate" on page 319) covered by a single license exceeds 110% of the total number of units covered by the license.</p> <p>Even when this event occurs, client devices are protected.</p> <p>You can respond to the event in the following ways:</p> <ul style="list-style-type: none"> • Look through the managed devices list. Delete devices that are not in use. • Provide a license for more devices (add a valid activation code or a key file to Administration Server). <p>Kaspersky Security Center determines the rules to generate events (see section "Events of the licensing limit exceeded" on page 329) when a licensing restriction is exceeded.</p>	180 days
Virus outbreak	26 (for File Threat Protection)	GNRL_EV_VIRUS_OUTBREAK	<p>Events of this type occur when the number of malicious objects detected on several managed devices exceeds the threshold within a short period of time.</p> <p>You can respond to the event in the following ways:</p> <ul style="list-style-type: none"> • Configure the threshold in the Administration Server properties (on page 611). • Create a stricter policy (see section "Activating a policy automatically at the Virus outbreak event" on page 390) that will be activated, or create a task (see section "Creating a task" on page 374) that will be run, at the occurrence of this event. 	180 days

Event type display name	Event type ID	Event type	Description	Default storage term
Virus outbreak	27 (for Mail Threat Protection)	GNRL_EV_VIRUS_OUTBR EAK	<p>Events of this type occur when the number of malicious objects detected on several managed devices exceeds the threshold within a short period of time.</p> <p>You can respond to the event in the following ways:</p> <ul style="list-style-type: none"> • Configure the threshold in the Administration Server properties (on page 611). • Create a stricter policy (see section "Activating a policy automatically at the Virus outbreak event" on page 390) that will be activated, or create a task (see section "Creating a task" on page 374) that will be run, at the occurrence of this event. 	180 days
Virus outbreak	28 (for firewall)	GNRL_EV_VIRUS_OUTBR EAK	<p>Events of this type occur when the number of malicious objects detected on several managed devices exceeds the threshold within a short period of time.</p> <p>You can respond to the event in the following ways:</p> <ul style="list-style-type: none"> • Configure the threshold in the Administration Server properties (on page 611). • Create a stricter policy (see section "Activating a policy automatically at the Virus outbreak event" on page 390) that will be activated, or create a task (see section "Creating a task" on page 374) that will be run, at the occurrence of this event. 	180 days
Device has become unmanaged	4111	KLSRV_H OST_OUT_CONT ROL	<p>Events of this type occur if a managed device is visible on the network but has not connected to Administration Server for a specific period of time.</p> <p>Find out what prevents the proper functioning of Network Agent on the device. Possible causes include network issues and removal of Network Agent from the device.</p>	180 days

Event type display name	Event type ID	Event type	Description	Default storage term
Device status is Critical	4113	KLSRV_HOST_STATUS_CRITICAL	Events of this type occur when a managed device is assigned the <i>Critical</i> status. You can configure the conditions (see section "Configuring the switching of device statuses" on page 647) under which the device status is changed to <i>Critical</i> .	180 days
The key file has been added to the denylist	4124	KLSRV_LICENSE_BLACKLISTED	Events of this type occur when Kaspersky has added the activation code or key file that you use to the denylist. Contact Technical Support (on page 1401) for more detail.	180 days
Limited functionality mode	4130	KLSRV_EV_LICENSE_SRV_LIMITED_MODE	Events of this type occur when Kaspersky Security Center starts to operate with basic functionality (see section "About restrictions on the main functionality" on page 322), without Vulnerability and Patch Management and without Mobile Device Management features. Following are causes of, and appropriate responses to, the event: <ul style="list-style-type: none"> • License term has expired. Provide a license to use the full functionality mode of Kaspersky Security Center (add a valid activation code or a key file to Administration Server). • Administration Server manages more devices than specified by the license limit. Move devices from the administration groups of an Administration Server to those of another Administration Server (if the license limit of the other Administration Server allows). 	180 days

Event type display name	Event type ID	Event type	Description	Default storage term
License expires soon	4129	KLSRV_EV_LICEN SE_SRV_ EXPIRE_ SOON	<p>Events of this type occur when the commercial license (see section "About the license" on page 319) expiration date is approaching.</p> <p>When the commercial license expires, Kaspersky Security Center provides only basic functionality (see section "About restrictions on the main functionality" on page 322).</p> <p>You can respond to the event in the following ways:</p> <ul style="list-style-type: none"> • Make sure that a reserve license key (see section "About the license key" on page 320) is added to Administration Server. • If you use a subscription (see section "About the subscription" on page 328), make sure to renew it. An unlimited subscription is renewed automatically if it has been prepaid to the service provider by the due date. 	180 days
Certificate has expired	4132	KLSRV_C ERTIFICA TE_EXPI RED	<p>Events of this type occur when the Administration Server certificate for Mobile Device Management expires.</p> <p>You need to update the expired certificate (see section "Working with certificates" on page 737).</p> <p>You can configure automatic updates of certificates by selecting the Reissue certificate automatically if possible check box in the certificate issuance settings (see section "Configuring certificate issuance rules" on page 742).</p>	180 days
Updates for Kaspersky software modules have been revoked	4142	KLSRV_S EAMLES S_UPDAT E_REVO KED	<p>Events of this type occur if seamless updates (see section "Approving and declining software updates" on page 1197) have been revoked (<i>Revoked</i> status is displayed for these updates) by Kaspersky technical specialists; for example, they must be updated to a newer version. The event concerns Kaspersky Security Center patches and does not concern modules of managed Kaspersky applications. The event provides the reason that the seamless updates are not installed.</p>	180 days

See also:

Administration Server functional failure events	543
Administration Server informational events	566
Administration Server warning events	552
Events in Kaspersky Security Center	792

Administration Server functional failure events

The table below shows the events of Kaspersky Security Center Administration Server that have the **Functional failure** severity level.

Table 49. Administration Server functional failure events

Event type display name	Event type ID	Event type	Description	Default storage term
Runtime error	4125	KLSRV_RUNTIME_ERROR	<p>Events of this type occur because of unknown issues.</p> <p>Most often these are DBMS issues, network issues, and other software and hardware issues.</p> <p>Details of the event can be found in the event description.</p>	180 days

Event type display name	Event type ID	Event type	Description	Default storage term
<p>Limit of installations has been exceeded for one of the licensed applications groups</p>	<p>4126</p>	<p>KLSRV_INVLICPROD_EXCEDED</p>	<p>Administration Server generates events of this type periodically (every hour). Events of this type occur if in Kaspersky Security Center you manage license keys of third-party applications and if the number of installations has exceeded the limit set by the license key of the third-party application. You can respond to the event in the following ways:</p> <ul style="list-style-type: none"> • Look through the managed devices list. Delete the third-party application from devices on which the application is not in use. • Use a third-party license for more devices. <p>You can manage license keys of third-party applications (see section "Managing license keys for licensed applications groups" on page 499) using the functionality of licensed applications groups. A licensed applications group includes third-party applications that meet criteria set by you.</p>	<p>180 days</p>

Event type display name	Event type ID	Event type	Description	Default storage term
Failed to poll the cloud segment	4143	KLSRV_KLCLLOUD_SCAN_ERROR	<p>Events of this type occur when Administration Server fails to poll a network segment in a cloud environment (see section "Network segment polling" on page 865).</p> <p>Read the details in the event description and respond accordingly.</p>	Not stored
Failed to copy the updates to the specified folder	4123	KLSRV_UPD_REPL_FAIL	<p>Events of this type occur when software updates are copied to an additional shared folder(s).</p> <p>You can respond to the event in the following ways:</p> <ul style="list-style-type: none"> • Check whether the user account that is employed to gain access to the folder(s) has write permission. • Check whether a user name and/or a password to the folder(s) changed. • Check the Internet connection, as it might be the cause of the event. Follow the instructions to update databases and software modules (see section "Creating the task for downloading updates to the repository of the Administration Server" on page 413). 	180 days

Event type display name	Event type ID	Event type	Description	Default storage term
No free disk space	4107	KLSRV_DISK_FULL	<p>Events of this type occur when the hard drive of the device on which Administration Server is installed runs out of free space.</p> <p>Free up disk space on the device.</p>	180 days
Shared folder is not available	4108	KLSRV_SHARED_FOLDER_UNAVAILABLE	<p>Events of this type occur if the shared folder of Administration Server (see section "Defining a shared folder" on page 224) is not available.</p> <p>You can respond to the event in the following ways:</p> <ul style="list-style-type: none"> • Check whether the Administration Server (where the shared folder is located) is turned on and available. • Check whether a user name and/or a password to the folder is/are changed. • Check the network connection. 	180 days

Event type display name	Event type ID	Event type	Description	Default storage term
The Administration Server database is unavailable	4109	KLSRV_DATABASE_UNAVAILABLE	<p>Events of this type occur if the Administration Server database becomes unavailable. You can respond to the event in the following ways:</p> <ul style="list-style-type: none"> • Check whether the remote server that has SQL Server installed is available. • View the DBMS logs to discover the reason for Administration Server database unavailability. For example, because of preventive maintenance a remote server with SQL Server installed might be unavailable. 	180 days

<p>No free space in the Administration Server database</p>	<p>4110</p>	<p>KLSRV_DATABASE_FULL</p>	<p>Events of this type occur when there is no free space in the Administration Server database.</p> <p>Administration Server does not function when its database has reached its capacity and when further recording to the database is not possible.</p> <p>Following are the causes of this event, depending on the DBMS that you use, and appropriate responses to the event:</p> <ul style="list-style-type: none"> • You use the SQL Server Express Edition DBMS: <ul style="list-style-type: none"> • In the SQL Server Express documentation, review the database size limit for the version you use. Probably your Administration Server database has exceeded the database size limit. • Limit the number of events to store in the Administration Server database (see section "Setting the maximum number of events in the event repository" on page 1008). • In the Administration 	<p>180 days</p>
---	-------------	----------------------------	---	-----------------

			<p>Server database there are too many events sent by the Application Control component. You can change the settings of the Kaspersky Endpoint Security for Windows policy relating to Application Control event storage in the Administration Server database.</p> <ul style="list-style-type: none">• You use a DBMS other than SQL Server Express Edition:<ul style="list-style-type: none">• Do not limit the number of events to store in the Administration Server database (see section "Setting the maximum number of events in the event repository" on page 1008).• Reduce the list of events to store in the Administration Server database (see section "Setting the storage term for an event" on page 1305). <p>Review the information on DBMS selection (see</p>	
--	--	--	---	--

Event type display name	Event type ID	Event type	Description	Default storage term
			section "Selecting a DBMS" on page 129).	

See also:

Administration Server critical events	538
Administration Server informational events	566
Administration Server warning events	552
Events in Kaspersky Security Center	792

Administration Server warning events

The table below shows the events of Kaspersky Security Center Administration Server that have the **Warning** severity level.

Table 50. Administration Server warning events

Event type display name	Event type ID	Event type	Description	Default storage term
<p>License limit has been exceeded</p>	<p>4098</p>	<p>KLSRV_EV_LIC NSE_CHECK_100 _110</p>	<p>Once a day Kaspersky Security Center checks whether a licensing restriction is exceeded.</p> <p>Events of this type occur when Administration Server detects that some licensing limits are exceeded by Kaspersky applications installed on client devices and if the number of currently used licensing units (see section "About the license certificate" on page 319) covered by a single license constitute 100% to 110% of the total number of units covered by the license.</p> <p>Even when this event occurs, client devices are protected.</p> <p>You can respond to the event in the following ways:</p> <ul style="list-style-type: none"> • Look through the managed devices list. Delete devices that are not in use. • Provide a license for more devices (add a valid activation code or a key file to Administration Server). <p>Kaspersky Security Center determines the rules to generate events (see section "Events of the licensing limit exceeded" on page 329) when a licensing restriction is exceeded.</p>	<p>90 days</p>

Event type display name	Event type ID	Event type	Description	Default storage term
Device has remained inactive on the network for a long time	4103	KLSRV_EVENT_HOSTS_NOT_VISIBLE	<p>Events of this type occur when a managed device shows inactivity for some time.</p> <p>Most often, this happens when a managed device is decommissioned. You can respond to the event in the following ways:</p> <ul style="list-style-type: none"> • Manually remove the device from the list of managed devices. • Specify the time interval after which the Device has remained inactive on the network for a long time event is created by using Administration Console (see section "Viewing and configuring the actions when devices show inactivity" on page 586) or by using Kaspersky Security Center 13 Web Console (see section "Viewing and configuring the actions when devices show inactivity" on page 1098). • Specify the time interval after which the device is automatically removed from the group by using Administration Console (see section "Viewing and configuring the actions when devices show inactivity" on page 586) or by using Kaspersky Security Center 13 Web Console (see section "Viewing and configuring the actions when devices show inactivity" on page 1098). 	90 days

Event type display name	Event type ID	Event type	Description	Default storage term
Conflict of device names	4102	KLSRV_EVENT_HOSTS_CONFLICT	<p>Events of this type occur when Administration Server considers two or more managed devices as a single device.</p> <p>Most often this happens when a cloned hard drive was used for software deployment on managed devices and without switching the Network Agent to the dedicated disk cloning mode on a reference device.</p> <p>To avoid this issue, switch Network Agent to the disk cloning mode (see section "Network Agent disk cloning mode" on page 889) on a reference device before cloning the hard drive of this device.</p>	90 days
Device status is Warning	4114	KLSRV_HOST_STATUS_WARNING	<p>Events of this type occur when a managed device is assigned the <i>Warning</i> status. You can configure the conditions (see section "Configuring the switching of device statuses" on page 647) under which the device status is changed to <i>Warning</i>.</p>	90 days

Event type display name	Event type ID	Event type	Description	Default storage term
<p>Limit of installations will soon be exceeded for one of the licensed applications groups</p>	<p>4127</p>	<p>KLSRV_INVLICPR OD_FILLED</p>	<p>Events of this type occur when the number of installations for third-party applications included in a licensed applications group (see section "Groups of applications" on page 485) reaches 90% of the maximum allowed value specified in the license key properties (see section "Managing license keys for licensed applications groups" on page 499).</p> <p>You can respond to the event in the following ways:</p> <ul style="list-style-type: none"> • If the third-party application is not in use on some of the managed devices, delete the application from these devices. • If you expect that the number of installations for the third-party application will exceed the allowed maximum in the near future, consider obtaining a third-party license for a greater number of devices in advance. <p>You can manage license keys of third-party applications (see section "Managing license keys for licensed applications groups" on page 499) using the functionality of licensed applications groups.</p>	<p>90 days</p>

Event type display name	Event type ID	Event type	Description	Default storage term
Certificate has been requested	4133	KLSRV_CERTIFICATE_REQUESTED	<p>Events of this type occur when a certificate for Mobile Device Management fails to be automatically reissued.</p> <p>Following might be the causes and appropriate responses to the event:</p> <ul style="list-style-type: none"> • Automatic reissue was initiated for a certificate for which the Reissue certificate automatically if possible option (see section "Configuring certificate issuance rules" on page 742) is disabled. This might be due to an error that occurred during creation of the certificate. Manual reissue of the certificate might be required. • If you use an integration with a public key infrastructure (see section "Integration with public key infrastructure" on page 743), the cause might be a missing SAM-Account-Name attribute of the account used for integration with PKI and for issuance of the certificate. Review the account properties. 	90 days
Certificate has been removed	4134	KLSRV_CERTIFICATE_REMOVED	<p>Events of this type occur when an administrator removes any type of certificate (General, Mail, VPN) for Mobile Device Management.</p> <p>After removing a certificate, mobile devices connected via this certificate will fail to connect to Administration Server.</p> <p>This event might be helpful when investigating malfunctions associated with the management of mobile devices.</p>	90 days

Event type display name	Event type ID	Event type	Description	Default storage term
APNs certificate has expired	4135	KLSRV_APN_CERTIFICATE_EXPIRED	<p>Events of this type occur when an APNs certificate expires.</p> <p>You need to manually renew the APNs certificate (see section "Renewing an APNs certificate" on page 203) and install it on an iOS MDM Server (see section "Installing an APNs certificate on an iOS MDM Server" on page 205).</p>	Not stored
APNs certificate expires soon	4136	KLSRV_APN_CERTIFICATE_EXPIRES_SOON	<p>Events of this type occur when there are fewer than 14 days left before the APNs certificate expires.</p> <p>When the APNs certificate expires, you need to manually renew the APNs certificate (see section "Renewing an APNs certificate" on page 203) and install it on an iOS MDM Server (see section "Installing an APNs certificate on an iOS MDM Server" on page 205).</p> <p>We recommend that you schedule the APNs certificate renewal in advance of the expiration date.</p>	Not stored

Event type display name	Event type ID	Event type	Description	Default storage term
Failed to send the FCM message to the mobile device	4138	KLSRV_GCM_DE VICE_ERROR	<p>Events of this type occur when Mobile Device Management is configured to use Google Firebase Cloud Messaging (FCM) (see section "Using Google Firebase Cloud Messaging" on page 735) for connecting to managed mobile devices with an Android operating system and FCM Server fails to handle some of the requests received from Administration Server. It means that some of the managed mobile devices will not receive a push notification.</p> <p>Read the HTTP code in the details of the event description and respond accordingly. For more information on the HTTP codes received from FCM Server and related errors, please refer to the Google Firebase service documentation https://firebase.google.com/docs/cloud-messaging/http-server-ref (see chapter "Downstream message error response codes").</p>	90 days

Event type display name	Event type ID	Event type	Description	Default storage term
HTTP error sending the FCM message to the FCM server	4139	KLSRV_GCM_HTTP_ERROR	<p>Events of this type occur when Mobile Device Management is configured to use Google Firebase Cloud Messaging (FCM) (see section "Using Google Firebase Cloud Messaging" on page 735) for connecting managed mobile devices with the Android operating system and FCM Server reverts to the Administration Server a request with a HTTP code other than 200 (OK).</p> <p>Following might be the causes and appropriate responses to the event:</p> <ul style="list-style-type: none"> • Problems on the FCM server side. Read the HTTP code in the details of the event description and respond accordingly. For more information on the HTTP codes received from FCM Server and related errors, please refer to the Google Firebase service documentation https://firebase.google.com/docs/cloud-messaging/http-server-ref (see chapter "Downstream message error response codes"). • Problems on the proxy server side (if you use proxy server). Read the HTTP code in the details of the event and respond accordingly. 	90 days
Failed to send the FCM message to the FCM server	4140	KLSRV_GCM_GENERAL_ERROR	<p>Events of this type occur due to unexpected errors on the Administration Server side when working with the Google Firebase Cloud Messaging HTTP protocol.</p> <p>Read the details in the event description and respond accordingly.</p> <p>If you cannot find the solution to an issue on your own, we recommend that you contact Kaspersky Technical Support.</p>	90 days

Event type display name	Event type ID	Event type	Description	Default storage term
Little free space on the hard drive	4105	KLSRV_NO_SPACE_ON_VOLUMES	Events of this type occur when the hard drive of the device on which Administration Server is installed almost runs out of free space. Free up disk space on the device.	90 days

<p>Little free space in the Administration Server database</p>	<p>4106</p>	<p>KLSRV_NO_SPAC E_IN_DATABASE</p>	<p>Events of this type occur if space in the Administration Server database is too limited. If you do not remedy the situation, soon the Administration Server database will reach its capacity and Administration Server will not function.</p> <p>Following are the causes of this event, depending on the DBMS that you use, and the appropriate responses to the event.</p> <p>You use the SQL Server Express Edition DBMS:</p> <ul style="list-style-type: none"> • In SQL Server Express documentation, review the database size limit for the version you use. Probably your Administration Server database is about to reach the database size limit. • Limit the number of events to store in the Administration Server database (see section "Setting the maximum number of events in the event repository" on page 1008). • In the Administration Server database there are too many events sent by the Application Control component. You can change the settings of the Kaspersky Endpoint Security for Windows policy relating to Application Control event storage in the Administration Server database. <p>You use a DBMS other than SQL Server Express Edition:</p> <ul style="list-style-type: none"> • Do not limit the number of events to store in the Administration Server database (see section "Setting the maximum number of events in the event repository" on page 1008) • Reduce the list of events to store in the Administration Server database (see section "Setting the storage term for an event" on page 1305) 	<p>90 days</p>
---	-------------	--	--	----------------

Event type display name	Event type ID	Event type	Description	Default storage term
			Review the information on DBMS selection (see section "Selecting a DBMS" on page 129).	
Connection to the secondary Administration Server has been interrupted	4116	KLSRV_EV_SLAVE_SRV_DISCONNECTED	Events of this type occur when a connection to the secondary Administration Server is interrupted. Read the Kaspersky Event Log on the device where the secondary Administration Server is installed and respond accordingly.	90 days
Connection to the primary Administration Server has been interrupted	4118	KLSRV_EV_MASTER_SRV_DISCONNECTED	Events of this type occur when a connection to the primary Administration Server is interrupted. Read the Kaspersky Event Log on the device where the primary Administration Server is installed and respond accordingly.	90 days
New updates for Kaspersky software modules have been registered	4141	KLSRV_SEAMLESS_UPDATE_REGISTERED	Events of this type occur when Administration Server registers new updates for the Kaspersky software installed on managed devices that require approval to be installed. Approve or decline the updates by using Administration Console (see section "Approving and declining software updates" on page 435) or using Kaspersky Security Center Web Console (see section "Approving and declining software updates" on page 1197).	90 days

Event type display name	Event type ID	Event type	Description	Default storage term
<p>Deletion of events from the database has started because the limit on the number of events was exceeded</p>	4145	KLSRV_EVP_DB_TRUNCATING	<p>Events of this type occur when deletion of old events from the Administration Server database has started after the Administration Server database capacity is reached (see section "Event processing and storage on the Administration Server" on page 610).</p> <p>You can respond to the event in the following ways:</p> <ul style="list-style-type: none"> • Change the maximum number of events stored in the Administration Server database (see section "Setting the maximum number of events in the event repository" on page 1008) • Reduce the list of events to store in the Administration Server database (see section "Setting the storage term for an event" on page 1305) 	Not stored
<p>Events have been deleted from the database because the limit on the number of events was exceeded</p>	4146	KLSRV_EVP_DB_TRUNCATED	<p>Events of this type occur when old events have been deleted from the Administration Server database after the Administration Server database capacity is reached (see section "Event processing and storage on the Administration Server" on page 610).</p> <p>You can respond to the event in the following ways:</p> <ul style="list-style-type: none"> • Change the allowed maximum number of events to be stored in the Administration Server database (see section "Setting the maximum number of events in the event repository" on page 1008) • Reduce the list of events to store in the Administration Server database (see section "Setting the storage term for an event" on page 1305) 	Not stored

See also:

Administration Server critical events	538
Administration Server functional failure events	543
Administration Server informational events	566
Events in Kaspersky Security Center	792

Administration Server informational events

The table below shows the events of Kaspersky Security Center Administration Server that have the **Info** severity level.

Table 51. Administration Server informational events

Event type display name	Event type ID	Event type	Default storage term
Over 90% of the license key is used up	4097	KLSRV_EV_LICENSE_CHECK_90	30 days
New device has been detected	4100	KLSRV_EVENT_HOSTS_NEW_DETECTED	30 days
Device has been automatically added to the group	4101	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	30 days
Device has been removed from the group: inactive on the network for a long time	4104	KLSRV_INVISIBLE_HOSTS_REMOVED	30 days
Limit of installations will soon be exceeded (more than 95% is used up) for one of the licensed applications groups	4128	KLSRV_INVLICPROD_EXPIRED_SOON	30 days
Files have been found to send to Kaspersky for analysis	4131	KLSRV_APS_FILE_APPEARED	30 days
FCM Instance ID has changed on this mobile device	4137	KLSRV_GCM_DEVICE_REGID_CHANGED	30 days
Updates have been successfully copied to the specified folder	4122	KLSRV_UPD_REPL_OK	30 days
Connection to the secondary Administration Server has been established	4115	KLSRV_EV_SLAVE_SRV_CONNECTED	30 days
Connection to the primary Administration Server has been established	4117	KLSRV_EV_MASTER_SRV_CONNECTED	30 days
Databases have been updated	4144	KLSRV_UPD_BASES_UPDATED	30 days
Audit: Connection to the Administration Server has been established	4147	KLAUD_EV_SERVERCONNECT	30 days
Audit: Object has been modified	4148	KLAUD_EV_OBJECTMODIFY	30 days
Audit: Object status has changed	4150	KLAUD_EV_TASK_STATE_CHANGED	30 days
Audit: Group settings have been modified	4149	KLAUD_EV_ADMGROUP_CHANGED	30 days
Audit: Connection to Administration Server has been terminated	4151	KLAUD_EV_SERVERDISCONNECT	30 days
Audit: Object properties have been modified	4152	KLAUD_EV_OBJECTPROPMODIFIED	30 days
Audit: User permissions have been modified	4153	KLAUD_EV_OBJECTACLMODIFIED	30 days

Network Agent events

This section contains information about the events related to Network Agent.

In this section

Network Agent functional failure events	568
Network Agent warning events	571
Network Agent informational events	572

Network Agent functional failure events

The table below shows the events of Kaspersky Security Center Network Agent that have the **Functional failure** severity level.

Table 52. Network Agent functional failure events

Event type display name	Event type ID	Event type	Description	Default storage term
Update installation error	7702	KLNAG_EV_PATCH_INSTALL_ERROR	<p>Events of this type occur if automatic updating and patching for Kaspersky Security Center components (on page 457) was not successful. The event does not concern updates of the managed Kaspersky applications.</p> <p>Read the event description. A Windows issue on the Administration Server might be a reason for this event. If the description mentions any issue of Windows configuration, resolve this issue.</p>	30 days
Failed to install the third-party software update	7697	KLNAG_EV_3P_PATCH_INSTALL_ERROR	<p>Events of this type occur if Vulnerability and Patch Management and Mobile Device Management features (see section "Kaspersky Security Center licensing options" on page 320) are in use, and if update of third-party software (see section "Installation of third-party software updates" on page 432) was not successful.</p> <p>Check whether the link to the third-party software is valid. Read the event description.</p>	30 days

Event type display name	Event type ID	Event type	Description	Default storage term
Failed to install the Windows Update updates	7717	KLNAG_EV_WUA_INSTALL_ERROR	<p>Events of this type occur if Windows Updates were not successful. Configure Windows Updates in a Network Agent policy (see section "Configuring Windows updates in a Network Agent policy" on page 455).</p> <p>Read the event description. Look for the error in the Microsoft Knowledge Base. Contact Microsoft Technical Support if you cannot resolve the issue yourself.</p>	30 days

See also:

Network Agent warning events.....	571
Network Agent informational events.....	572

Network Agent warning events

The table below shows the events of Kaspersky Security Center Network Agent that have the **Warning** severity level.

Table 53. Network Agent warning events

Event type display name	Event type ID	Event type	Default storage term
Warning has been returned during installation of the software module update	7701	KLNAG_EV_PATCH_INSTALL_WARNING	30 days
Third-party software update installation has completed with a warning	7696	KLNAG_EV_3P_PATCH_INSTALL_WARNING	30 days
Third-party software update installation has been postponed	7698	KLNAG_EV_3P_PATCH_INSTALL_SLIPPED	30 days
Incident has occurred	549	GNRL_EV_APP_INCIDENT_OCCURRED	30 days
KSN Proxy has started. Failed to check KSN for availability	7718	KSNPROXY_STARTED_CON_CHECK_FAILED	30 days

See also:

Network Agent functional failure events	568
Network Agent informational events	572

Network Agent informational events

The table below shows the events of Kaspersky Security Center Network Agent that have the **Info** severity level.

Table 54. Network Agent informational events

Event type display name	Event type ID	Event type	Default storage term
Update for software modules has been installed successfully	7699	KLNAG_EV_PATCH_INSTALLED_SUCCESSFULLY	30 days
Installation of the software module update has started	7700	KLNAG_EV_PATCH_INSTALL_STARTING	30 days
Application has been installed	7703	KLNAG_EV_INV_APP_INSTALLED	30 days
Application has been uninstalled	7704	KLNAG_EV_INV_APP_UNINSTALLED	30 days
Monitored application has been installed	7705	KLNAG_EV_INV_OBS_APP_INSTALLED	30 days
Monitored application has been uninstalled	7706	KLNAG_EV_INV_OBS_APP_UNINSTALLED	30 days
Third-party application has been installed	7707	KLNAG_EV_INV_CMPTR_APP_INSTALLED	30 days
New device has been added	7708	KLNAG_EV_DEVICE_ARRIVAL	30 days
Device has been removed	7709	KLNAG_EV_DEVICE_REMOVE	30 days
New device has been detected	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30 days
Device has been authorized	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	30 days
Windows Desktop Sharing: File has been read	7712	KLUSRLOG_EV_FILE_READ	30 days
Windows Desktop Sharing: File has been modified	7713	KLUSRLOG_EV_FILE_MODIFIED	30 days
Windows Desktop Sharing: Application has been started	7714	KLUSRLOG_EV_PROCESS_LAUNCHED	30 days
Windows Desktop Sharing: Started	7715	KLUSRLOG_EV_WDS_BEGIN	30 days
Windows Desktop Sharing: Stopped	7716	KLUSRLOG_EV_WDS_END	30 days
Third-party software update has been installed successfully	7694	KLNAG_EV_3P_PATCH_INSTALLED_SUCCESSFULLY	30 days
Third-party software update installation has started	7695	KLNAG_EV_3P_PATCH_INSTALL_STARTING	30 days
KSN Proxy has started. KSN availability check has completed successfully	7719	KSNPROXY_STARTED_CON_CHK_OK	30 days

Event type display name	Event type ID	Event type	Default storage term
KSN Proxy has stopped	7720	KSNPROXY_STOPPED	30 days

See also:

Network Agent functional failure events	568
Network Agent warning events	571

iOS MDM Server events

This section contains information about the events related to iOS MDM Server.

In this section

iOS MDM Server functional failure events.....	575
iOS MDM Server warning events	578
iOS MDM Server informational events	578

iOS MDM Server functional failure events

The table below shows the events of Kaspersky Security Center iOS MDM Server that have the **Functional failure** severity level.

Table 55. *iOS MDM Server functional failure events*

Event type display name	Event type ID	Event type	Default storage term
Failed to request the list of profiles.		PROFILELIST_COMMAND_FAILED	30 days
Failed to install the profile.		INSTALLPROFILE_COMMAND_FAILED	30 days
Failed to remove the profile.		REMOVEPROFILE_COMMAND_FAILED	30 days
Failed to request the list of provisioning profiles.		PROVISIONINGPROFILELIST_COMMAND_FAILED	30 days
Failed to install provisioning profile.		INSTALLPROVISIONINGPROFILE_COMMAND_FAILED	30 days
Failed to remove the provisioning profile.		REMOVEPROVISIONINGPROFILE_COMMAND_FAILED	30 days
Failed to request the list of digital certificates.		CERTIFICATELIST_COMMAND_FAILED	30 days
Failed to request the list of installed applications.		INSTALLEDAPPLICATIONLIST_COMMAND_FAILED	30 days
Failed to request general information about the mobile device.		DEVICEINFORMATION_COMMAND_FAILED	30 days
Failed to request security information.		SECURITYINFO_COMMAND_FAILED	30 days
Failed to lock the mobile device.		DEVICELOCK_COMMAND_FAILED	30 days
Failed to reset the password.		CLEARPASSCODE_COMMAND_FAILED	30 days
Failed to wipe data from the mobile device.		ERASEDEVICE_COMMAND_FAILED	30 days
Failed to install the app.		INSTALLAPPLICATION_COMMAND_FAILED	30 days
Failed to set the redemption code for the app.		APPLYREDEMPTIONCODE_COMMAND_FAILED	30 days
Failed to request the list of managed apps.		MANAGEDAPPLICATIONLIST_COMMAND_FAILED	30 days
Failed to remove the managed app.		REMOVEAPPLICATION_COMMAND_FAILED	30 days
Roaming settings have been rejected.		SETROAMINGSETTINGS_COMMAND_FAILED	30 days
Error has occurred in the app operation.		PRODUCT_FAILURE	30 days
Command result contains invalid data.		MALFORMED_COMMAND	30 days
Failed to send the push notification.		SEND_PUSH_NOTIFICATION_FAILED	30 days

Event type display name	Event type ID	Event type	Default storage term
Failed to send the command.		SEND_COMMAND_FAILED	30 days
Device not found.		DEVICE_NOT_FOUND	30 days

iOS MDM Server warning events

The table below shows the events of Kaspersky Security Center iOS MDM Server that have the **Warning** severity level.

Table 56. iOS MDM Server warning events

Event type display name	Event type ID	Event type	Default storage term
Attempt to connect a locked mobile device has been detected.		INACTICE_DEVICE_TRY_CONNECTED	30 days
Profile has been removed.		MDM_PROFILE_WAS_REMOVED	30 days
Attempt to re-use a client certificate has been detected.		CLIENT_CERT_ALREADY_IN_USE	30 days
Inactive device has been detected.		FOUND_INACTIVE_DEVICE	30 days
Redemption code is required.		NEED_REDEMPTION_CODE	30 days
Profile has been included in a policy removed from the device.		UMDM_PROFILE_WAS_REMOVED	30 days

iOS MDM Server informational events

The table below shows the events of Kaspersky Security Center iOS MDM Server that have the **Info** severity level.

Table 57. iOS MDM Server informational events

Event type display name	Event type ID	Event type	Default storage term
New mobile device has been connected.		NEW_DEVICE_CONNECTED	30 days
List of profiles has been successfully requested.		PROFILELIST_COMMAND_SUCCESSFULL	30 days
Profile has been successfully installed.		INSTALLPROFILE_COMMAND_SUCCESSFULL	30 days
Profile has been successfully removed.		REMOVEPROFILE_COMMAND_SUCCESSFULL	30 days
List of provisioning profiles has been successfully requested.		PROVISIONINGPROFILELIST_COMMAND_SUCCESSFULL	30 days
Provisioning profile has been successfully installed.		INSTALLPROVISIONINGPROFILE_COMMAND_SUCCESSFULL	30 days
Provisioning profile has been successfully removed.		REMOVEPROVISIONINGPROFILE_COMMAND_SUCCESSFULL	30 days
List of digital certificates has been successfully requested.		CERTIFICATELIST_COMMAND_SUCCESSFULL	30 days
List of installed applications has been successfully requested.		INSTALLEDAPPLICATIONLIST_COMMAND_SUCCESSFULL	30 days
General information about the mobile device has been successfully requested.		DEVICEINFORMATION_COMMAND_SUCCESSFULL	30 days
Security information has been successfully requested.		SECURITYINFO_COMMAND_SUCCESSFULL	30 days
Mobile device has been successfully locked.		DEVICELOCK_COMMAND_SUCCESSFULL	30 days
The password has been successfully reset.		CLEARPASSCODE_COMMAND_SUCCESSFULL	30 days
Data has been wiped from the mobile device.		ERASEDEVICE_COMMAND_SUCCESSFULL	30 days
App has been successfully installed.		INSTALLAPPLICATION_COMMAND_SUCCESSFULL	30 days
Redemption code has been successfully set for the app.		APPLYREDEMPTIONCODE_COMMAND_SUCCESSFULL	30 days
The list of managed apps has been successfully requested.		MANAGEDAPPLICATIONLIST_COMMAND_SUCCESSFULL	30 days
Managed app has been removed successfully.		REMOVEAPPLICATION_COMMAND_SUCCESSFULL	30 days
Roaming settings have been successfully applied.		SETROAMINGSETTINGS_COMMAND_SUCCESSFUL	30 days

Exchange Mobile Device Server events

This section contains information about the events related to Exchange Mobile Device Server.

In this section

Exchange Mobile Device Server functional failure events	581
Exchange Mobile Device Server informational events	581

Exchange Mobile Device Server functional failure events

The table below shows the events of Kaspersky Security Center Exchange Mobile Device Server that have the **Functional failure** severity level.

Table 58. Exchange Mobile Device Server functional failure events

Event type display name	Event type ID	Event type	Default storage term
Failed to wipe data from the mobile device.		WIPE_FAILED	30 days
Cannot delete information about mobile device connection to mailbox.		DEVICE_REMOVE_FAILED	30 days
Failed to apply the ActiveSync policy to the mailbox.		POLICY_APPLY_FAILED	30 days
Application operation error.		PRODUCT_FAILURE	30 days
Failed to modify the state of ActiveSync functionality.		CHANGE_ACTIVE_SYNC_STATE_FAILED	30 days

Exchange Mobile Device Server informational events

The table below shows the events of Kaspersky Security Center Exchange Mobile Device Server that have the **Info** severity level.

Table 59. Exchange Mobile Device Server informational events

Event type display name	Event type ID	Event type	Default storage term
New mobile device has connected.		NEW_DEVICE_CONNECTED	30 days
Data has been wiped from the mobile device.		WIPE_SUCCESSFULL	30 days

Blocking frequent events

This section provides information about managing frequent events blocking, about removing blocking of frequent events, and about exporting the list of frequent events to a file.

In this section

About blocking frequent events	582
Managing frequent events blocking.....	583
Removing blocking of frequent events	583
Exporting a list of frequent events to a file.....	583

About blocking frequent events

A managed application, for example, Kaspersky Endpoint Security for Windows, installed on a single or several managed devices can send a lot of events of the same type to the Administration Server. Receiving frequent events may overload the Administration Server database and overwrite other events. Administration Server starts blocking the most frequent events when the number of all the received events exceeds the specified limit for the database (see section "Setting the maximum number of events in the event repository" on page [1008](#)).

Administration Server blocks the frequent events from receiving automatically. You cannot block the frequent events yourself, or choose which events to block.

If you want to find out if an event is blocked, you can see if this event is present in the **Blocking frequent events** section of the Administration Server properties. If the event is blocked, you can do the following:

- If you want to prevent overwriting the database, you can continue blocking (see section "Managing frequent events blocking" on page [583](#)) such type of events from receiving.
- If you want, for example, to find the reason of sending the frequent events to the Administration Server you can unblock (see section "Managing frequent events blocking" on page [583](#)) frequent events and continue receiving the events of this type anyway.
- If you want to continue receiving the frequent events until they become blocked again, you can remove from blocking (see section "Removing blocking of frequent events" on page [583](#)) the frequent events.

Managing frequent events blocking

Administration Server automatically blocks the receiving of frequent events, but you can stop blocking and continue to receive frequent events. You can also block the receiving of frequent events that you unblocked before.

► *To manage frequent events blocking:*

1. In the Kaspersky Security Center console tree, open the context menu of the **Administration Server** folder, and then select **Properties**.
2. In the Administration Server properties window, go to the **Sections** pane, and then select **Blocking frequent events**.
3. In the **Blocking frequent events** section:
 - Select the **Event type** options of the events that you want to block from being received.
 - Unselect the **Event type** options of the events that you want to continue receiving.
4. Click the **Apply** button.
5. Click the **OK** button.

Administration Server receives the frequent events for which you unselected the option **Event type** and blocks receiving frequent events for which you selected the option **Event type**.

Removing blocking of frequent events

You can remove blocking for frequent events and start receiving them until Administration Server blocks this type of frequent events again.

► *To remove the blocking of frequent events:*

1. In the Kaspersky Security Center console tree, open the context menu of the **Administration Server** folder, and then select **Properties**.
2. In the Administration Server properties window, go to the **Sections** pane, and then select **Blocking frequent events**.
3. In the **Blocking frequent events** section, click the row of the frequent event for which you want to remove blocking.
4. Click the **Delete** button.

The frequent event is removed from the list of the frequent events. Administration Server will receive events of this type.

Exporting a list of frequent events to a file

► *To export a list of frequent events to a file:*

1. In the Kaspersky Security Center console tree, open the context menu of the **Administration Server** folder, and then select **Properties**.

2. In the Administration Server properties window, go to the **Sections** pane, and then select **Blocking frequent events**.
3. Click the **Export to file** button.
4. In the **Save as** window that opens, specify the path to the file to which you want to save the list.
5. Click the **Save** button.

All the records on the frequent events list are exported to a file.

Controlling changes in the status of virtual machines

Administration Server stores information about the status of managed devices, such as the hardware registry and the list of installed applications, and the settings of managed applications, tasks and policies. If a virtual machine functions as a managed device, the user can restore its status at any time using a previously created snapshot of the virtual machine. Information about the status of the virtual machine on Administration Server may become outdated.

For example, the administrator had created a protection policy on Administration Server at 12:00 P.M., which started to run on virtual machine VM_1 at 12:01 P.M. At 12:30 P.M., the user of virtual machine VM_1 changed its status by restoring it from a snapshot made at 11:00 A.M. The protection policy stops running on the virtual machine. However, outdated information stored on Administration Server states that the protection policy on virtual machine VM_1 continues.

Kaspersky Security Center allows you to monitor changes in the status of virtual machines.

After each synchronization with a device, the Administration Server generates a unique ID that is stored on the device and on the Administration Server. Before starting the next synchronization, Administration Server compares the values of those IDs on both sides. If the values of the IDs do not match, Administration Server recognizes the virtual machine as restored from a snapshot. Administration Server resets all the settings of policies and tasks that are active for the virtual machine and sends it the up-to-date policies and the list of group tasks.

Monitoring the anti-virus protection status using information from the system registry

► *To monitor the anti-virus protection status on a client device using information logged by Network Agent, depending on the operating system of the device:*

- On the devices running Windows:
 1. Open the system registry of the client device (for example, locally, using the regedit command in the **Start** → **Run** menu).
 2. Go to the following hive:

- 32-bit systems:

```
HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1103\1.0.0.0\Statistics\AVState
```

- 64-bit systems:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1103\1.0.0.0\Statistics\AVState
```

The system registry displays information about the anti-virus protection status of the client device.

- On the devices running Linux:
 - Information is enclosed in separate text files, one for each type of data, located at `/var/opt/kaspersky/klagent/1103/1.0.0.0/Statistics/AVState/`.
- On the devices running macOS:
 - Information is enclosed in separate text files, one for each type of data, located at `/Library/Application Support/Kaspersky Lab/klagent/Data/1103/1.0.0.0/Statistics/AVState/`.

The anti-virus protection status corresponds to the values of the keys described in the table below.

Table 60. Registry keys and their possible values

Key (data type)	Value	Description
Protection_LastConnected (REG_SZ)	DD-MM-YYYY HH-MM-SS	Date and time (in UTC format) of the last connection to the Administration Server
Protection_AdmServer (REG_SZ)	IP, DNS name, or NetBIOS name	Name of the Administration Server that manages the device
Protection_NagentVersion (REG_SZ)	a.b.c.d	Build number of the Network Agent installed on the device
Protection_NagentFullVersion (REG_SZ)	a.b.c.d (patch1; patch2; ...; patchN)	Full number of the Network Agent version (with patches) installed on the device
Protection_HostId (REG_SZ)	Device ID	ID of the device
Protection_DynamicVM (REG_DWORD)	0 — no 1 — yes	The Network Agent is installed in the dynamic VDI mode
Protection_AvInstalled (REG_DWORD)	0 — no 1 — yes	A security application is installed on the device
Protection_AvRunning (REG_DWORD)	0 — no 1 — yes	Real-time protection is enabled on the device
Protection_HasRtp (REG_DWORD)	0 — no 1 — yes	A real-time protection component is installed
Protection_RtpState (REG_DWORD)	Real-time protection status:	
	0	Unknown
	1	Disabled
	2	Paused
	3	Starting
	4	Enabled
	5	Enabled with the high protection level (maximum protection)

Key (data type)	Value	Description
	6	Enabled with the low protection level (maximum speed)
	7	Enabled with the default (recommended) settings
	8	Enabled with custom settings
	9	Operation failure
Protection_LastFscan (REG_SZ)	DD-MM-YYYY HH-MM-SS	Date and time (in UTC format) of the last full scan
Protection_BasesDate (REG_SZ)	DD-MM-YYYY HH-MM-SS	Date and time (in UTC format) of the application databases release

Viewing and configuring the actions when devices show inactivity

If client devices within a group are inactive, you can get notifications about it. You can also automatically delete such devices.

► *To view or configure the actions when the devices in the group show inactivity:*

1. In the console tree, right-click the name of the required administration group.
2. In the context menu, select **Properties**.
This opens the administration group properties window.
3. In the Properties window, go to the **Devices** section.
4. If needed, enable or disable the following options:

- **Notify the administrator if the device has been inactive for longer than (days)**

If this option is enabled, the administrator receives notifications about inactive devices. You can specify the time interval after which the **Device has remained inactive on the network in a long time** event is created. The default time interval is 7 days.

By default, this option is enabled.

- **Remove the device from the group if it has been inactive for longer than (days)**

If this option is enabled, you can specify the time interval after which the device is automatically removed from the group. The default time interval is 60 days.

By default, this option is enabled.

- **Inherit from parent group**

The settings in this section will be inherited from the parent group in which the client device is included. If this option is enabled, the settings under **Device activity on the network** are locked from any changes.

This option is available only if the administration group has a parent group.

By default, this option is enabled.

- **Force inheritance in child groups**

The setting values will be distributed to child groups but in the properties of the child groups these settings are locked.

By default, this option is disabled.

1. Click **OK**.

Your changes are saved and applied.

Adjustment of distribution points and connection gateways

A structure of administration groups in Kaspersky Security Center performs the following functions:

- Sets the scope of policies

There is an alternate way of applying relevant collections of settings on devices, by using *policy profiles*. In this case, the scope of policies is set with tags, device locations in Active Directory organizational units, membership in Active Directory security groups, etc (see section "Hierarchy of policies, using policy profiles" on page [385](#)).

- Sets the scope of group tasks

There is an approach to defining the scope of group tasks that is not based on a hierarchy of administration groups: use of tasks for device selections and tasks for specific devices.

- Sets access rights to devices, virtual Administration Servers, and secondary Administration Servers

- Assigns distribution points

When building the structure of administration groups, you must take into account the topology of the organization's network for the optimum assignment of distribution points. The optimum distribution of distribution points allows you to save traffic on the organization's network.

Depending on the organizational schema and network topology, the following standard configurations can be applied to the structure of administration groups:

- Single office
- Multiple small remote offices

Devices functioning as distribution points must be protected, including physical protection, against any unauthorized access.

In this section

Standard configuration of distribution points: Single office.....	588
Standard configuration of distribution points: Multiple small remote offices.....	588
Assigning a managed device to act as a distribution point.....	589
Connecting a new network segment by using Linux devices	590
Connecting a Linux device as a gateway in the demilitarized zone	590
Connecting a Linux device to the Administration Server via a connection gateway	591
Adding a connection gateway in the DMZ as a distribution point.....	592
Assigning distribution points automatically	593
Local installation of Network Agent on a device selected as distribution point	593
Using a distribution point as connection gateway	594
Adding IP ranges to the scanned ranges list of a distribution point	594

Standard configuration of distribution points: Single office

In a standard "single-office" configuration, all devices are on the organization's network so they can "see" each other. The organization's network may consist of a few separate parts (networks or network segments) linked by narrow channels.

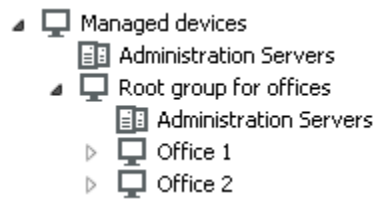
The following methods of building the structure of administration groups are possible:

- Building the structure of administration groups taking into account the network topology. The structure of administration groups may not reflect the network topology with absolute precision. A match between the separate parts of the network and certain administration groups would be enough. You can use automatic assignment of distribution points or assign them manually.
- Building the structure of administration groups, without taking the network topology into account. In this case, you must disable automatic assignment of distribution points, and then assign one or several devices to act as distribution points for a root administration group in each of the separate parts of the network, for example, for the **Managed devices** group. All distribution points will be at the same level and will feature the same scope spanning all devices on the organization's network. In this case, each Network Agent in version 10 Service Pack 1 or later will connect to the distribution point that has the shortest route. The route to a distribution point can be traced with the tracert utility.

Standard configuration of distribution points: Multiple small remote offices

This standard configuration provides for a number of small remote offices, which may communicate with the head office over the Internet. Each remote office is located behind the NAT, that is, connection from one remote office to another is not possible because offices are isolated from one another.

The configuration must be reflected in the structure of administration groups: a separate administration group must be created for each remote office (groups **Office 1** and **Office 2** in the figure below).



One or multiple distribution points must be assigned to each administration group that correspond to an office. Distribution points must be devices at the remote office that have a sufficient amount of free disk space. Devices deployed in the **Office 1** group, for example, will access distribution points assigned to the **Office 1** administration group.

If some users move between offices physically, with their laptops, you must select two or more devices (in addition to the existing distribution points) in each remote office and assign them to act as distribution points for a top-level administration group (**Root group for offices** in the figure above).

Example: A laptop is deployed in the **Office 1** administration group and then is moved physically to the office that corresponds to the **Office 2** administration group. After the laptop is moved, Network Agent attempts to access the distribution points assigned to the **Office 1** group, but those distribution points are unavailable. Then, Network Agent starts attempting to access the distribution points that have been assigned to the **Root group for offices**. Because remote offices are isolated from one another, attempts to access distribution points assigned to the **Root group for offices** administration group will only be successful when Network Agent attempts to access distribution points in the **Office 2** group. That is, the laptop will remain in the administration group that corresponds to the initial office, but the laptop will use the distribution point of the office where it is physically located at the moment.



Assigning a managed device to act as a distribution point

You can manually assign a device to act as a distribution point for an administration group and configure it as a connection gateway in Administration Console.

► *To assign a device as distribution point of an administration group:*

1. In the console tree, select the **Administration Server** node.
2. In the context menu of Administration Server, select **Properties**.
3. In the Administration Server properties window, select the **Distribution points** section.
4. In the right part of the window, select the **Manually assign distribution points** option.
5. Click the **Add** button.

This opens the **Add distribution point** window.

6. In the **Add distribution point** window, perform the following actions:
 - a. Under **Device to act as distribution point**, click the down arrow  on the **Select** split button and select the **Add device from group** option.
 - b. In the **Select devices** window that opens, select the device to act as a distribution point.
 - c. Under **Distribution point scope**, click the down arrow  on the **Select** split button.
 - d. Indicate the specific devices to which the distribution point will distribute updates. You can specify an administration group or a network location description.

- e. Click **OK** to close the **Add distribution point** window.

The distribution point that you have added will be displayed in the list of distribution points, in the **Distribution points** section.

The first device with Network Agent installed that connects to the virtual Administration Server will be automatically assigned to act as distribution point and configured as connection gateway.

See also:

Adding a connection gateway in the DMZ as a distribution point.....[592](#)

Connecting a new network segment by using Linux devices

You can connect a new network segment on a Linux device. You need at least two different devices. One device, you can configure as connection gateway in the DMZ; and the other device, you can configure as a distribution point.

Follow the procedure described in this section only after you have completed the main installation scenario (see section "Main installation scenario" on page [59](#)).

► *To connect a new network segment on a Linux device:*

1. Connect a Linux device as a gateway in the DMZ (see section "Connecting a Linux device as a gateway in the demilitarized zone" on page [590](#)).
2. Connect a Linux device to the Administration Server via a connection gateway (see section "Connecting a Linux device to the Administration Server via a connection gateway" on page [591](#)).

Connecting a new network segment on a Linux device is configured.

See also:

Distribution point.....[55](#)

Usage of Network Agent for Windows, for macOS and for Linux: comparison.....[942](#)

Connecting a Linux device as a gateway in the demilitarized zone



► *To connect a Linux device as a gateway in the demilitarized zone (DMZ):*

1. Download and install Network Agent on the Linux device (see section "Installing Network Agent for Linux in silent mode (with an answer file)" on page [180](#)).
2. Run the post-install script and follow the wizard in order to setup the local environment configuration. In the command prompt, run the following command:

```
$ sudo /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl
```

3. On the step asking for the Network Agent mode, choose the **Use as connection gateway** option.
4. In the Administration Server properties window that opens, select the **Distribution points** section.
5. In the **Distribution points** window that opens, in the right part of the window:
 - a. Select the **Manually assign distribution points** option.
 - b. Click the **Add** button.

This opens the **Add distribution point** window.

6. In the **Add distribution point** window, perform the following actions:
 - a. Under **Device to act as distribution point**, click the down arrow  on the **Select** split button, and then select the **Add connection gateway in DMZ by address** option.
 - b. Under **Distribution point scope**, click the down arrow  on the **Select** split button.
 - c. Indicate the specific devices to which the distribution point will distribute updates. You can specify an administration group.
 - d. Click **OK** to close the **Add distribution point** window.
7. The distribution point that you have added will be displayed in the list of distribution points, in the **Distribution points** section.
8. Run the `klnagchk` utility in order to check whether a connection to Kaspersky Security Center has been successfully configured. In the command prompt, run:


```
$ sudo /opt/kaspersky/klnagent64/bin/klnagchk
```
9. In the main application window, go to Kaspersky Security Center and discover the device (see section "Device discovery" on page [304](#)).
10. In the window that opens, click the <Device name>.
11. In the drop-down list, select the **Move to Group** link.
12. In the **Select group** window that opens, click the **Distribution points** link.
13. Click **OK**.
14. Restart the Network Agent service on the Linux client by executing the following command in the command prompt:

```
$ sudo /opt/kaspersky/klnagent64/bin/klnagchk -restart
```

Connecting a Linux device as a gateway in the DMZ is completed.

Connecting a Linux device to the Administration Server via a connection gateway

► *To connect a Linux device to the Administration Server via a connection gateway, perform the following actions on this device:*

1. Download and install Network Agent on the Linux device (see section "Installing Network Agent for Linux in silent mode (with an answer file)" on page [180](#)).
2. Run the Network Agent post-install script by executing the following command in the command prompt:

```
$ sudo /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl
```

3. On the step asking for the Network Agent mode, choose the **Connect to server using connection gateway** option and enter the address of connection gateway.
4. Check the connection with Kaspersky Security Center and the connection gateway, by using the following command in the command prompt:

```
$ sudo /opt/kaspersky/klnagent64/bin/klnagchk
```

The address of connection gateway is displayed in the output.

Connecting a Linux device to the Administration Server via a connection gateway is completed. You can use this device to update distribution, for remote installation of applications, and to retrieve information about networked devices.



Adding a connection gateway in the DMZ as a distribution point

A connection gateway (on page [57](#)) waits for connections from Administration Server, rather than establishes connections to Administration Server. It means that right after a connection gateway is installed on a device in the DMZ, Administration Server does not list the device among managed devices. Therefore, you need a special procedure to ensure that Administration Server initiates a connection to the connection gateway.

► *To add a device with a connection gateway as a distribution point:*

1. In the console tree, select the **Administration Server** node.
2. In the context menu of Administration Server, select **Properties**.
3. In the Administration Server properties window, select the **Distribution points** section.
4. In the right part of the window, select the **Manually assign distribution points** option.
5. Click the **Add** button.

This opens the **Add distribution point** window.

6. In the **Add distribution point** window, perform the following actions:
 - a. Under **Device to act as distribution point**, click the down arrow  on the **Select** split button, and then select the **Add connection gateway in DMZ by address** option.
 - b. In the **Enter connection gateway address** window that opens, enter the IP address of the connection gateway (or enter the name if the connection gateway is accessible by name).
 - c. Under **Distribution point scope**, click the down arrow  on the **Select** split button.
 - d. Indicate the specific devices to which the distribution point will distribute updates. You can specify an administration group or a network location description.

We recommend that you have a separate group for external managed devices.

After you perform these actions, the list of distribution points contains a new entry named **Temporary entry for connection gateway**.

Administration Server almost immediately attempts to connect to the connection gateway at the address that you specified. If it succeeds, the entry name changes to the name of the connection gateway device. This process takes up to five minutes.

While the temporary entry for the connection gateway is being converted to a named entry, the connection gateway also appears in the **Unassigned devices** group.

See also:

Assigning a managed device to act as a distribution point [589](#)

Assigning distribution points automatically

We recommend that you opt to assign distribution points automatically. Kaspersky Security Center will then select on its own which devices must be assigned distribution points.

► *To assign distribution points automatically:*

1. Open the main application window.
2. In the console tree, select the node with the name of the Administration Server for which you want to assign distribution points automatically.
3. In the context menu of the Administration Server, click **Properties**.
4. In the Administration Server properties window, in the **Sections** pane select **Distribution points**.
5. In the right part of the window, select the **Automatically assign distribution points** option.

If automatic assignment of devices as distribution points is enabled, you cannot configure distribution points manually or edit the list of distribution points.

6. Click **OK**.

Administration Server assigns and configures distribution points automatically.

Local installation of Network Agent on a device selected as distribution point

To allow the device selected as the distribution point to directly communicate with the virtual Administration Server in order to act as connection gateway, the Network Agent must be installed locally on this device.

The procedure of local installation of Network Agent on the device defined as distribution point is the same as local installation of Network Agent on any network device.

The following conditions must be met for a device selected as a distribution point:

- During local installation of Network Agent, specify the address of a virtual Administration Server that manages the device in the **Server Address** field in the **Administration Server** window of the Setup Wizard. You can use either the device IP address or device name in the Windows network.
The following format is used for the virtual Administration Server address: <Full address of the physical Administration Server to which the virtual Server is subordinate>/<Name of virtual Administration Server>.
- So that it can act as connection gateway, open all ports of the device that are necessary for communication with the Administration Server.

After Network Agent with specified settings is installed on a device, Kaspersky Security Center performs the following actions automatically:

- Includes this device in the **Managed devices** group of the virtual Administration Server.
- Assigns this device as the distribution point of the **Managed devices** group of the virtual Administration Server.

It is necessary and sufficient to install Network Agent locally on the device that is assigned as the distribution point for the **Managed devices** group on the organization's network. You can install Network Agent remotely on devices that act as distribution points in the nested administration groups. To do this, use the distribution point of the **Managed devices** group as connection gateway.

See also:

Local installation of Network Agent	178
Kaspersky applications. Centralized deployment	332

Using a distribution point as connection gateway

If the Administration Server is outside the demilitarized zone (DMZ), Network Agents from this zone cannot connect to the Administration Server.

When connecting the Administration Server with Network Agents, you can use a distribution point as the connection gateway. The distribution point opens a port to Administration Server for the connection to be created. When the Administration Server is started, it connects to that distribution point and maintains this connection during the entire session.

Upon receiving a signal from the Administration Server, the distribution point sends a UDP signal to the Network Agents in order to allow connection to the Administration Server. When the Network Agents receive that signal, they connect to the distribution point, which exchanges information between them and the Administration Server.

We recommend that you use a specially assigned device as the connection gateway and cover a maximum of 10 000 client devices (including mobile devices) with this connection gateway.

See also:

Assigning a managed device to act as a distribution point.....	589
Local installation of Network Agent	178

Adding IP ranges to the scanned ranges list of a distribution point

You can add IP ranges to the list of scanned ranges of a distribution point.

► *To add an IP range to the list of scanned ranges:*

1. In the console tree, select the **Administration Server** node.
2. In the context menu of the node, select **Properties**.

This opens the Administration Server properties window.

3. In the Administration Server properties window, select the **Distribution points** section.
4. In the list, select the necessary distribution point and click **Properties**.

This opens the distribution point properties window.

5. In the window that opens, in the left **Sections** pane, select **Device discovery** → **IP ranges**.
6. Select the **Enable range polling** check box.
7. Click the **Add** button.

The **Add** button is active only if you select the **Enable range polling** check box.

The **IP range** window opens.

8. In the **IP range** window, enter the name of the new IP range (the default name is New range).
9. Click the **Add** button.
10. Do one of the following:
 - Specify the IP range using the start and end IP addresses.
 - Specify the IP range using the address and subnet mask.
 - Click **Browse** and add a subnet from the global list of subnets (on page [941](#)).

11. Click **OK**.

12. Click **OK** to add the new range with the specified name.

The new range will appear in the list of scanned ranges.

Other routine tasks

This section provides recommendations on routine work with Kaspersky Security Center.

In this chapter

Managing Administration Servers.....	596
Managing administration groups	630
Managing client devices	635
Managing user accounts.....	678
Remote installation of operating systems and applications.....	712
Managing object revisions	719
Deletion of objects	725
Mobile Device Management	727
Data encryption and protection.....	768
Data repositories.....	774
Kaspersky Security Network (KSN)	785
Switching between Online Help and Offline Help	791

Managing Administration Servers

This section provides information about working with Administration Servers and configuring them.

In this section

Creating a hierarchy of Administration Servers: adding a secondary Administration Server.....	597
Connecting to an Administration Server and switching between Administration Servers	600
Access rights to Administration Server and its objects.....	601
Conditions of connection to an Administration Server over the Internet	602
Encrypted connection to an Administration Server	603
Disconnecting from an Administration Server	605
Adding an Administration Server to the console tree	605
Removing an Administration Server from the console tree	605
Adding a virtual Administration Server to the console tree.....	605
Changing an Administration Server service account. Utility tool klsrvswch	606
Changing DBMS credentials	607
Resolving issues with Administration Server nodes	608
Viewing and modifying the settings of an Administration Server	608
Backup and restoration of Administration Server settings.....	615
Backup copying and restoration of Administration Server data.....	617
Avoiding conflicts between multiple Administration Servers	623
Two-step verification.....	623

Creating a hierarchy of Administration Servers: adding a secondary Administration Server

You can add an Administration Server as a secondary Administration Server thus running a "primary / secondary" hierarchy. Adding a secondary Administration Server is possible regardless of whether the Administration Server that you intend to use as secondary is available for connection through Administration Console.

When combining two Administration Servers into a hierarchy, make sure that port 13291 is accessible on both Administration Servers. Port 13291 is required to receive connections from Administration Console to the Administration Server (see section "Administration Server and Administration Console" on page [111](#)).

Connecting an Administration Server as secondary in reference to the primary Administration Server

You can add an Administration Server as secondary by connecting it to the primary Administration Server via port 13000. You will need a device that has Administration Console installed from which TCP ports 13291 can be accessed on both Administration Servers: supposed primary Administration Server and supposed secondary Administration Server.

► *To add as secondary an Administration Server that is available for connection through Administration Console:*

1. Make sure that port 13000 of the supposed primary Administration Server is available for receipt of connections from secondary Administration Servers.

2. Use Administration Console to connect to the supposed primary Administration Server.
3. Select the administration group to which you intend to add the secondary Administration Server.
4. In the workspace of the **Administration Servers** node of the selected group, click the **Add secondary Administration Server** link.

The Add Secondary Administration Server Wizard starts.

5. At the first step of the Wizard (entering the address of the Administration Server being added to the group), enter the network name of the supposed secondary Administration Server.
6. Follow the instructions of the Wizard.

The "primary / secondary" hierarchy is built. The primary Administration Server will receive connection from the secondary Administration Server (see section "Hierarchy of Administration Servers: primary Administration Server and secondary Administration Server" on page [114](#)).

If you do not have a device that has Administration Console installed from which TCP ports 13291 can be accessed on both Administration Servers (if, for example, the supposed secondary Administration Server is located at a remote office and the system administrator of that office cannot open Internet access to port 13291 for security reasons), you will still be able to add a secondary Administration Server.

► *To add as secondary an Administration Server that is not available for connection through Administration Console:*

1. Make sure that port 13000 of the supposed primary Administration Server is available for connection from secondary Administration Servers.
2. Write the certificate file of the supposed primary Administration Server to an external device, such as a flash drive, or send it to the system administrator of the remote office where the Administration Server is located.

The certificate file of the Administration Server is on the same Administration Server, at %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert\klserver.cer.

3. Write the certificate file of the supposed secondary Administration Server to an external device, such as a flash drive. If the supposed secondary Administration Server is located at a remote office, contact the system administrator of that office to prompt him or her to send you the certificate.

The certificate file of the Administration Server is on the same Administration Server, at %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert\klserver.cer.

4. Use Administration Console to connect to the supposed primary Administration Server.
5. Select the administration group to which you intend to add the secondary Administration Server.
6. In the workspace of the **Administration Servers** node, click the **Add secondary Administration Server** link.

The Add Secondary Administration Server Wizard starts.

7. At the first step of the Wizard (entering the address), leave the **Secondary Administration Server address (optional)** field blank.
8. In the **Secondary Administration Server certificate file** window, click the **Browse** button and select the certificate file of the secondary Administration Server that you saved.
9. When the Wizard is complete, use a different instance of Administration Console to connect to the supposed secondary Administration Server. If this Administration Server is located at a remote office, contact the system administrator of that office to prompt him or her to connect to the supposed secondary Administration Server and perform further due steps.

10. In the context menu of the **Administration Server** node, select **Properties**.
11. In the Administration Server properties, proceed to the **Advanced** section and then to the **Hierarchy of Administration Servers** subsection.
12. Select the **This Administration Server is secondary in the hierarchy** check box.
The entry fields become available for data input and editing.
13. In the **Primary Administration Server address** field, enter the network name of the supposed primary Administration Server.
14. Select the previously saved file with the certificate of the supposed primary Administration Server by clicking the **Browse** button.
15. Click **OK**.

The "primary / secondary" hierarchy is built. You can connect to the secondary Administration Server through Administration Console. The primary Administration Server will receive connection from the secondary Administration Server (see section "Hierarchy of Administration Servers: primary Administration Server and secondary Administration Server" on page [114](#)).

Connecting the primary Administration Server to a secondary Administration Server

You can add a new Administration Server as secondary so that the primary Administration Server connects to the secondary Administration Server via port 13000. This is advisable if, for example, you place a secondary Administration Server in DMZ.

You will need a device that has Administration Console installed from which TCP ports 13291 can be accessed on both Administration Servers: supposed primary Administration Server and supposed secondary Administration Server.

► *To add a new Administration Server as secondary and connect the primary Administration Server via port 13000:*

1. Make sure that port 13000 of the supposed secondary Administration Server is available for receipt of connections from the primary Administration Server.
2. Use Administration Console to connect to the supposed primary Administration Server.
3. Select the administration group to which you intend to add the secondary Administration Server.
4. In the workspace of the **Administration Servers** node of the relevant administration group, click the **Add secondary Administration Server** link.
The Add Secondary Administration Server Wizard starts.
5. At the first step of the Wizard (entering the address of the Administration Server to be added to the group), enter the network name of the supposed secondary Administration Server and select the **Connect primary Administration Server to secondary Administration Server in DMZ** check box.
6. If you connect to the supposed secondary Administration Server by using a proxy server, at the first step of the Wizard select the **Use proxy server** check box and specify the connection settings.
7. Follow the instructions of the Wizard.

The hierarchy of Administration Servers is created. The secondary Administration Server will receive connection from the primary Administration Server (see section "Hierarchy of Administration Servers with a secondary Administration Server in DMZ" on page [115](#)).

See also:

Hierarchy of Administration Servers with a secondary Administration Server in DMZ.....	115
Hierarchy of Administration Servers: primary Administration Server and secondary Administration Server.....	114
Ports used by Kaspersky Security Center	65

Connecting to an Administration Server and switching between Administration Servers

After Kaspersky Security Center is started, it attempts to connect to an Administration Server. If several Administration Servers are available on the network, the application requests the server to which it was connected during the previous session of Kaspersky Security Center.

When the application is started for the first time after installation, it attempts to connect to the Administration Server that was specified during Kaspersky Security Center installation.

After connection to an Administration Server is established, the folders tree of that Server is displayed in the console tree.

If several Administration Servers have been added to the console tree, you can switch between them.

Administration Console is required for work with each Administration Server. Before the first connection to a new Administration Server, make sure that port 13291, which receives connections from Administration Console, is open (see section "Administration Server and Administration Console" on page [111](#)), as well as all the remaining ports required for communication between Administration Server and other Kaspersky Security Center components (see section "Ports used by Kaspersky Security Center" on page [65](#)).

► *To switch to another Administration Server:*

1. In the console tree, select the node with the name of the required Administration Server.
2. In the context menu of the node, select **Connect to Administration Server**.
3. In the **Connection settings** window that opens, in the **Administration Server address** field specify the name of the Administration Server to which you want to connect. You can specify an IP address or the name of a device on a Windows network as the name of the Administration Server. You can click the **Advanced** button to configure the connection to the Administration Server (see figure below).

To connect to the Administration Server through a different port than the default port, enter a value in the **Administration Server address** field in <Administration Server name>:<Port> format.

Users who do not have **read** rights will be denied access to Administration Server.

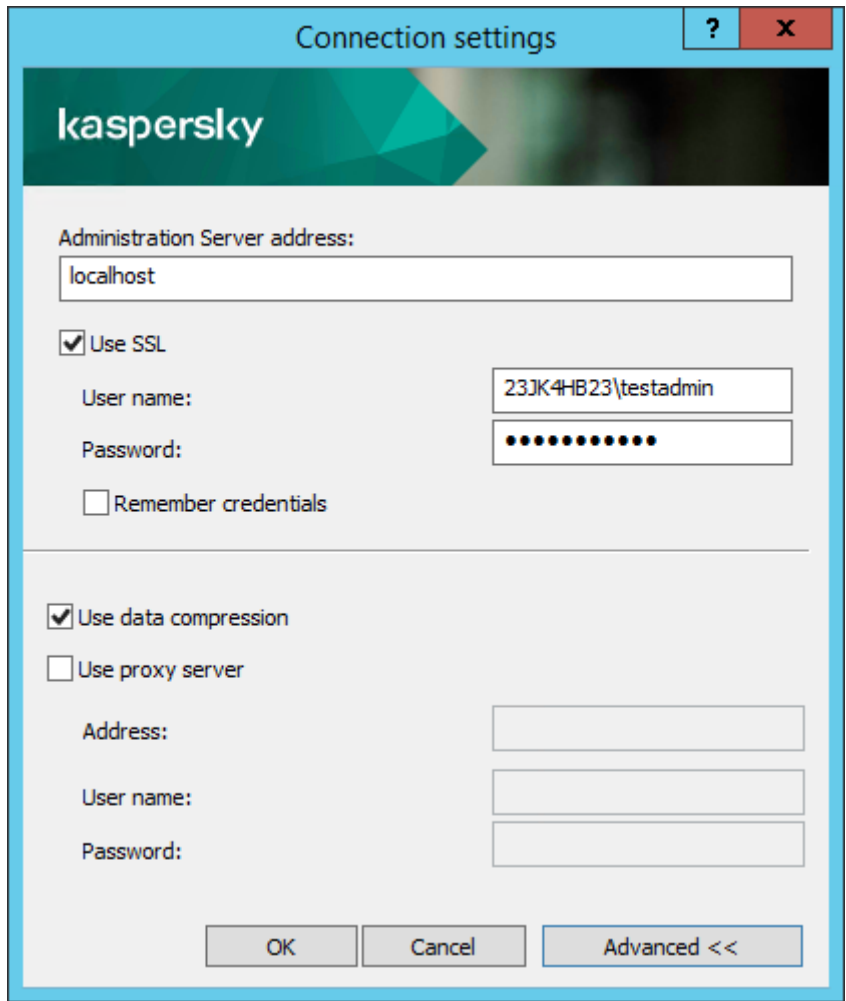


Figure 2. Connecting to Administration Server

4. Click **OK** to complete the switch between Servers.

After the Administration Server is connected, the folders tree of the corresponding node in the console tree is updated.

See also:

Ports used by Kaspersky Security Center	65
Administration Server and Administration Console.....	111

Access rights to Administration Server and its objects

The **KLAdmins** and **KLOperators** groups are created automatically during Kaspersky Security Center installation. These groups are granted permissions to connect to the Administration Server and to process Administration Server objects.

Depending on the type of account that is used for installation of Kaspersky Security Center, the **KLAdmins** and **KLOperators** groups are created as follows:

- If the application is installed under a user account included in a domain, the groups are created on the Administration Server and in the domain that includes the Administration Server.
- If the application is installed under a system account, the groups are created on the Administration Server only.

You can view the **KLAdmins** and **KLOperators** groups and modify the access privileges of the users that belong to the **KLAdmins** and **KLOperators** groups by using the standard administrative tools of the operating system.

The **KLAdmins** group is granted all access rights; the **KLOperators** group is granted only Read and Execute rights. The rights granted to the **KLAdmins** group are locked.

Users that belong to the **KLAdmins** group are called *Kaspersky Security Center administrators*, while users from the **KLOperators** group are called *Kaspersky Security Center operators*.

In addition to users included in the **KLAdmins** group, administrator rights for Kaspersky Security Center are also provided to the local administrators of devices on which Administration Server is installed.

You can exclude local administrators from the list of users who have Kaspersky Security Center administrator rights.

All operations started by the administrators of Kaspersky Security Center are performed using the rights of the Administration Server account.

An individual **KLAdmins** group can be created for each Administration Server from the network; the group will have the necessary rights for that Administration Server only.

If devices belonging to the same domain are included in the administration groups of different Administration Servers, the domain administrator is the Kaspersky Security Center administrator for all the groups. The **KLAdmins** group is the same for those administration groups; it is created during installation of the first Administration Server. All operations initiated by a Kaspersky Security Center administrator are performed using the account rights of the Administration Server for which these operations have been started.

After the application is installed, an administrator of Kaspersky Security Center can do the following:

- Modify the rights granted to the **KLOperators** groups.
- Grant rights—to access Kaspersky Security Center functionality—to other user groups and individual users who are registered on the administrator's workstation.
- Assign user access rights within each administration group.

The Kaspersky Security Center administrator can assign access rights to each administration group or to other objects of Administration Server in the **Security** section in the properties window of the selected object.

You can track user activity by using the records of events in the Administration Server operation. Event records are displayed in the **Administration Server** node on the **Events** tab. These events have the importance level **Info events** and the event types begin with "Audit".

Conditions of connection to an Administration Server over the Internet

If an Administration Server is remotely located outside a corporate network, client devices can connect to it over the

Internet.

For devices to connect to an Administration Server over the Internet, the following conditions must be met:

- The remote Administration Server must have an external IP address and the incoming port 13000 must remain open (for connection of Network Agents). We recommend that you also open UDP port 13000 (for receiving notifications of device shut down).
- Network Agents must be installed on the devices.
- When installing Network Agent on devices, you must specify the external IP address of the remote Administration Server. If an installation package is used for installation, specify the external IP address manually in the properties of the installation package, in the **Settings** section.
- To use the remote Administration Server to manage applications and tasks for a device, in the properties window of the device, in the **General** section, select the **Do not disconnect from the Administration Server** check box. After the check box is selected, wait until the Administration Server is synchronized with the remote device. The number of client devices maintaining a continuous connection with an Administration Server cannot exceed 300.

To speed up the performance of tasks initiated by a remote Administration Server, you can open port 15000 on a device. In this case, to run a task, the Administration Server sends a special packet to Network Agent over port 15000 without waiting until completion of synchronization with the device.

Encrypted connection to an Administration Server

Data exchange between client devices and Administration Server, as well as Administration Console connection to Administration Server, can be performed using the TLS (Transport Layer Security) protocol. The TLS protocol can identify the interacting parties, encrypt the data that is transferred, and protect data against modification during transfer. The TLS protocol uses public keys to authenticate the interacting parties and encrypt data.

In this section

Authenticating Administration Server when a device is connected	603
Administration Server authentication during Administration Console connection	604
Administration Server certificate	604:
Viewing log of connections to the Administration Server	1008

Authenticating Administration Server when a device is connected

When a client device connects to Administration Server for the first time, Network Agent on the device downloads a copy of the Administration Server certificate and stores it locally.

If you install Network Agent on a device locally, you can select the Administration Server certificate manually.

The downloaded copy of the certificate is used to verify Administration Server rights and permissions during subsequent connections.

During future sessions, Network Agent requests the Administration Server certificate at each connection of the device to Administration Server and compares it with the local copy. If the copies do not match, the device is not allowed access to Administration Server.

Administration Server authentication during Administration Console connection

At the first connection to Administration Server, Administration Console requests the Administration Server certificate and saves it locally on the administrator's workstation. After that, each time when Administration Console tries to connect to this Administration Server, the Administration Server is identified based on the certificate copy.

If the Administration Server certificate does not match the copy stored on the administrator's workstation, Administration Console prompts you to confirm connection to the Administration Server with the specified name and download a new certificate. After the connection is established, Administration Console saves a copy of the new Administration Server certificate, which will be used to identify the Administration Server in the future.

Administration Server certificate

Two operations—Administration Server authentication during connection by Administration Console and data exchange with devices—are performed based on the *Administration Server certificate*. The certificate is also used for authentication when primary Administration Servers are connected to secondary Administration Servers.

Certificate issued by Kaspersky

The Administration Server certificate is created automatically during installation of the Administration Server component and is stored in the ALLUSERSPROFILE%\Application Data\KasperskyLab\admindkit\1093\cert folder.

The Administration Server certificate is valid for five years, if the certificate was issued before 1 September 2020. Otherwise, the certificate validity term is limited to 397 days. A new certificate is generated by the Administration Server as the reserve certificate 90 days before the expiration date of the current certificate. Subsequently, the new certificate automatically replaces the current certificate one day before the expiration date. All Network Agents on the client devices are automatically reconfigured to authenticate the Administration Server with the new certificate.

If you specify a validity term longer than 397 days for the Administration Server certificate, the web browser returns an error.

Custom certificates

If necessary, you can assign a custom certificate for the Administration Server. For example, this may be necessary for better integration with the existing PKI of your enterprise or for custom configuration of the certificate fields. When replacing the certificate, all Network Agents that were previously connected to Administration Server through SSL will lose their connection and will return "Administration Server authentication error". To eliminate this error, you will have to restore the connection after the certificate replacement.

► *To replace the Administration Server certificate manually:*

1. Use the `klsetsrvcert` utility to replace the certificate.

From the command line, run the command with the following syntax:

```
klsetsrvcert -t <type> [-i <inputfile> [-p <password>] | -g <dnsname>] [-l <logfile>]
```

2. On the client devices, use the klmover utility (see section "Manually connecting a client device to the Administration Server. Klmover utility" on page [638](#)) to specify the new certificate and restore connection of the Network Agents to the Administration Server.

From the command line, run a command with the following syntax:

```
klmover [-address <server address>] [-pn <port number>] [-ps <SSL port number>] [-nossll] [-cert <path to certificate file>]
```

The Administration Server certificate is replaced and the server is authenticated by the Network Agents on the client devices.

If the Administration Server certificate is lost, you must reinstall the Administration Server component and restore the data (see section "Backup copying and restoration of Administration Server data" on page [617](#)) in order to recover it.

Disconnecting from an Administration Server

► *To disconnect from an Administration Server:*

1. In the console tree select the node corresponding to the Administration Server that you want to disconnect.
2. In the context menu of the node select **Disconnect from Administration Server**.

Adding an Administration Server to the console tree

► *To add an Administration Server to the console tree:*

1. In the Kaspersky Security Center main window, in the console tree select the **Kaspersky Security Center 13** node.
2. In the context menu of the node, select **New** → **Administration Server**.

A node named **Administration Server - <Device name> (Not connected)** is created in the console tree from which you will be able to connect to any of the Administration Servers installed on the network.

Removing an Administration Server from the console tree

► *To remove an Administration Server from the console tree:*

1. In the console tree select the node corresponding to the Administration Server that you want to remove.
2. In the context menu of the node select **Remove**.

Adding a virtual Administration Server to the console tree

► *To add a virtual Administration Server to the console tree:*

1. In the console tree, select the node with the name of the Administration Server for which you need to create a virtual Administration Server.
2. In the Administration Server node, select the **Administration Servers** folder.
3. In the workspace of the **Administration Servers** folder, click the **Add virtual Administration Server** link.

The New Virtual Administration Server Wizard starts.

4. In the **Name of virtual Administration Server** window, specify the name of the virtual Administration Server to be created.

The name of a virtual Administration Server cannot be more than 255 characters long and cannot include any special characters (such as "*" <>? \:|).

5. In the **Enter address for device connection to virtual Administration Server** window, specify the device connection address

The connection address of a virtual Administration Server is the network address through which devices will connect to that Server. The connection address has two parts: the network address of a physical Administration Server and the name of a virtual Administration Server, separated with a slash. The name of the virtual Administration Server will be substituted automatically. The specified address will be used on the virtual Administration Server as the default address in Network Agent installation packages.

6. In the **Create the virtual Administration Server administrator account** window, assign a user from the list to act as virtual Server administrator, or add a new administrator account by clicking the **Create** button.

You can specify multiple accounts.

A node named **Administration Server <Name of virtual Administration Server>** is created in the console tree.

Changing an Administration Server service account. Utility tool klsrvswch

If you have to change the Administration Server service account that was set during installation of Kaspersky Security Center, you can use a utility named klsrvswch that is designed for changing the Administration Server account.

When Kaspersky Security Center is installed, the utility is automatically copied to the application installation folder.

The number of launches of the utility is essentially unlimited.

The klsrvswch utility allows you to change the account type. For example, if you use a local account, you can change it to a domain account or to a managed service account (and vice versa).

Windows Vista and later Windows versions do not allow the use of a LocalSystem account for the Administration Server. In these Windows versions, the **LocalSystem account** option is inactive.

► *To change an Administration Server service account to a domain account:*

1. Launch the klsrvswch utility from the installation folder of Kaspersky Security Center.

This action also launches the wizard for modification of Administration Server service account. Follow the instructions of the Wizard.

2. In the **Administration Server service account** window, select **LocalSystem account**.

After the wizard finishes, the Administration Server account is changed. The Administration Server service will start under the *Local/System Account* and use its credentials.

Correct operation of Kaspersky Security Center requires that the account used to start the Administration Server service has administrator rights to the resource where the Administration Server database is hosted.

- *To change an Administration Server service account to a user account or a managed service account:*

1. Launch the `klsvswch` utility from the installation folder of Kaspersky Security Center.
This action also launches the wizard for modification of Administration Server service account. Follow the instructions of the Wizard.
2. In the **Administration Server service account** window, select **Custom account**.
3. Click the **Find now** button.
The **Select User** window opens.
4. In the **Select User** window, click the **Object Types** button.
5. In the object types list, select **Users** (if you want a user account) or **Service Accounts** (if you want a managed service account) and click **OK**.
6. In the object name field, enter the name of the account, or a part of the name, and click **Check Names**.
7. In the list of the matching names, select the necessary name, and then click **OK**.
8. If you selected **Service Accounts**, in the **Account password** window, leave the **Password** and **Confirm password** fields blank. If you selected **Users**, enter a new password for the user and confirm it.

The Administration Server service account will be changed to the account that you selected.

When Microsoft SQL Server is used in a mode that presupposes authenticating user accounts with Windows tools, access to the database must be granted. The user account must have the status of owner of the Kaspersky Security Center database. The `dbo` schema is used by default.

Changing DBMS credentials

Sometimes, you may need to change DBMS credentials, for example, in order to perform a credential rotation for security purposes.

- *To change DBMS credentials in a Windows environment by using `klsvswch.exe`:*

1. Launch the `klsvswch` utility that is located in the installation folder of Kaspersky Security Center.
2. Click the **Next** button of the wizard until you reach the **Change DBMS access credentials** step.
3. At the **Change DBMS access credentials** step of the wizard, perform the following:
 - Select the **Apply new credentials** option.
 - Specify a new account name in the **Account** field.
 - Specify a new password for an account in the **Password** field.
 - Specify the new password in the **Confirm password** field.

You should specify credentials of an account that exists in the DBMS.

4. Click the **Next** button.

After the wizard finishes, the DBMS credentials are changed.

Resolving issues with Administration Server nodes

The console tree in the left pane of Administration Console contains nodes of Administration Servers. You can add as many Administration Servers as you need to the console tree (see section "Adding an Administration Server to the console tree" on page [605](#)).

The list of Administration Server nodes in the console tree is stored in a shadow copy of a .msc file by means of Microsoft Management Console. The shadow copy of this file is located in the %USERPROFILE%\AppData\Roaming\Microsoft\MMC\ folder on the device where the Administration Console is installed. For each Administration Server node, the file contains the following information:

- Administration Server address
- Port number
- Whether TLS is in use

This parameter depends on the port number (see section "Configuring the connection of Administration Console to Administration Server" on page [278](#)) used to connect Administration Console to the Administration Server.

- User name
- Administration Server certificate

Troubleshooting

When Administration Console connects to the Administration Server (see section "Administration Server authentication during Administration Console connection" on page [604](#)), the certificate stored locally is compared to the Administration Server certificate. If the certificates do not match, Administration Console generates an error. For example, a certificate mismatch may occur when you replace the Administration Server certificate (see section "Administration Server certificate" on page [604](#)). In this case, recreate the Administration Server node in the console.

► *To recreate an Administration Server node:*

1. Close the Kaspersky Security Center Administration Console window.
2. Delete the Kaspersky Security Center 13 file at %USERPROFILE%\AppData\Roaming\Microsoft\MMC\.
3. Run Kaspersky Security Center Administration Console.

You will be prompted to connect to the Administration Server and accept its existing certificate.

4. Do one of the following:
 - Accept the existing certificate by clicking the **Yes** button.
 - To specify your certificate, click the **No** button, and then browse to the certificate file to be used to authenticate the Administration Server.

The certificate issue is resolved. You can use Administration Console to connect to the Administration Server.

Viewing and modifying the settings of an Administration Server

You can adjust the settings of an Administration Server in the properties window of this Server.

- *To open the Properties: Administration Server window,*

Select **Properties** in the context menu of the Administration Server node in the console tree.

In this section

Adjusting the general settings of Administration Server	609
Administration Console interface settings	609
Event processing and storage on the Administration Server	610
Viewing log of connections to the Administration Server	610
Control of virus outbreaks	611
Limiting traffic	611
Configuring Web Server	612
Reissuing the Web Server certificate	612
Working with internal users	614

Adjusting the general settings of Administration Server

You can adjust the general settings of Administration Server in the **General**, **Administration Server connection settings**, **Events repository**, and **Security** sections of the Administration Server properties window.

The **Security** section is not displayed in the Administration Server properties window if the display has been disabled in the Administration Console interface.

- *To enable the display of the **Security** section in Administration Console:*

1. In the console tree, select the Administration Server that you want.
2. In the **View** menu of the main application window, select **Configure interface**.
3. In the **Configure interface** window that opens, select the **Display security settings sections** check box and click **OK**.
4. In the window with the application message, click **OK**.

The **Security** section will be displayed in the Administration Server properties window.

Administration Console interface settings

You can adjust the interface settings of Administration Console to display or hide the user interface controls related to the following features:

- Vulnerability and Patch Management
- Data encryption and protection
- Endpoint control settings
- Mobile Device Management
- Secondary Administration Servers

- Security Settings sections

► *To configure the Administration Console interface settings:*

1. In the console tree, select the Administration Server that you want.
2. In the **View** menu of the main application window, select **Configure interface**.
3. In the **Configure interface** window that opens, select the check boxes next to the features that you want displayed and click **OK**.
4. In the window with the application message, click **OK**.

The selected features will be displayed in the Administration Console interface.

Event processing and storage on the Administration Server

Information about events during the operation of the application and managed devices is saved in the Administration Server database. Each event is attributed to a certain type and level of severity (*Critical event*, *Functional failure*, *Warning*, or *Info*). Depending on the conditions under which an event occurred, the application can assign different levels of severity to events of the same type.

You can view types and levels of severity assigned to events in the **Event configuration** section of the Administration Server properties window. In the **Event configuration** section, you can also configure processing of every event by the Administration Server:

- Registration of events on the Administration Server and in event logs of the operating system on a device and on the Administration Server.
- Method used for notifying the administrator of an event (for example, an SMS or email message).

In the **Events repository** section of the Administration Server properties window, you can edit the settings of events storage in the Administration Server database by limiting the number of event records and record storage term. When you specify the maximum number of events, the application calculates an approximate amount of storage space required for the specified number. You can use this approximate calculation to evaluate whether you have enough free space on the disk to avoid database overflow. The default capacity of the Administration Server database is 400,000 events. The maximum recommended capacity of the database is 45 million events.

If the number of events in the database reaches the maximum value specified by the administrator, the application deletes the oldest events and rewrites them with new ones. When the Administration Server deletes old events, it cannot save new events to the database. During this period of time, information about events that were rejected is written to the Kaspersky Event Log. The new events are queued and then saved to the database after the deletion operation is complete.

Viewing log of connections to the Administration Server

The history of connections and attempts to connect to the Administration Server during its operation can be saved to a log file. The information in the file allows you to track not only connections on your network infrastructure, but unauthorized attempts to access the Administration Server as well.

► *To log the events of connection to the Administration Server:*

1. In the console tree, select the Administration Server for which you want to enable connection event logging.
2. In the context menu of the Administration Server, select **Properties**.

3. In the properties window that opens, in the **Administration Server connection settings** section, select the **Connection ports** subsection.
4. Enable the **Log Administration Server connection events** option.
5. Click the **OK** button to close the Administration Server properties window.

All further events of inbound connections to the Administration Server, authentication results, and SSL errors will be saved to the %ProgramData%\KasperskyLab\adminkit\logs\sc.syslog file.

Control of virus outbreaks

Kaspersky Security Center allows you to quickly respond to emerging threats of virus outbreaks. Risks of virus outbreaks are assessed by monitoring virus activity on devices.

You can configure assessment rules for threats of virus outbreaks and actions to take in case one emerges; to do this, use the **Virus outbreak** section of the properties window of Administration Server.

You can specify the notification procedure for the *Virus outbreak* event in the **Event configuration** section of the Administration Server properties window (see section "Event processing and storage on the Administration Server" on page [610](#)), in the *Virus outbreak* event properties window.

The *Virus outbreak* event is generated upon detection of *Malicious object detected* events during the operation of security applications. Therefore, you must save information about all *Malicious object detected* events on Administration Server in order to recognize virus outbreaks.

You can specify the settings for saving information about any *Malicious object detected* event in the policies of the security applications.

When *Malicious object detected* events are counted, only information from the devices of the primary Administration Server is taken into account. The information from secondary Administration Servers is not taken into account. For each secondary Server, the *Virus outbreak* event is configured individually.

See also:

Scenario: Monitoring and reporting[1279](#)

Limiting traffic

To reduce traffic volumes within a network, the application provides the option to limit the speed of data transfer to an Administration Server from specified IP ranges and IP subnets.

You can create and configure traffic-limiting rules in the **Traffic** section of the Administration Server properties window.

► To create a traffic-limiting rule:

1. In the console tree, select the node with the name of the Administration Server for which you want to create a traffic-limiting rule.
2. In the context menu of the Administration Server, select **Properties**.

3. In the Administration Server properties window, select the **Traffic** section.
4. Click the **Add** button.
5. In the **New rule** window, specify the following settings:

In the **IP range to limit traffic** section, select the method that will be used to define the subnet or range for which the data transfer rate will be limited, and then enter the values of the settings for the selected method. Select one of the following methods:

- **Specify the range by using address and network mask**

Traffic is limited based on subnet settings. Specify the subnet address and the subnet mask for determining the range in which traffic will be limited.

You can also click **Browse** to add subnets from the global list of subnets (see section "Viewing and modifying subnet properties in the global list of subnets" on page [942](#)).

- **Specify the range by using start and end addresses**

Traffic is limited based on a range of IP addresses. Specify the range of IP addresses in the **Start** and **End** entry fields.

This option is selected by default.

In the **Traffic limit** section, you can adjust the following restrictive settings for the data transfer rate:

- **Time interval**

Time interval during which the traffic restriction will be in force. You can specify the boundaries of the time interval in the entry fields.

- **Limit (KB/s)**

Maximum total transfer speed of incoming and outgoing data of the Administration Server. Traffic restriction will only be effective within the interval specified in the **Time interval** field.

- **Limit traffic for the remaining time (KB/s)**

Traffic will be limited not only within the interval specified in the **Time interval** field, but also at other times.

By default, this check box is cleared. The value of this field may not match the value of the **Limit (KB/s)** field.

Primarily, traffic limiting rules affect the transfer of files. These rules do not apply to the traffic generated by synchronization between Administration Server and Network Agent, or between primary and secondary Administration Servers.

Configuring Web Server

Web Server is designed for publishing stand-alone installation packages, iOS MDM profiles, and files from a shared folder.

You can define the settings for Web Server connection to the Administration Server and set the Web Server certificate in the **Web Server** section of the Administration Server properties window.

Reissuing the Web Server certificate

The Web Server (see section "Kaspersky Security Center Web Server" on page [Error! Bookmark not defined.](#)) certificate used in Kaspersky Security Center is required for publishing Network Agent installation packages that

you subsequently download to managed devices, as well as for publishing iOS MDM profiles, iOS apps, and Kaspersky Endpoint Security for Mobile installation packages. Depending on the current application configuration, various certificates can function as the Web Server certificate (for more detail, see About Kaspersky Security Center certificates (on page [86](#))).

You may need to reissue the Web Server certificate to meet the specific security requirements of your organization or to maintain continuous connection of your managed devices before starting to upgrade the application (see section "Upgrading Kaspersky Security Center from a previous version" on page [262](#)). Kaspersky Security Center provides two ways of reissuing the Web Server certificate; the choice between the two methods depends on whether you have mobile devices connected (see section "Connecting KES devices to the Administration Server" on page [208](#)) and managed through the mobile protocol (i.e., by using the mobile certificate).

If you have never specified your own custom certificate as the Web Server certificate in the **Web Server** section of the Administration Server properties window, the mobile certificate acts as the Web Server certificate. In this case, the Web Server certificate reissuance is performed through the reissuance of the mobile protocol itself.

► *To reissue the Web Server certificate when you have no mobile devices managed through the mobile protocol:*

1. In the console tree, right-click the name of the relevant Administration Server and in the context menu select **Properties**.
2. In the Administration Server properties window that opens, in the left pane select the **Administration Server connection settings** section.
3. In the list of subsections, select the **Certificates** subsection.
4. If you plan to continue using the certificate issued by Kaspersky Security Center, do the following:
 - a. On the right pane, in the **Administration Server authentication by mobile devices** group of settings, select the **Certificate issued through Administration Server** option and click the **Reissue** button.
 - b. In the **Reissue certificate** window that opens, in the **Connection address** and **Activation term** group of settings select the relevant options and click **OK**.
 - c. In the confirmation window, click **Yes**.

Alternatively, if you plan to use your own custom certificate, do the following:

- d. Check whether your custom certificate meets the requirements of Kaspersky Security Center (see section "Requirements to custom certificates used in Kaspersky Security Center" on page [279](#)) and the requirements for trusted certificates by Apple <https://support.apple.com/en-us/HT210176>. If necessary, modify the certificate.
- e. Select the **Other certificate** option and click the **Browse** button.
- f. In the **Certificate** window that opens, in the **Certificate type** field select the type of your certificate and then specify the certificate location and settings:
 - If you have selected **PKCS #12 container**, click the **Browse** button next to the **Certificate file** field and specify the certificate file on your hard drive. If the certificate file is password-protected, enter the password in the **Password (if any)** field.
 - If you have selected **X.509 certificate**, click the **Browse** button next to the **Private key (.prk, .pem)** field and specify the private key on your hard drive. If the private key is password-protected,

enter the password in the **Password (if any)** field. Then click the **Browse** button next to the **Public key (.cer)** field and specify the private key on your hard drive.

- g. In the **Certificate** window, click **OK**.
- h. In the confirmation window, click **Yes**.

The mobile certificate is reissued to be used as the Web Server certificate.

► *To reissue the Web Server certificate when you have any mobile devices managed through the mobile protocol:*

1. Generate your custom certificate and prepare it for the usage in Kaspersky Security Center. Check whether your custom certificate meets the requirements of Kaspersky Security Center (see section "Requirements to custom certificates used in Kaspersky Security Center" on page [279](#)) and the requirements for trusted certificates by Apple <https://support.apple.com/en-us/HT210176>. If necessary, modify the certificate.

You can use the `kliossvcertgen.exe` utility <https://support.kaspersky.com/10890#block1> for certificate generation.

2. In the console tree, right-click the name of the relevant Administration Server and in the context menu select **Properties**.
3. In the Administration Server properties window that opens, in the left pane select the **Web Server** section.
4. In the **Over HTTPS** menu, select the **Specify another certificate** option.
5. In the **Over HTTPS** menu, click the **Change** button.
6. In the **Certificate** window that opens, in the **Certificate type** field select the type of your certificate:
 - If you have selected **PKCS #12 container**, click the **Browse** button next to the **Certificate file** field and specify the certificate file on your hard drive. If the certificate file is password-protected, enter the password in the **Password (if any)** field.
 - If you have selected **X.509 certificate**, click the **Browse** button next to the **Private key (.prk, .pem)** field and specify the private key on your hard drive. If the private key is password-protected, enter the password in the **Password (if any)** field. Then click the **Browse** button next to the **Public key (.cer)** field and specify the private key on your hard drive.
7. In the **Certificate** window, click **OK**.
8. If necessary, in the Administration Server properties window, in the **Web Server HTTPS port** field change the number of the HTTPS port for Web Server. Click **OK**.

The Web Server certificate is reissued.

Working with internal users

The accounts of *internal users* are used to work with virtual Administration Servers. Kaspersky Security Center grants the rights of real users to internal users of the application.

The accounts of internal users are created and used only within Kaspersky Security Center. No data on internal users is transferred to the operating system. Kaspersky Security Center authenticates internal users.

You can configure accounts of internal users in the **User accounts** folder of the console tree (see section "Working with user accounts" on page [678](#)).

Backup and restoration of Administration Server settings

Backup of the settings of Administration Server and its database is performed through the backup task and klbackup utility. A backup copy includes all the main settings and objects pertaining to the Administration Server, such as certificates, primary keys for encryption of drives on managed devices, keys for various licenses, structure of administration groups with all of its contents, tasks, policies, etc. With a backup copy you can recover the operation of an Administration Server as soon as possible, spending from a dozen minutes to a couple of hours on this.

Never neglect regular backups of Administration Server using the standard backup task.

If no backup copy is available, a failure may lead to an irrevocable loss of certificates and all Administration Server settings. This will necessitate reconfiguring Kaspersky Security Center from scratch, and performing initial deployment of Network Agent on the organization's network again. All primary keys for encryption of drives on managed devices will also be lost, risking irrevocable loss of encrypted data on devices with Kaspersky Endpoint Security.

The Quick Start Wizard creates the backup task for Administration Server settings and sets it to run daily, at 4:00 AM. Backup copies are saved by default in the folder %ALLUSERSPROFILE%\Application Data\KasperskySC.

If an instance of Microsoft SQL Server installed on another device is used as the DBMS, you must modify the backup task by specifying a UNC path, which is available for write by both the Administration Server service and the SQL Server service, as the folder to store backup copies. This requirement, which is not obvious, derives from a special feature of backup in the Microsoft SQL Server DBMS.

If a local instance of Microsoft SQL Server is used as the DBMS, we also recommend to save backup copies on a dedicated medium in order to secure them against damage together with Administration Server.

Because a backup copy contains important data, the backup task and klbackup utility provide for password protection of backup copies. By default, the backup task is created with a blank password. You must set a password in the properties of the backup task. Neglecting this requirement causes a situation where all keys of Administration Server certificates, keys for licenses, and primary keys for encryption of drives on managed devices remain unencrypted.

In addition to the regular backup, you must also create a backup copy prior to every significant change, including installation of Administration Server upgrades and patches.

To minimize the size of backup copies, enable the **Compress backup** option in the SQL Server settings.

Restoration from a backup copy is performed with the utility klbackup on an operable instance of Administration Server that has just been installed and has the same version (or later) for which the backup copy was created.

The instance of Administration Server on which the restoration is to be performed, must use a DBMS of the same type (same SQL Server, MySQL, or MariaDB) and the same (or later) version. The version of Administration Server can be the same (with an identical or later patch), or later.

This section describes standard scenarios for restoring settings and objects of Administration Server.

In this section

Using a file system snapshot to reduce the backup duration	616
A device with Administration Server is inoperable	616
The settings of Administration Server or the database are corrupted	617

Using a file system snapshot to reduce the backup duration

In Kaspersky Security Center 13, the idle time of Administration Server during backup has been reduced as compared to earlier versions. Moreover, the **Use file system snapshot for data backup** feature has been added to the task settings. This feature provides additional idle reduction by using the kbackup utility, which creates a shadow copy of the disk during backup (this takes a few seconds) and simultaneously copies the database (this takes a few minutes at longest). When kbackup creates a shadow copy of the disk and a copy of the database, the utility makes the Administration Server connectible again.

You can use the file system snapshotting feature only if these two conditions are met:

- The Administration Server shared folder and the %ALLUSERSPROFILE%\KasperskyLab folder are located on the same logical disk and are local in reference to the Administration Server.
- The %ALLUSERSPROFILE%\KasperskyLab folder does not contain any symbolic links that have been created manually.

Do not use the feature if either of these conditions cannot be met. In this case, the application would return an error message in response to any attempt to create a file system snapshot.

To use the feature, you must have an account that has been granted the permission to create snapshots of the logical disk storing the %ALLUSERSPROFILE% folder. Note that the Administration Server service account has no such permission.

► *To use the file system snapshotting feature in order to reduce the backup duration:*

1. In the **Tasks** section, select the backup task.
2. In the context menu, select **Properties**.
3. In the task properties window that opens, select the **Settings** section.
4. Select the **Use file system snapshot for data backup** check box.
5. In the **User name** and **Password** fields, enter the name and password of an account that has the permission to create snapshots of the logical disk storing the %ALLUSERSPROFILE% folder.
6. Click **Apply**.

At any further startup of the backup task, the kbackup utility will create file system snapshots thus reducing the Administration Server idle time during the task run.

A device with Administration Server is inoperable

If a device with Administration Server is inoperable due to a failure, you are recommended to perform the following actions:

- The new Administration Server must be assigned the same address: NetBIOS name, FQDN, or static IP (depending on which of them was set when Network Agents were deployed).

- Install Administration Server, using a DBMS of the same type, of the same (or later) version. You can install the same version of Server with the same (or later) patch, or a later version. After installation, do not perform the initial setup through the Wizard.
- In the **Start** menu, run the utility klbackup and perform restoration.

The settings of Administration Server or the database are corrupted

If Administration Server is inoperable due to corrupted settings or database (e.g., after a power surge), you are recommended to use the following restoration scenario:

1. Scan the file system on the damaged device.
2. Uninstall the inoperable version of Administration Server.
3. Reinstall Administration Server, using a DBMS of the same type and of the same (or later) version. You can install the same version of Server with the same (or later) patch, or a later version. After installation, do not perform the initial setup through the Wizard.
4. In the **Start** menu, run the utility klbackup and perform restoration.

It is prohibited to restore Administration Server in any way other than through the klbackup utility. Any attempts to restore Administration Server through third-party software will inevitably lead to desynchronization of data on nodes of the distributed application Kaspersky Security Center and, consequently, to improper functioning of the application.

Backup copying and restoration of Administration Server data

Data backup allows you to move Administration Server from one device to another without data loss. Through backup, you can restore data when moving the Administration Server database to another device, or when upgrading to a newer version of Kaspersky Security Center.

You can create a backup copy of Administration Server data in one of the following ways:

- By creating and running a data backup task through Administration Console.
- By running the klbackup utility on the device that has Administration Server installed. This utility is included in the Kaspersky Security Center distribution kit. After the installation of Administration Server, the utility is located in the root of the destination folder specified at the application installation.

The following data is saved in the backup copy of Administration Server:

- Database of Administration Server (policies, tasks, application settings, events saved on the Administration Server).
- Configuration details of the structure of administration groups and client devices.
- Repository of distribution packages of applications for remote installation.
- Administration Server certificate.

Recovery of Administration Server data is only possible using the klbackup utility.

In this section

Creating a data backup task	618
Data backup and recovery utility (klbackup)	618
Data backup and recovery in interactive mode	619
Data backup and recovery in non-interactive mode	621
Moving Administration Server to another device	622

Creating a data backup task

Backup tasks are Administration Server tasks; they are created through the Quick Start Wizard. If a backup task created by the Quick Start Wizard has been deleted, you can create one manually.

► *To create an Administration Server data backup task:*

1. In the console tree, select the **Tasks** folder.
2. Start creation of the task in one of the following ways:
 - By selecting **New** → **Task** in the context menu of the **Tasks** folder in the console tree.
 - By clicking the **Create a task** button in the workspace.

The New Task Wizard starts. Follow the instructions of the Wizard. In the **Select the task type** window of the Wizard select the task type named **Backup of Administration Server data**.

The **Backup of Administration Server data** task can only be created in a single copy. If the Administration Server data backup task has already been created for the Administration Server, it is not displayed in the task type selection window of the Backup Task Creation Wizard.

Data backup and recovery utility (klbackup)

You can copy Administration Server data for backup and future recovery using the klbackup utility, which is part of the Kaspersky Security Center distribution kit.

The klbackup utility can run in either of the two following modes:

- Interactive (see section "Data backup and recovery in interactive mode" on page [619](#))
- Non-interactive (see section "Data backup and recovery in non-interactive mode" on page [621](#))

See also:

Scenario: Upgrading Kaspersky Security Center and managed applications	405
--	---------------------

Data backup and recovery in interactive mode

► *To create a backup copy of Administration Server data in interactive mode:*

1. Run the klbackup utility located in the Kaspersky Security Center installation folder.

The Backup and Restore Wizard starts.

2. In the first window of the Wizard, select **Perform backup of Administration Server data**.

If you select the **Restore or back up Administration Server certificate only** check box, only a backup copy of the Administration Server certificate will be saved.

Click **Next**.

3. In the next window of the Wizard, specify a password and a destination folder for backup. Click the **Next** button to start backup.

4. If you are working with a database in a cloud environment such as Amazon Web Services (AWS) or Microsoft Azure, in the **Sign In to Online Storage** window, fill in the following fields:

- For AWS:

- **S3 bucket name**

The name of the S3 bucket (see section "Preparing Amazon S3 bucket for database" on page [840](#)) that you created for the Backup.

- **Access key ID**

You received the key ID (sequence of alphanumeric characters) when you created the IAM user account (see section "Creating an IAM user account for work with Kaspersky Security Center" on page [833](#)) for working with S3 bucket storage instance.

The field is available if you selected RDS database on an S3 bucket.

- **Secret key**

The secret key that you received with the access key ID when you created the IAM user account (see section "Creating an IAM user account for work with Kaspersky Security Center" on page [833](#)).

The characters of the secret key are displayed as asterisks. After you begin entering the secret key, the **Show** button is displayed. Click and hold this button for the necessary amount of time to view the characters you entered.

The field is available if you selected an AWS IAM access key for authorization instead of an IAM role.

- For Microsoft Azure:

- **Azure storage account name**

You created the name of the Azure storage account (see section "Creating Azure storage account" on page [846](#)) for working with Kaspersky Security Center.

- **Azure Subscription ID**

You created (see section "Creating a subscription, Application ID, and password" on page [843](#)) the subscription on the Azure portal.

- **Azure password**

You received the password of the Application ID when you created the Application ID (see section "Creating a subscription, Application ID, and password" on page [843](#)).

The characters of the password are displayed as asterisks. After you begin entering the password, the **Show** button becomes available. Click and hold this button to view the characters you entered.

- **Azure Application ID**

You created (see section "Creating a subscription, Application ID, and password" on page [843](#)) this application ID on the Azure portal.

You can provide only one Azure Application ID for polling and other purposes. If you want to poll another Azure segment, you must first delete the existing Azure connection.

- **Azure SQL server name**

The name and the resource group are available in your Azure SQL Server properties.

- **Azure SQL server resource group**

The name and the resource group are available in your Azure SQL Server properties.

- **Azure storage access key**

Available in the properties of your storage account (see section "Working with Azure SQL" on page [846](#)), in the Access Keys section. You can use any of the keys (key1 or key2).

► *To recover Administration Server data in interactive mode:*

1. Run the klbackup utility located in the Kaspersky Security Center installation folder.

The Backup and Restore Wizard starts.

The klbackup utility must be started under the same account that you used to install Administration Server.

2. In the first window of the Wizard, select **Restore Administration Server data**.

If you select the **Restore or back up Administration Server certificate only** check box, the Administration Server will only be recovered.

Click **Next**.

3. In the **Restore settings** window of the Wizard:

- Specify the folder that contains a backup copy of Administration Server data. If you are working in a cloud environment such as AWS or Azure, specify the address of the storage.
- Specify the password that was entered during data backup.

4. Click the **Next** button to restore data.

When restoring data, you must specify the same password that was entered during backup. If you specify an invalid password, data will not be restored. If the path to a shared folder changed after backup, check the operation of tasks that use restored data (restore tasks and remote installation tasks). If necessary, edit the settings of these tasks. While data is being restored from a backup file, no one must access the shared folder of Administration Server. The account under which the klbackup utility is started must have full access to the shared folder.

See also:

Data backup and recovery in non-interactive mode..... [621](#)

Data backup and recovery in non-interactive mode

- ▶ *To create a backup copy or recover Administration Server data in non-interactive mode,*

Run `klbackup` with the required set of keys from the command line of the device that has Administration Server installed.

Utility command line syntax:

```
klbackup -path BACKUP_PATH [-logfile LOGFILE] [-use_ts][[-restore] [-password PASSWORD] [-online]
```

If no password is specified in the command line of the `klbackup` utility, the utility prompts you to enter the password interactively.

Descriptions of the keys:

- `-path BACKUP_PATH`—Save information in the `BACKUP_PATH` folder, or use data from the `BACKUP_PATH` folder for recovery (mandatory parameter).
- `-logfile LOGFILE`—Save a report about Administration Server data backup and recovery.

The database server account and the `klbackup` utility should be granted permissions for changing data in the folder `BACKUP_PATH`.

- `-use_ts`—When saving data, copy information to the `BACKUP_PATH` folder, to the subfolder with a name containing the current system date and operation time in `klbackup YYYY-MM-DD # HH-MM-SS` format. If no key is specified, information is saved in the root of the folder `BACKUP_PATH`.

During attempts to save information in a folder that already stores a backup copy, an error message appears. No information will be updated.

Availability of the `-use_ts` key allows an Administration Server data archive to be maintained. For example, if the `-path` key indicates the folder `C:\KLBackups`, the folder `klbackup 6/19/2017 # 11-30-18` then stores information about the status of the Administration Server as of June, 19, 2017, at 11:30:18 AM.

- `-restore`—Recover Administration Server data. Data recovery is performed based on information contained in the `BACKUP_PATH` folder. If no key is available, data is backed up in the `BACKUP_PATH` folder.
- `-password PASSWORD`—Save or recover the Administration Server certificate; to encrypt and decrypt the certificate, use the password specified by the `PASSWORD` parameter.

A forgotten password cannot be recovered. There are no password requirements. The password length is unlimited and zero length (no password) is also possible.

- `-online`—Back up Administration Server data by creating a volume snapshot to minimize the offline time of the Administration Server. When you use the utility to recover data, this option is ignored.

When restoring data, you must specify the same password that was entered during backup. If you specify an invalid password, data will not be restored. If the path to a shared folder changed after backup, check the operation of tasks that use restored data (restore tasks and remote installation tasks). If necessary, edit the settings of these tasks. While data is being restored from a backup file, no one must access the shared folder of Administration Server. The account under which the kbackup utility is started must have full access to the shared folder.

Moving Administration Server to another device

► *To move Administration Server to another device without shifting the Administration Server database:*

1. Create a backup copy of Administration Server data.
2. Install Administration Server on the selected device.

To simplify the process of moving administration groups, we recommend that you make sure that the address of the new Administration Server matches the address of the previous Administration Server. The address (the device name in the Windows network or an IP address) is specified in the settings for Network Agent connection to Administration Server.

3. On the new Administration Server recover Administration Server data from the backup copy.
4. If the address (the device name in the Windows network or the IP address) of the new Administration Server does not match the address of the previous Administration Server, connect client devices to the new Administration Server, by creating an Administration Server shift task for the **Managed devices** group on the previous Administration Server.

If the addresses match, you do not have to create an Administration Server shift task, and the connection will be made to the address specified in the settings.

5. Delete the previous Administration Server.

► *To move Administration Server to another device and change the Administration Server database:*

1. Create a backup copy of Administration Server data.
2. Set a new SQL Server device.

To transfer information correctly, the database on the new SQL Server must have the same collation schemes as the previous SQL Server.

3. Install a new Administration Server. The name of the previous SQL Server database and that of the new one must match.

To simplify the process of moving administration groups, we recommend that you make sure that the address of the new Administration Server matches the address of the previous Administration Server. The address (the device name in the Windows network or an IP address) is specified in the settings for connecting Network Agent to Administration Server.

4. On the new Administration Server, recover the data from the previous Administration Server from the backup copy.
5. If the address (the device name in the Windows network or the IP address) of the new Administration Server does not match the address of the previous Administration Server, connect client devices to the new Administration Server, by creating an Administration Server shift task for the **Managed devices** group on the previous Administration Server.

If the addresses match, you do not have to create an Administration Server shift task, and the connection will be made to the address specified in the settings.
6. Delete the previous Administration Server.

Avoiding conflicts between multiple Administration Servers

If you have more than one Administration Server on your network, they can see the same client devices. This may result, for example, in remote installation of the same application to one and the same device from more than one Server and other conflicts. To avoid such a situation, Kaspersky Security Center 13 allows you to prevent an application from being installed on a device managed by another Administration Server (see section "Installing applications using Remote Installation Wizard" on page [338](#)).

You can also use the **Managed by a different Administration Server** property as a criterion for the following purposes:

- Searching for devices (see section "Finding devices" on page [914](#))
- Device selections (on page [521](#))
- Device moving rules (on page [401](#))
- Auto-tagging rules (see section "Automatic device tagging" on page [649](#))

Kaspersky Security Center 13 uses heuristics to determine whether a client device is managed by the Administration Server you are working with or by a different Administration Server.

Two-step verification

This section describes how you can use two-step verification to reduce the risk of unauthorized access to Administration Console.

In this section

Scenario: configuring two-step verification for all users	624
About two-step verification.....	625
Enabling two-step verification for your own account	627
Enabling two-step verification for all users	628
Disabling two-step verification for a user account	628
Disabling two-step verification for all users	629
Excluding accounts from two-step verification.....	629
Editing the name of a security code issuer	630

Scenario: configuring two-step verification for all users

This scenario describes how to enable two-step verification for all users and how to exclude user accounts from two-step verification. If you did not enable two-step verification for your account before you enable it for other users, the application opens the window for enabling two-step verification for your account, first. This scenario also describes how to enable two-step verification for your own account.

If you enabled two-step verification for your account, you may proceed to the stage of enabling of two-step verification for all users.

Prerequisites

Before you start:

- Make sure that your user account has the Modify object ACLs (see section "Access rights to application features" on page [684](#)) right of the **General features: User permissions** functional area for modifying security settings for other users' accounts.
- Make sure that the other users of Administration Server install an authenticator application on their devices.

Stages

Enabling two-step verification for all users proceeds in stages:

a. Installing an authenticator application on a device

You can install Google Authenticator, Microsoft Authenticator, or any other authenticator application that supports the Time-based One-time Password algorithm.

b. Synchronizing the authenticator application time with the time of the device on which Administration Server is installed

Ensure that the time set in the authenticator application is synchronized with the time of Administration Server.

c. Enabling two-step verification for your account and receiving the secret key for your account

How-to instructions:

For MMC-based Administration Console: Enabling two-step verification for your own account (on page [627](#))

For Kaspersky Security Center 13 Web Console: Enabling two-step verification for your own account (on page [1019](#))

After you enable two-step verification for your account, you can enable two-step verification for all users.

d. Enabling two-step verification for all users

Users with two-step verification enabled must use it to log in to Administration Server.

How-to instructions:

For MMC-based Administration Console: Enabling two-step verification for all users (on page [628](#))

For Kaspersky Security Center 13 Web Console: Enabling two-step verification for all users (on page [1019](#))

e. Editing the name of a security code issuer

If you have several Administration Servers with similar names, you may have to change the security code issuer names for better recognition of different Administration Servers.

How-to instructions:

For MMC-based Administration Console: Editing the name of a security code issuer (on page [630](#))

For Kaspersky Security Center 13 Web Console: Editing the name of a security code issuer (on page [1022](#))

f. Excluding user accounts for which you do not need to enable two-step verification

If required, exclude users from two-step verification. Users with excluded accounts do not have to use two-step verification to log in to Administration Server.

How-to instructions:

For MMC-based Administration Console: Excluding accounts from two-step verification (on page [629](#))

For Kaspersky Security Center 13 Web Console: Excluding accounts from two-step verification (on page [1021](#))

Results

Upon completion of this scenario:

- Two-step verification is enabled for your account.
- Two-step verification is enabled for all user accounts of the Administration Server, except for user accounts that were excluded.

See also:

About two-step verification.....	625
Enabling two-step verification for your own account	627
Enabling two-step verification for all users	628
Excluding accounts from two-step verification.....	629

About two-step verification

Kaspersky Security Center provides two-step verification for users of Administration Console. When two-step verification is enabled for your own account, every time you log in to Administration Console, you enter your user name, password, and an additional single-use security code. If you use domain authentication (see section "Configuring domain authentication by using the NTLM and Kerberos protocols" on page [992](#)) for your account, you

only have to enter an additional single-use security code. To receive a single-use security code, you must have an authenticator application on your computer or your mobile device.

A security code has an identifier referred to as *issuer name*. The security code issuer name is used as an identifier of the Administration Server in the authenticator application. You can change the name of the security code issuer name. The security code issuer name has a default value that is the same as the name of the Administration Server. The issuer name is used as an identifier of the Administration Server in the authenticator application. If you change the security code issuer name, you must issue a new secret key and pass it to the authenticator application. A security code is single-use and valid for 30 seconds.

Any user for whom two-step verification is enabled can reissue his or her own secret key. When a user authenticates with the reissued secret key and uses it for logging in, Administration Server saves the new secret key for the user account. If the user enters the new secret key incorrectly, Administration Server does not save the new secret key and leaves the current secret key valid for the further authentication.

Any authentication software that supports the Time-based One-time Password algorithm (TOTP) can be used as an authenticator application, for example, Google Authenticator. In order to generate the security code, you must synchronize the time set in the authenticator application with the time set for Administration Server.

An authenticator application generates the security code as follows:

1. Administration Server generates a special secret key and QR code.
2. You pass the generated secret key or QR code to the authenticator application.
3. The authenticator application generates a single-use security code that you pass to the authentication window of Administration Server.

We highly recommend that you install an authenticator application on more than one device. Save the secret key (or QR code) and keep it in a safe place. This will help you to restore access to Administration Console in case you lose access to your mobile device.

To secure the usage of Kaspersky Security Center, you can enable two-step verification for your own account and enable two-step verification for all users.

You can exclude (see section "Excluding accounts from two-step verification" on page [1021](#)) accounts from two-step verification. This can be necessary for service accounts that cannot receive a security code for authentication.

Two-step verification works according to the following rules:

- Only a user account that has the Modify object ACLs (see section "Access rights to application features" on page [684](#)) right in the **General features: User permissions** functional area can enable two-step verification for all users.
- Only a user that enabled two-step verification for his or her own account can enable the option of two-step verification for all users.
- Only a user that enabled two-step verification for his or her own account can exclude other user accounts from the list of two-step verification enabled for all users.

- A user can enable two-step verification only for his or her own account.
- A user account that has the Modify object ACLs (see section "Access rights to application features" on page 684) right in the **General features: User permissions** functional area and is logged in to Administration Console by using two-step verification can disable two-step verification: for any other user only if two-step verification for all users is disabled, for a user excluded from the list of two-step verification that is enabled for all users.
- Any user that logged in to Administration Console by using two-step verification can reissue his or her own secret key.
- You can enable the two-step verification for all users option for the Administration Server you are currently working with. If you enable this option on the Administration Server, you also enable this option for the user accounts of its virtual Administration Servers (on page 135) and do not enable two-step verification for the user accounts of the secondary Administration Servers.

If two-step verification is enabled for a user account on Kaspersky Security Center 13 Administration Server, the user will not be able to log in to the Kaspersky Security Center Web Console of versions 12, 12.1 or 12.2.

Enabling two-step verification for your own account

Before you enable two-step verification for your account, ensure that an authenticator application is installed on your mobile device. Ensure that the time set in the authenticator application is synchronized with the time of Administration Server.

► To enable two-step verification for your account:

1. In the Kaspersky Security Center console tree, open the context menu of the **Administration Server** folder, and then select **Properties**.
2. In the Administration Server properties window, go to the **Sections** pane and select **Advanced**, and then **Two-step verification**.
3. In the **Two-step verification** section, click the **Set up** button:
 - In the two-step verification window that opens, enter the secret key in the authenticator application or scan the QR code and receive one-time security code.
You can specify the secret key into the authenticator application manually or scan the QR code by your mobile device.
 - In the two-step verification window, specify the security code generated by the authenticator application, and then click the **OK** button.
4. Click the **Apply** button.
5. Click the **OK** button.

Two-step verification is enabled for your own account.

Enabling two-step verification for all users

You can enable two-step verification for all users of Administration Server if your account has the Modify object ACLs (see section "Access rights to application features" on page [684](#)) right in the **General features: User permissions** functional area and if you are authenticated by using two-step verification. If you did not enable two-step verification for your account before enabling it for all users, the application opens the window for enabling two-step verification for your own account (on page [627](#)).

► *To enable two-step verification for all users:*

1. In the Kaspersky Security Center console tree, open the context menu of the **Administration Server** folder, and then select **Properties**.
2. In the Administration Server properties window, in the **Sections** pane, select **Advanced**, and then **Two-step verification**.
3. Click the **Set as required** button to enable two-step verification for all users.
4. In the **Two-step verification** section, click the **Apply** button, and then click the **OK** button.

Two-step verification is enabled for all users. From now on, all users of Administration Server, including the users that were added after enabling this option, have to configure two-step verification for their accounts, except for the users whose accounts are excluded (see section "Excluding accounts from two-step verification" on page [629](#)) from two-step verification.

Disabling two-step verification for a user account

► *To disable two-step verification for your own account:*

1. In the Kaspersky Security Center console tree, open the context menu of the **Administration Server** folder, and then select **Properties**.
2. In the Administration Server properties window, in the **Sections** pane, select **Advanced**, and then **Two-step verification**.
3. In the **Two-step verification** section, click the **Disable** button.
4. Click the **Apply** button.
5. Click the **OK** button.

Two-step verification is disabled for your account.

You can disable two-step verification of other users' accounts. This provides protection in case, for example, a user loses or breaks a mobile device.

You can disable two-step verification of another user's account only if you have the Modify object ACLs (see section "Access rights to application features" on page [684](#)) right in the **General features: User permissions** functional area. Following the steps below, you can disable two-step verification for your own account as well.

► *To disable two-step verification for any user account:*

1. In the console tree, open the **User accounts** folder.

The **User accounts** folder is a subfolder of the **Advanced** folder by default.

2. In the workspace, double-click the user account for which you want to disable two-step verification.
3. In the **Properties: <user name>** window that opens, select the **Two-step verification** section.
4. In the **Two-step verification** section, select the following options:
 - If you want to disable two-step verification for a user account, click the **Disable** button.
 - If you want to exclude this user account from two-step verification, select the **User can pass authentication by using user name and password only** option.
5. Click the **Apply** button.
6. Click the **OK** button.

Two-step verification for a user account is disabled.

Disabling two-step verification for all users

You can disable two-step verification for all users of the Administration Server if you have Modify object ACLs (see section "Access rights to application features" on page 684) right in the **General features: User permissions** functional area and if you are authenticated by using two-step verification.

► *To disable two-step verification for all users:*

1. In the Kaspersky Security Center console tree, open the context menu of the **Administration Server** folder, and then select **Properties**.
2. In the Administration Server properties window, in the **Sections** pane, select **Advanced**, and then **Two-step verification**.
3. Click the **Set as optional** button to disable two-step verification for all the users.
4. Click the **Apply** button in the **Two-step verification** section.
5. Click the **OK** button in the **Two-step verification** section.

Two-step verification is disabled for all users.

Excluding accounts from two-step verification

You can exclude an account from two-step verification if your account has the Modify object ACLs (see section "Access rights to application features" on page 684) right in the **General features: User permissions** functional area.

If a user account is excluded from two-step verification, that user can log in to Administration Console without using two-step verification.

Excluding accounts from two-step verification can be necessary for service accounts that cannot pass the security code during authentication.

► *To exclude a user account from two-step verification:*

1. If you want to exclude an Active Directory account, perform Active Directory polling (on page [308](#)) to refresh the list of Administration Server users.
2. In the console tree, open the **User accounts** folder.
The **User accounts** folder is a subfolder of the **Advanced** folder by default.
3. In the workspace, double-click the user account that you want to exclude from two-step verification
4. In the **Properties: <user name>** window that opens, select the **Two-step verification** section.
5. In the opened section, select the **User can pass authentication by using user name and password only** option.
6. In the **Two-step verification** section, click the **Apply** button, and then click the **OK** button.

This user account is excluded from two-step verification. You can check the excluded accounts in the list of user accounts (see section "Working with user accounts" on page [678](#)).

Editing the name of a security code issuer

You can have several identifiers (they are called issuers) for different Administration Servers. You can change the name of a security code issuer in case, for example, the Administration Server already uses a similar name of security code issuer for another Administration Server. By default, the name of a security code issuer is the same as the name of the Administration Server.

After you change the security code issuer name you have to reissue a new secret key and pass it to the authenticator application.

► *To specify a new name of a security code issuer:*

1. In the Kaspersky Security Center console tree, open the context menu of the **Administration Server** folder, and then select **Properties**.
2. In the Administration Server properties window, in the **Sections** pane, select **Advanced**, and then **Two-step verification**.
3. Specify a new security code issuer name in the **Security code issuer** field.
4. Click the **Apply** button in the **Two-step verification** section.
5. Click the **OK** button in the **Two-step verification** section.

A new security code issuer name is specified for the Administration Server.

Managing administration groups

This section provides information about how to manage administration groups.

You can perform the following actions on administration groups:

- Add any number of nested groups at any level of hierarchy to administration groups.
- Add devices to administration groups.

- Change the hierarchy of administration groups by moving individual devices and entire groups to other groups.
- Remove nested groups and devices from administration groups.
- Add secondary and virtual Administration Servers to administration groups.
- Move devices from the administration groups of an Administration Server to those of another Server.
- Define which Kaspersky applications will be automatically installed on devices included in a group.

You can perform these actions only if you have the **Modify** permission (see section "Assigning permissions to users and groups" on page [707](#)) in the **Management of administration groups** area for the administration groups you want to manage (or for the Administration Server to which these groups belong).

In this section

Creating administration groups.....	631
Moving administration groups.....	632
Deleting administration groups	633
Automatic creation of a structure of administration groups	634
Automatic installation of applications on devices in an administration group.....	635

Creating administration groups

The hierarchy of administration groups is created in the main application window of Kaspersky Security Center in the **Managed devices** folder. Administration groups are displayed as folders in the console tree (see the figure below).

Immediately after Kaspersky Security Center installation, the **Managed devices** folder contains only an empty **Administration Servers** folder.

The user interface settings determine whether the **Administration Servers** folder appears in the console tree. To display this folder, on the menu bar select **View** → **Configure interface** and in the **Configure interface** window that opens select the **Display secondary Administration Servers** check box.

When creating a hierarchy of administration groups, you can add devices and virtual machines to the **Managed devices** folder, and add nested groups. You can add secondary and virtual Administration Servers to the **Administration Servers** folder.

Just like the **Managed devices** folder, each created group initially only contains an empty **Administration Servers** folder intended to work with secondary and virtual Administration Servers of this group. Information about policies

and tasks for this group, and information about devices included into this group, is displayed on the tabs with corresponding names in the workspace of this group.

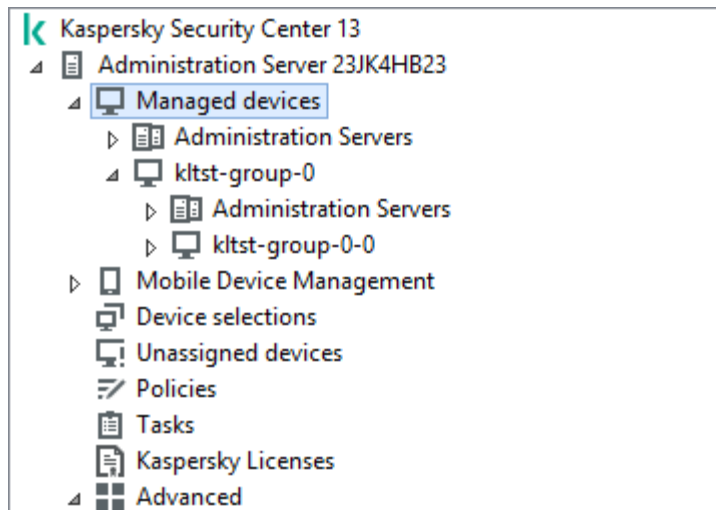


Figure 3. Viewing administration groups hierarchy

► *To create an administration group:*

1. In the console tree, expand the **Managed devices** folder.
2. If you want to create a subgroup in an existing administration group, in the **Managed devices** folder select a nested folder corresponding to the group that is to include the new administration group.
If you create a new top-level administration group, you can skip this step.
3. Start the administration group creation in one of the following ways:
 - By using the **New** → **Group** command in the context menu.
 - By clicking the **New group** button located in the workspace of the main application window, on the **Devices** tab.

4. In the **Group name** window that opens, enter a name for the group and click **OK**.

A new administration group folder with the specified name appears in the console tree.

The application allows creating a hierarchy of administration groups based on the structure of Active Directory or the domain network's structure. Also, you can create a structure of groups from a text file.

► *To create a structure of administration groups:*

1. In the console tree, select the **Managed devices** folder.
2. In the context menu of the **Managed devices** folder, select **All Tasks** → **New group structure**.

The New Administration Group Structure Wizard starts. Follow the instructions of the Wizard.

Moving administration groups

You can move nested administration groups within the groups hierarchy.

An administration group is moved together with all nested groups, secondary Administration Servers, devices, group policies, and tasks. The system will apply to the group all the settings that correspond to its new position in the hierarchy of administration groups.

The name of the group must be unique within one level of the hierarchy. If a group with the same name already exists in the folder into which you move the administration group, you should change the name of the latter. If you have not changed the name of the moved group, an index in (**<next sequence number>**) format is automatically added to its name when it is moved, for example: **(1)**, **(2)**.

You cannot rename the **Managed devices** group because it is a built-in element of Administration Console.

► *To move a group to another folder in the console tree:*

1. Select a group to move in the console tree.
2. Do one of the following:
 - Move the group by using the context menu:
 1. Select **Cut** from the context menu of the group.
 2. Select **Paste** from the context menu of the administration group to which you want to move the selected group.
 - Move the group using the main application menu:
 - a. In the main menu, select **Action** → **Cut**.
 - b. Select the administration group to which you have to move the selected group in the console tree.
 - c. In the main menu, select **Action** → **Paste**.
 - Move the group to another in the console tree using the mouse.

Deleting administration groups

You can delete an administration group if it contains no secondary Administration Servers, nested groups, or client devices, and if no group tasks or policies have been created for it.

Before deleting an administration group, you must delete all secondary Administration Servers, nested groups, and client devices from that group.

► *To delete a group:*

1. Select an administration group in the console tree.
2. Do one of the following:
 - Select **Delete** from the context menu of the group.
 - In the main application menu, select **Action** → **Delete**.
 - Press the **DELETE** key.

Automatic creation of a structure of administration groups

Kaspersky Security Center allows you to create a structure of administration groups using the Groups Hierarchy Creation Wizard.

The Wizard creates a structure of administration groups based on the following data:

- Structures of Windows domains and workgroups
- Structures of Active Directory groups
- Contents of a text file created by the administrator manually

When the text file is generated, the following requirements must be met:

- The name of each new group must begin with a new line; the delimiter must begin with a line break. Blank lines are ignored.

Example:

Office 1

Office 2

Office 3

Three groups of the first hierarchy level will be created in the target group.

- The name of the nested group must be entered with a slash mark (/).

Example:

Office 1/Division 1/Department 1/Group 1

Four subgroups nested inside each other will be created in the target group.

- To create several nested groups of the same hierarchy level, you must specify the "full path to the group".

Example:

Office 1/Division 1/Department 1

Office 1/Division 2/Department 1

Office 1/Division 3/Department 1

Office 1/Division 4/Department 1

One group of the first hierarchy level Office 1 will be created in the destination group; this group will include four nested groups of the same hierarchy level: "Division 1", "Division 2", "Division 3", and "Division 4". Each of these groups will include the "Department 1" group.

Creating the hierarchy of administration groups through the Wizard does not affect the network integrity: instead of existing groups being replaced, new groups are added. A client device cannot be included in an administration group a second time because the device is removed from the **Unassigned devices** group when it is moved to the administration group.

If, during creation of the administration group structure, a device was not included in the **Unassigned devices** group for some reason (it was shut down or disconnected from the network), the device will not be automatically moved to the administration group. You can add devices to administration groups manually after the Wizard completes.

► *To launch the automatic creation of a structure of administration groups:*

1. Select the **Managed devices** folder in the console tree.
2. In the context menu of the **Managed devices** folder, select **All Tasks** → **New group structure**.

The New Administration Group Structure Wizard starts. Follow the instructions of the Wizard.

Automatic installation of applications on devices in an administration group

You can specify which installation packages must be used for automatic remote installation of Kaspersky applications to client devices that have recently been added to a group.

► *To configure automatic installation of applications on new devices in an administration group:*

1. In the console tree, select the required administration group.
2. Open the properties window of this administration group.
3. In the **Sections** pane, select **Automatic installation**, and in the workspace select the installation packages of the applications to be installed on new devices.
4. Click **OK**.

Group tasks are created. These tasks are run on the client devices immediately after they are added to the administration group.

If some installation packages of one application are selected for automatic installation, the installation task is created for the most recent application version only.

Managing client devices

This section contains information about working with client devices.

In this section

Connecting client devices to the Administration Server	636
Manually connecting a client device to the Administration Server. Klmover utility.....	638
Tunneling the connection between a client device and the Administration Server	639
Remotely connecting to the desktop of a client device	639
Connecting to devices through Windows Desktop Sharing.....	641
Configuring the restart of a client device	641
Auditing actions on a remote client device	641
Checking the connection between a client device and the Administration Server	642
Identifying client devices on the Administration Server	644
Moving devices to an administration group	644
Changing the Administration Server for client devices.....	645
Clusters and server arrays.....	645
Turning on, turning off, and restarting client devices remotely.....	646
Access to local tasks and statistics, "Do not disconnect from the Administration Server" check box.....	646
Forced synchronization.....	646
About connection schedule	647
Sending messages to device users.....	647
Managing Kaspersky Security for Virtualization	647
Configuring the switching of device statuses	647
Tagging devices and viewing assigned tags	649
Remote diagnostics of client devices. Kaspersky Security Center remote diagnostics utility.....	651
UEFI protection devices.....	657
Settings of a managed device	658
General policy settings	663
Network Agent policy settings	665

Connecting client devices to the Administration Server

The connection of the client device to Administration Server is established by the Network Agent installed on the client device.

When a client device connects to Administration Server, the following operations are performed:

- Automatic data synchronization:
 - Synchronization of the list of applications installed on the client device.
 - Synchronization of policies, application settings, tasks, and task settings.

- Retrieval of up-to-date information about the condition of applications, execution of tasks, and applications' operation statistics by Administration Server.
- Delivery of the event information to Administration Server that is for processing.

Automatic data synchronization is performed regularly in accordance with the Network Agent settings (for example, every 15 minutes). You can specify the connection interval manually.

Information about an event is delivered to Administration Server as soon as it occurs.

If an Administration Server is remotely located outside a corporate network, client devices can connect to it over the Internet.

For devices to connect to an Administration Server over the Internet, the following conditions must be met:

- The remote Administration Server must have an external IP address and the incoming port 13000 must remain open (for connection of Network Agents). We recommend that you also open UDP port 13000 (for receiving notifications of device shut down).
- Network Agents must be installed on the devices.
- When installing Network Agent on devices, you must specify the external IP address of the remote Administration Server. If an installation package is used for installation, specify the external IP address manually in the properties of the installation package, in the **Settings** section.
- To use the remote Administration Server to manage applications and tasks for a device, in the properties window of the device, in the **General** section, select the **Do not disconnect from the Administration Server** check box. After the check box is selected, wait until the Administration Server is synchronized with the remote device. The number of client devices maintaining a continuous connection with an Administration Server cannot exceed 300.

To speed up the performance of tasks initiated by a remote Administration Server, you can open port 15000 on a device. In this case, to run a task, the Administration Server sends a special packet to Network Agent over port 15000 without waiting until completion of synchronization with the device.

Kaspersky Security Center allows you to configure connection between a client device and Administration Server so that the connection remains active after all operations are completed. Uninterrupted connection is necessary in cases when real-time monitoring of application status is required and Administration Server is unable to establish a connection to the client for some reason (for example, connection is protected by a firewall, opening of ports on the client device is not allowed, or the client device IP address is unknown). You can establish an uninterrupted connection between a client device and Administration Server in the device properties window in the **General** section.

We recommend that you establish an uninterrupted connection with the most important devices. The total number of connections simultaneously maintained by the Administration Server is limited to 300.

When synchronized manually, the system uses an auxiliary connection method that allows connection initiated by Administration Server. Before establishing the connection on a client device, you must open the UDP port. Administration Server sends a connection request to the UDP port of the client device. In response, the Administration Server's certificate is verified. If the Administration Server certificate matches the certificate copy stored on the client device, the connection is established.

The manual launch of synchronization is also used for obtaining up-to-date information about the condition of applications, execution of tasks, and operation statistics of applications.

Manually connecting a client device to the Administration Server. Klmover utility

If you have to manually connect a client device to the Administration Server, you can use the klmover utility on the client device.

When Network Agent is installed on a client device, the utility is automatically copied to the Network Agent installation folder.

► *To manually connect a client device to the Administration Server by using the klmover utility:*

On the device, start the klmover utility from the command line.

When started from the command line, the klmover utility can perform the following actions (depending on which keys are in use):

- Connects Network Agent to Administration Server with the specified settings;
- Records the operation results in the event log file or displays them on the screen.

Utility command line syntax:

```
klmover [-logfile <file name>] [-address <server address>] [-pn <port number>] [-ps <SSL port number>] [-noSSL] [-cert <path to certificate file>] [-silent] [-dupfix]
```

Descriptions of the keys:

- `-logfile <file name>`—Record the utility run results in a log file.
By default, information is saved in the standard output stream (stdout). If the key is not in use, results and error messages are displayed on the screen.
- `-address <server address>`—Address of the Administration Server for connection.
You can specify an IP address, the NetBIOS name, or the DNS name of a device as its address.
- `-pn <port number>`—Number of the port through which non-encrypted connection to the Administration Server is established.
The default port number is 14000.
- `-ps <SSL port number>`—Number of the SSL port through which encrypted connection to the Administration Server is established using SSL.
The default port number is 13000.
- `-noSSL`—Use non-encrypted connection to the Administration Server.
If the key is not in use, Network Agent is connected to Administration Server by using encrypted SSL protocol.
- `-cert <path to certificate file>`—Use the specified certificate file for authentication of access to Administration Server.
If the key is not in use, Network Agent receives a certificate at the first connection to Administration Server.
- `-silent`—Run the utility in silent mode.

Using the key may be useful if, for example, the utility is started from the logon script at the user's registration.

- `-dupfix`—The key is used if Network Agent has been installed using a method that differs from the usual one (with the distribution package)—for example, by recovering it from an ISO disk image.

Tunneling the connection between a client device and the Administration Server

Kaspersky Security Center allows tunneling TCP connections from Administration Console via the Administration Server and then via Network Agent to a specified port on a managed device. Tunneling is designed for connecting a client application on a device with Administration Console installed to a TCP port on a managed device—if no direct connection is possible between Administration Console and the target device.

For example, tunneling is used for connections to a remote desktop, both for connecting to an existing session, and for creating a new remote session.

Tunneling can also be enabled by using external tools. For example, the administrator can run the putty utility, the VNC client, and other tools in this way.

Connection tunneling between a remote client device and Administration Server is required if the port used for connection to Administration Server is not available on the device. The port on the device may be unavailable in the following cases:

- The remote device is connected to a local network that uses the NAT mechanism.
- The remote device is part of the local network of Administration Server, but its port is closed by a firewall.

► *To tunnel the connection between a client device and Administration Server:*

1. In the console tree, select the folder of the group that contains the client device.
2. On the **Devices** tab, select the device.
3. In the context menu of the device, select **All tasks** → **Connection Tunneling**.
4. In the **Connection Tunneling** window that opens, create a tunnel.

Remotely connecting to the desktop of a client device

The administrator can obtain remote access to the desktop of a client device through a Network Agent installed on the device. Remote connection to a device through the Network Agent is possible even if the TCP and UDP ports of the client device are closed.

Upon establishing the connection with the device, the administrator gains full access to information stored on this device and can manage applications installed on it.

Remote connection with a device can be established in one of the following ways:

- By using a standard Microsoft Windows component named Remote Desktop Connection. Connection to a remote desktop is established through the standard Windows utility `mstsc.exe` in accordance with the utility's settings.
Connection to the current remote desktop session of the user is established without the user's knowledge. Once the administrator connects to the session, the device user is disconnected from the session without an advance notification.
- By using the Windows Desktop Sharing technology. When connecting to an existing session of the remote desktop, the session user on the device receives a connection request from the administrator. No

information about remote activity on the device and its results will be saved in reports created by Kaspersky Security Center.

The administrator can connect to an existing session on a client device without disconnecting the user in this session. In this case, the administrator and the session user on the device share access to the desktop.

The administrator can configure an audit of user activity on a remote client device. During the audit, the application saves information about files on the client device that have been opened and/or modified by the administrator (see section "Auditing actions on a remote client device" on page [641](#)).

To connect to the desktop of a client device through Windows Desktop Sharing, the following conditions must be met:

- Microsoft Windows Vista or a later Windows operating system is installed on the client device.
- Microsoft Windows Vista or a later Windows operating system is installed on the administrator's workstation. The type of operating system of the device hosting Administration Server imposes no restrictions on connection through Windows Desktop Sharing.
- Kaspersky Security Center uses a license for Vulnerability and Patch Management.

► *To connect to the desktop of a client device through the Remote Desktop Connection component:*

1. In the Administration Console tree, select the device to which you need to obtain access.
2. In the context menu of the device, select **All tasks** → **Connect to device** → **New RDP session**.

The standard Windows utility mstsc.exe starts, which helps to connect to the remote desktop.

3. Follow the instructions shown in the utility's dialog boxes.

Upon connection to the device is established, the desktop is available in the remote connection window of Microsoft Windows.

► *To connect to the desktop of a client device through Windows Desktop Sharing:*

1. In the Administration Console tree, select the device to which you need to obtain access.
2. In the context menu of the device, select **All tasks** → **Connect to device** → **Windows Desktop Sharing**.
3. In the **Select remote desktop session** window that opens, select the session on the device to which you need to connect.

If connection to the device is established successfully, the desktop of the device will be available in the **Kaspersky Remote Desktop Session Viewer** window.

4. To start interacting with the device, in the main menu of the **Kaspersky Remote Desktop Session Viewer** window, select **Actions** → **Interactive mode**.

See also:

| Kaspersky Security Center licensing options [320](#)

Connecting to devices through Windows Desktop Sharing

► *To connect to a device through Windows Desktop Sharing:*

1. In the console tree, on the **Devices** tab, select the **Managed devices** folder.
The workspace of this folder displays a list of devices.
2. In the context menu of the device to which you want to connect, select **Connect to device** → **Windows Desktop Sharing**.
The **Select remote desktop session** window opens.
3. In the **Select remote desktop session** window, select a desktop session for connection to the device.
4. Click **OK**.
The device is connected.

Configuring the restart of a client device

When using, installing, or removing Kaspersky Security Center, you may have to restart the device. You can specify the restart settings only for devices running Windows.

► *To configure the restart of a client device:*

1. In the console tree, select the administration group for which you have to configure the restart.
2. In the workspace of the group, select the **Policies** tab.
3. In the workspace, select a policy of Kaspersky Security Center Network Agent in the list of policies, and then select **Properties** in the context menu of the policy.
4. In the properties window of the policy, select the **Restart management** section.
5. Select the action that must be performed if a restart of the device is required:
 - Select **Do not restart the operating system** to block automatic restart.
 - Select **Restart the operating system automatically if necessary** to allow automatic restart.
 - Select **Prompt user for action** to enable prompting the user to allow the restart.

You can specify the frequency of restart requests, and enable forced restart and forced closure of applications in blocked sessions on the device by selecting the corresponding check boxes and time settings in spin boxes.

6. Click **OK** to save changes and close the policy properties window.

Restart of the device will now be configured.

Auditing actions on a remote client device

The application enables auditing of the administrator's actions on a remote client devices running Windows. During the audit, the application saves, on the device, information about files that have been opened and/or modified by the administrator. Audit of the administrator's actions is available when the following conditions are met:

- The Vulnerability and Patch Management license is in use.
- The administrator has the right to start shared access to the desktop of the remote device.

► *To enable auditing of actions on a remote client device:*

1. In the console tree, select the administration group for which the audit of the administrator's actions should be configured.
2. In the workspace of the group, select the **Policies** tab.
3. Select a policy of Kaspersky Security Center Network Agent, then select **Properties** in the context menu of the policy.
4. In the policy properties window, select the **Windows Desktop Sharing** section.
5. Select the **Enable audit** check box.
6. In the **Masks of files to monitor when read** and **Masks of files to monitor when modified** lists, add file masks on which the application must monitor actions during the audit.
By default, the application monitors actions on files with .txt, .rtf, .doc, .xls, .docx, .xlsx, .odt, and .pdf extensions.
7. Click **OK** to save changes and close the policy properties window.

This results in configuration of the audit of the administrator's actions on the user's remote device with shared desktop access.

Records of the administrator's actions on the remote device are logged:

- In the event log on the remote device.
- In a file with the syslog extension located in the Network Agent folder on a remote device (for example, C:\ProgramData\KasperskyLab\adminkit\1103\logs).
- In the events database of Kaspersky Security Center.

Checking the connection between a client device and the Administration Server

Kaspersky Security Center allows you to check connections between a client device and the Administration Server, automatically or manually.

Automatic check of connection is performed on Administration Server. Manual check of the connection is performed on the device.

In this section

Automatically checking the connection between a client device and the Administration Server	642
Manually checking the connection between a client device and the Administration Server. Klnagchk utility	643
Checking the time of connection between a device and the Administration Server	643

Automatically checking the connection between a client device and the Administration Server

► *To start an automatic check of the connection between a client device and Administration Server:*

1. In the console tree, select the administration group that includes the device.
2. In the workspace of the administration group, on the **Devices** tab, select the device.
3. In the context menu of the device, select **Check device accessibility**.

A window opens that contains information about the accessibility of the device.

Manually checking the connection between a client device and the Administration Server. Klnagchk utility

You can check the connection and obtain detailed information about the settings of the connection between a client device and Administration Server by using the klnagchk utility.

When Network Agent is installed on a device, the klnagchk utility is automatically copied to the Network Agent installation folder.

When started from the command line, the klnagchk utility can perform the following actions (depending on the keys in use):

- Displays on the screen or logs the values of the settings used for connecting the Network Agent installed on the device to Administration Server.
- Records into an event log file Network Agent statistics (since its last startup) and utility operation results, or displays the information on the screen.
- Makes an attempt to establish connection between Network Agent and Administration Server.
If the connection attempt fails, the utility sends an ICMP packet to check the status of the device on which Administration Server is installed.

► *To check the connection between a client device and Administration Server using the klnagchk utility:*

On the device, start the klnagchk utility from the command line.

Utility command line syntax:

```
klnagchk [-logfile <file name>] [-sp] [-savecert <path to certificate file>] [-restart]
```

Descriptions of the keys:

- `-logfile <file name>` —Record in a log file the values of the settings of connection between Network Agent and Administration Server and the utility operation results.
By default, information is saved in the standard output stream (stdout). If the key is not in use, settings, results, and error messages are displayed on the screen.
- `-sp` —Show the password for the user's authentication on the proxy server.
The setting is in use if connection to the Administration Server is established through a proxy server.
- `-savecert <file name>` —Save the certificate, used to access the Administration Server, in the specified file.
- `-restart` —Restart Network Agent after the utility has completed.

Checking the time of connection between a device and the Administration Server

Upon shutting down a device, Network Agent notifies the Administration Server of this event. In Administration Console, that device is displayed as shut down. However, Network Agent cannot notify Administration Server of all such events. The Administration Server, therefore, periodically analyzes the **Connected to Administration Server** attribute (the value of this attribute is displayed in Administration Console, in the device properties, in the **General** section) for each device and compares it against the synchronization interval from the current settings of Network

Agent. If a device has not responded over more than three successive synchronization intervals, that device is marked as shut down.

Identifying client devices on the Administration Server

Client devices are identified based on their names. A device name is unique among all the names of devices connected to Administration Server.

The name of a device is relayed to Administration Server either when the Windows network is polled and a new device is discovered in it, or at the first connection of Network Agent installed on a device to Administration Server. By default, the name matches the device name in the Windows network (NetBIOS name). If a device with this name is already registered on the Administration Server, an index with the next sequence number will be added to the new device name, for example: <Name>-1, <Name>-2. Under this name, the device is added to the administration group.

Moving devices to an administration group

You can move devices from one administration group to another only if you have the **Modify** permission (see section "Assigning permissions to users and groups" on page [707](#)) in the **Management of administration groups** area for both source and target administration groups (or for the Administration Server to which these groups belong).

► *To include one or several devices in a selected administration group:*

1. In the console tree, expand the **Managed devices** folder.
2. In the **Managed devices** folder, select the nested folder that corresponds to the group in which the client devices will be included.

If you want to include the devices in the **Managed devices** group, you can skip this step.

3. In the workspace of the selected administration group, on the **Devices** tab, start the process of including the devices in the group in one of the following ways:
 - By adding the devices to the group by clicking the **Move devices to group** button in the information box for the list of devices.
 - By selecting **Create** → **Device** in the context menu of the list of devices.

The Move Devices Wizard starts. Following its instructions, select a method for moving the devices to the group and create a list of devices to include in the group.

If you create the list of devices manually, you can use an IP address (or an IP range), a NetBIOS name, or a DNS name as the address of a device. You can manually move to the list only devices for which information has already been added to the Administration Server database upon connection of the device, or after device discovery.

To import a list of devices from a file, specify a .txt file with a list of addresses of the devices to be added. Each address must be specified in a separate line.

After the wizard completes, the selected devices are included in the administration group and are displayed in the list of devices under names generated by Administration Server.

You can move a device to the selected administration group by dragging it from the **Unassigned devices** folder to the folder of that administration group.

Changing the Administration Server for client devices

You can change the Administration Server that manages client devices to a different Server using the **Change Administration Server** task.

► *To change the Administration Server that manages client devices to a different Server:*

1. Connect to the Administration Server that manages the devices.
2. Create the Administration Server change task in one of the following ways:
 - If you need to change the Administration Server for devices included in the selected administration group, create a task for the selected group (see section "Creating a task" on page [374](#)).
 - If you need to change the Administration Server for devices included in different administration groups or in none of the existing administration groups, create a task for specific devices (see section "Creating a task for specific devices" on page [376](#)).

The New Task Wizard starts. Follow the instructions of the Wizard. In the **Select the task type** window of the New Task Wizard, select the **Kaspersky Security Center** node, open the **Advanced** folder, and select the **Change Administration Server** task.

3. Run the created task.

After the task is complete, the client devices for which it was created are put under the management of the Administration Server specified in the task settings.

If the Administration Server supports encryption and data protection and you are creating a **Change Administration Server** task, a warning is displayed. The warning states that if any encrypted data is stored on devices, after the new Server begins managing the devices, users will be able to access only the encrypted data with which they previously worked. In other cases, no access to encrypted data is provided. For detailed descriptions of scenarios in which access to encrypted data is not provided, please refer to the Kaspersky Endpoint Security for Windows Online Help <https://support.kaspersky.com/KESWin/11.6.0/en-US/127971.htm>.

Clusters and server arrays

Kaspersky Security Center supports the cluster technology. If Network Agent sends information to Administration Server confirming that an application installed on a client device is part of a server array, this client device becomes a cluster node. The cluster will be added as an individual object in the **Managed devices** folder of the console tree

with the  icon.

A few typical features of a cluster can be distinguished:

- A cluster and any of its nodes are always in the same administration group.
- If the administrator attempts to move a cluster node, the node moves back to its original location.

- If the administrator attempts to move a cluster to a different group, all of its nodes move with it.

Turning on, turning off, and restarting client devices remotely

Kaspersky Security Center allows you to manage client devices remotely by turning on, shutting down, or restarting them.

► *To remotely manage client devices:*

1. Connect to the Administration Server that manages the devices.
2. Create a device management task in one of the following ways:
 - If you need to turn on, turn off or restart devices that are included in the selected administration group, create a task for the selected group (see section "Creating a task" on page [374](#)).
 - If you have to turn on, turn off or restart devices that are included in various administration groups or belong to none of them, create a task for specific devices (see section "Creating a task for specific devices" on page [376](#)).

The New Task Wizard starts. Follow the instructions of the Wizard. In the **Select the task type** window of the New Task Wizard, select the **Kaspersky Security Center** node, open the **Advanced** folder, and select the **Manage devices** task.

3. Run the created task.

After the task is complete, the command (turn on, turn off, or restart) will be executed on the selected devices.

Access to local tasks and statistics, "Do not disconnect from the Administration Server" check box

By default, Kaspersky Security Center does not feature continuous connectivity between managed devices and the Administration Server. Network Agents on managed devices periodically establish connections and synchronize with the Administration Server. The interval between those synchronization sessions (by default, it is 15 minutes) is defined in a policy of Network Agent. If an early synchronization is required (for example, to force the application of a policy), the Administration Server sends Network Agent a signed network packet to port UDP 15000. If no connection through UDP is possible between the Administration Server and a managed device for any reason, synchronization will run at the next routine connection between Network Agent and the Administration Server within the synchronization interval.

Some operations cannot be performed without an early connection between Network Agent and the Administration Server, such as running and stopping local tasks, receiving statistics for a managed application (security application or Network Agent), creating a tunnel, etc. To resolve this issue, in the properties of the managed device (**General** section), select the **Do not disconnect from the Administration Server** check box. The maximum total number of devices with the **Do not disconnect from the Administration Server** check box selected is 300.

Forced synchronization

Although Kaspersky Security Center automatically synchronizes the status, settings, tasks, and policies for managed devices, in some cases the administrator needs to know exactly whether synchronization has already been performed for a specified device at the present moment.

In the context menu of managed devices in Administration Console, the **All tasks** menu item contains the **Force synchronization** command. When Kaspersky Security Center 13 executes this command, the Administration Server attempts to connect to the device. If this attempt is successful, forced synchronization will be performed.

Otherwise, synchronization will be forced only after the next scheduled connection between Network Agent and the Administration Server.

About connection schedule

In the Network Agent properties window, in the **Connectivity** section, in the **Connection schedule** subsection, you can specify time intervals during which Network Agent will transmit data to the Administration Server.

Connect when necessary. If this option is selected, the connection is established when Network Agent has to send data to the Administration Server.

Connect at specified time intervals. If this option is selected, Network Agent connects to the Administration Server at a specified time. You can add several connection time periods.

Sending messages to device users

► *To send a message to users of devices:*

1. In the console tree, select the node with the name of the required Administration Server.
2. Create a message sending task for device users in one of the following ways:
 - If you want to send a message to the users of devices that belong to the selected administration group, create a task for the selected group (see section "Creating a task" on page [374](#)).
 - If you want to send a message to the users of devices that belong to different administration groups or that do not belong to any administration groups, create a task for specific devices (see section "Creating a task for specific devices" on page [376](#)).

The New Task Wizard starts. Follow the instructions of the Wizard.

3. In the task type window of the New Task Wizard, select the **Kaspersky Security Center 13 Administration Server** node, open the **Advanced** folder, and select the **Send message to user** task. The send messages to user task is available only for devices running Windows. You can also send messages in the user's context menu in the **User accounts** folder (see section "Delivering messages to users" on page [710](#)).
4. Run the created task.

After the task is complete, the created message will be sent to the users of the selected devices. The send messages to user task is available only for devices running Windows. You can also send messages in the user's context menu in the **User accounts** folder (see section "Delivering messages to users" on page [710](#)).

Managing Kaspersky Security for Virtualization

Kaspersky Security Center supports the option of connection of virtual machines to the Administration Server. Virtual machines are managed through Kaspersky Security for Virtualization. For more details, please refer to the documentation for this application.

Configuring the switching of device statuses

You can change conditions to assign the *Critical* or *Warning* status to a device.

► *To enable changing the device status to Critical:*

1. Open the properties window in one of the following ways:
 - In the **Policies** folder, in the context menu of an Administration Server policy, select **Properties**.
 - Select **Properties** in the context menu of an administration group.
2. In the properties window that opens, in the **Sections** pane, select **Device status**.
3. In the right pane, in the **Set to Critical if these are specified** section, select the check box next to a condition in the list.

You can change only settings that are not locked in the parent policy (see section "Hierarchy of policies" on page [385](#)).

4. Set the required value for the selected condition.
You can set values for some, but not all, conditions.
5. Click **OK**.

When specified conditions are met, the managed device is assigned the *Critical* status.

► *To enable changing the device status to Warning:*

1. Open the properties window in one of the following ways:
 - In the **Policies** folder, in the context menu of the Administration Server policy, select **Properties**.
 - Select **Properties** in the context menu of the administration group.
2. In the properties window that opens, in the **Sections** pane select **Device status**.
3. In the right pane, in the **Set to Warning if these are specified** section select the check box next to a condition in the list.

You can change only settings that are not locked in the parent policy (see section "Hierarchy of policies" on page [385](#)).

4. Set the required value for the selected condition.
You can set values for some, but not all, conditions.
5. Click **OK**.

When specified conditions are met, the managed device is assigned the *Warning* status.



See also:

| Adjusting the general settings of Administration Server[609](#)

Tagging devices and viewing assigned tags

Kaspersky Security Center allows you to tag devices. A *tag* is the ID of a device that can be used for grouping, describing, or finding devices. Tags assigned to devices can be used for creating selections, for finding devices, and for distributing devices among administration groups.

You can tag devices manually or automatically. Tag a device manually in the device properties; you may use manual tagging when you have to tag an individual device. Auto-tagging is performed by Administration Server in accordance with the specified tagging rules.

In the properties of an Administration Server, you can set up auto-tagging for devices managed by this Administration Server. Devices are tagged automatically when specified rules are met. An individual rule corresponds to each tag. Rules are applied to the network properties of the device, operating system, applications installed on the device, and other device properties. For example, you can set up a rule that will assign the *Win* tag to all devices running Windows. Then, you can use this tag when creating a device selection; this will help you sort out all devices running Windows, and assign them a task.

You can also use tags as conditions of policy profile activation on a managed device in order to apply specific policy profiles only on devices with specific tags. For example, if a device tagged as *Courier* appears in the *Users* administration group and if activation of the corresponding policy profile by the *Courier* tag has been enabled, then the policy created for the *Users* group will not be applied to this device—but the profile of the policy profile will be applied. The policy profile can allow this device to start some applications that have been blocked from running by the policy.

You can create multiple tagging rules. A single device can be assigned multiple tags if you have created multiple tagging rules and if the respective conditions of these rules are met simultaneously. You can view the list of all assigned tags in the device properties. Each tagging rule can be enabled or disabled. If a rule is enabled, it is applied to devices managed by Administration Server. If you are not using a rule currently but may need it in the future, you do not have to remove it; you can simply clear the **Enable rule** check box instead. In this case, the rule is disabled; it will not be executed until the **Enable rule** check box is selected again. You may need to disable a rule without removing it if you have to exclude the rule from the list of tagging rules temporarily and then include it again.

In this section

Automatic device tagging.....	649
Viewing and configuring tags assigned to a device.....	650

Automatic device tagging

You can create and edit automatic tagging rules in the Administration Server properties window.

► To tag devices automatically:

1. In the console tree, select the node with the name of the Administration Server for which you have to specify tagging rules.
2. In the context menu of the Administration Server, select **Properties**.
3. In the Administration Server properties window, select the **Tagging rules** section.
4. In the **Tagging rules** section, click the **Add** button.

The **New rule** window opens.

5. In the **New rule** window, configure the general properties of the rule:

- Specify the rule name.

The rule name cannot be more than 255 characters long and cannot include any special characters (such as "*<>? \ : |).

- Enable or disable the rule using the **Enable rule** check box.

By default, the **Enable rule** check box is selected.

- In the **Tag** field, enter a tag name.

The tag name cannot be more than 255 characters long and cannot include any special characters (such as "*<>? \ : |).

6. In the **Conditions** section, click the **Add** button to add a new condition, or click the **Properties** button to edit an existing condition.

The New Auto-Tagging Rule Condition Wizard window opens.

7. In the **Tag assignment condition** window, select the check boxes for the conditions that must affect tagging. You can select multiple conditions.

8. Depending on which tagging conditions you selected, the Wizard displays the windows for setup of the corresponding conditions. Set up the triggering of the rule by the following conditions:

- **Device's use or association with a specific network**—Network properties of the device, such as device name in the Windows network, and device inclusion in a domain or an IP subnet.
- **Use of Active Directory**—Presence of the device in an Active Directory organizational unit and membership of the device in an Active Directory group.
- **Specific applications**—Presence of Network Agent on the device, operating system type, version, and architecture.
- **Virtual machines**—Inclusion of the device in a specific type of virtual machines.
- **Application from the applications registry installed**—Presence of applications of different vendors on the device.

9. After the condition is set up, enter a name for it, and then close the Wizard.

If necessary, you can set multiple conditions for a single rule. In this case, the tag will be assigned to a device if it meets at least one condition. The conditions that you added will be displayed in the rule properties window.

10. Click **OK** in the **New rule** window, then click **OK** in the Administration Server properties window.

The newly created rules are enforced on devices managed by the selected Administration Server. If the settings of a device meet the rule conditions, the device is assigned the tag.

Viewing and configuring tags assigned to a device

You can view the list of all tags that have been assigned to a device, as well as proceed to set up automatic tagging rules in the device properties window.

► *To view and set up the tags that have been assigned to a device:*

1. In the console tree, open the **Managed devices** folder.

2. In the workspace of the **Managed devices** folder, select the device for which you want to view the assigned tags.
3. In the context menu of the mobile device, select **Properties**.
4. In the device properties window, select the **Tags** section.

A list of tags assigned to the selected device is displayed, as well as the way in which each of the tags were assigned: manually or by a rule.

5. If necessary, perform one of the following actions:
 - To proceed to setup of tagging rules, click the **Set up auto-tagging rules** link (only for Windows).
 - To rename a tag, select one and click the **Rename** button.
 - To remove a tag, select one and click the **Remove** button.
 - To add a tag manually, enter one in the field in the lower part of the **Tags** section and click the **Add** button.
6. Click the **Apply** button, if you have made changes to the **Tags** section, for your changes to take effect.
7. Click **OK**.

If you removed or renamed a tag in the device properties, this change will not affect the tagging rules that have been set up in the Administration Server properties. The change will only apply to the device whose properties it has been made.

Remote diagnostics of client devices. Kaspersky Security Center remote diagnostics utility

The utility for remote diagnostics of Kaspersky Security Center (hereinafter referred to as the remote diagnostics utility) is designed for remote execution of the following operations on client devices:

- Enabling and disabling tracing, changing the tracing level, downloading the trace file.
- Downloading system information and application settings.
- Downloading event logs.
- Generating a dump file for an application.
- Starting diagnostics and downloading diagnostics reports.
- Starting and stopping applications.

You can use event logs and diagnostics reports downloaded from a client device to troubleshoot problems on your own. Also, a Kaspersky Technical Support specialist might ask you to download trace files, dump files, event logs, and diagnostics reports from a client device for further analysis at Kaspersky.

The remote diagnostics utility is automatically installed on the device together with Administration Console.

In this section

Connecting the remote diagnostics utility to a client device	652
Enabling and disabling tracing, downloading the trace file.....	654
Downloading application settings	656
Downloading event logs.....	656
Downloading multiple diagnostic information items.....	656
Starting diagnostics and downloading the results	657
Starting, stopping, and restarting applications	657

Connecting the remote diagnostics utility to a client device

► *To connect the remote diagnostics utility to a client device:*

1. Select any administration group in the console tree.
2. In the workspace, on the **Devices** tab, in the context menu of any device select **Custom tools** → **Remote diagnostics**.

The main window of the remote diagnostics utility opens.

3. In the first field of the main window of the remote diagnostics utility, specify which tools you intend to use to connect to the device:
 - **Access using Microsoft Windows network.**
 - **Access using Administration Server.**
4. If you have selected **Access using Microsoft Windows network** in the first field of the main utility window, perform the following actions:
 - In the **Device** field, specify the address of the device to which you need to connect
You can use an IP address, NetBIOS name, or DNS name as the device address.
The default value is the address of the device from whose context menu the utility was started.
 - Specify an account for connecting to the device:
 - **Connect as current user** (selected by default). Connecting under the current user account.
 - **Use provided user name and password to connect.** Connecting under a provided user account. Specify the **User name** and the **Password** of the required account.

Connection to a device is possible only under the account of the local administrator of the device.

5. If you have selected **Access using Administration Server** in the first field of the main utility window, perform the following actions:
 - In the **Administration Server** field, specify the address of the Administration Server from which you intend to connect to the device.
You can use an IP address, NetBIOS name, or DNS name as the server address.

The default value is the address of the Administration Server from which the utility has been run.

- If required, select the **Use SSL**, **Compress traffic**, and **Device belongs to secondary Administration Server** check boxes.

If the **Device belongs to secondary Administration Server** check box is selected, you can fill in the **Device belongs to secondary Administration Server** field with the name of the secondary Administration Server that manages the device by clicking the **Browse** button.

6. To connect to the device, click the **Sign in** button.

This opens the window intended for remote diagnostics of the device (see the figure below). The left part of the window contains links to operations of device diagnostics. The right part of the window contains the object tree of the device with which the utility can operate. The lower part of the window displays the progress of the utility operations.

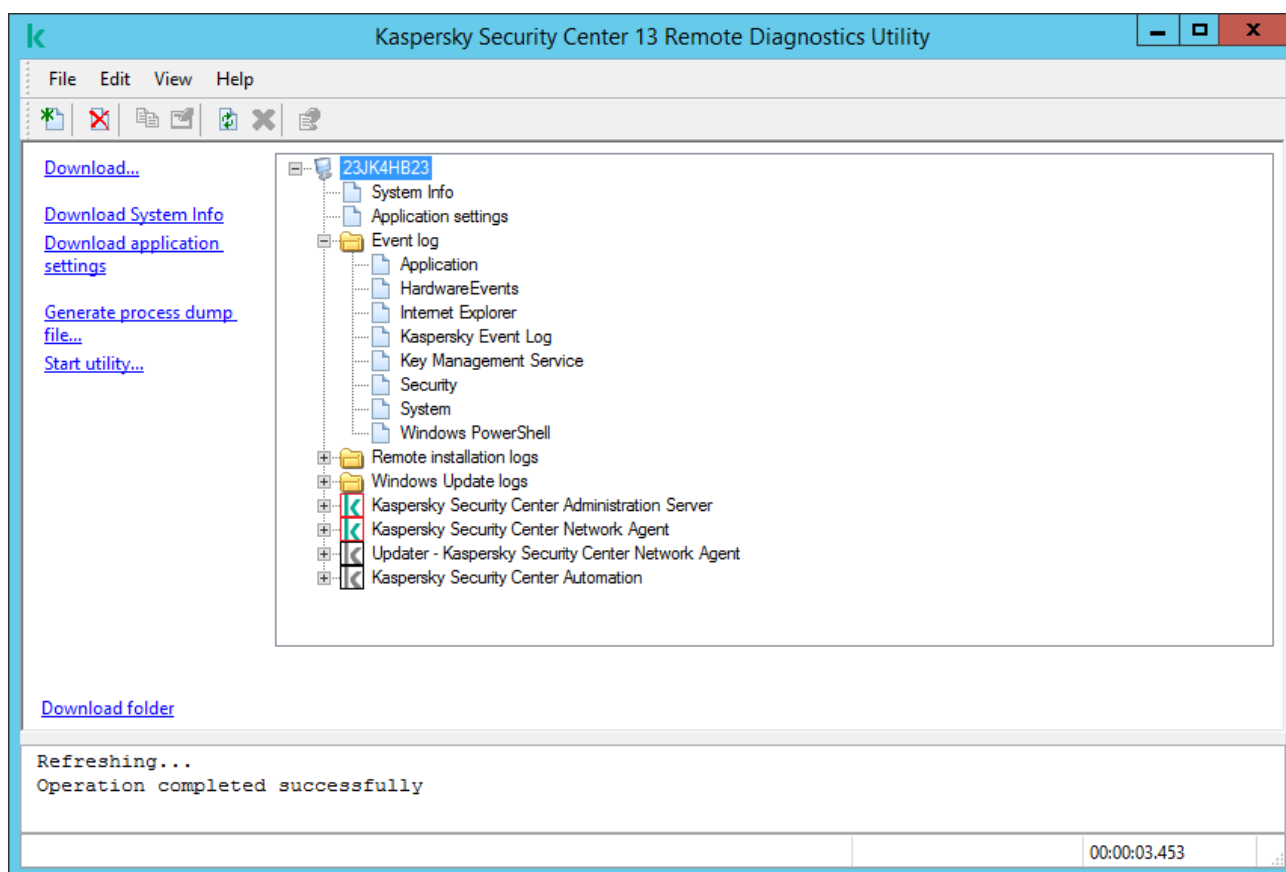


Figure 4. Remote diagnostics utility. Remote device diagnostics window

The remote diagnostics utility saves files downloaded from devices on the desktop of the device from which it was started.

Enabling and disabling tracing, downloading the trace file

► *To enable tracing on a remote device:*

1. Run the remote diagnostics utility and connect to the necessary device (see section "Connecting the remote diagnostics utility to a client device" on page [652](#)).
2. In the objects tree of the device, select the application for which you want to enable tracing.

Tracing can be enabled and disabled for applications with self-defense only if the device is connected using Administration Server tools.

If you want to enable tracing for Network Agent, you can also do it while creating the Install required updates and fix vulnerabilities (see section "Fixing vulnerabilities in applications" on page [469](#)) task. In this case, Network Agent will write the tracing information even if tracing is disabled for Network Agent in the remote diagnostics utility.

3. To enable tracing:
 - a. In the left part of the remote diagnostics utility window, click **Enable tracing**.
 - b. In the **Select tracing level** window that opens, we recommend that you keep the default values of the settings. When required, a Technical Support specialist will guide you through the configuration process. The following settings are available:
 - **Tracing level**

The tracing level defines the amount of detail that the trace file contains.

- **Rotation-based tracing** (available for Kaspersky Endpoint Security only)

The application overwrites the tracing information to prevent excessive increase in the size of the trace file. Specify the maximum number of files to be used to store the tracing information, and the maximum size of each file. If the maximum number of trace files of the maximum size are written, the oldest trace file is deleted so that a new trace file can be written.

- a. Click **OK**.

1. For Kaspersky Endpoint Security, a Technical Support specialist may ask you to enable Xperf tracing for information about the system performance.

To enable Xperf tracing:

- a. In the left part of the remote diagnostics utility window, click **Enable Xperf tracing**.
- b. In the **Select tracing level** window that opens, depending on the request from the Technical Support specialist, select one of the following tracing levels:

- **Light level**

A trace file of this type contains the minimum amount of information about the system.

By default, this option is selected.

- **Deep level**

A trace file of this type contains more detailed information than trace files of the *Light* type and may be requested by Technical Support specialists when a trace file of the *Light* type is not enough for the performance evaluation. A *Deep* trace file contains technical information about the system including information about hardware, operating system, list of started and finished processes and applications, events used for performance

evaluation, and events from Windows System Assessment Tool.

c. Select one of the following tracing types:

- **Basic type**

The tracing information is received during operation of the Kaspersky Endpoint Security application.

By default, this option is selected.

- **On-restart type**

The tracing information is received when the operating system starts on the managed device. This tracing type is effective when the issue that affects the system performance occurs after the device is turned on and before Kaspersky Endpoint Security starts.

d. You may also be asked to enable the **Rotation-based tracing** option to prevent excessive increase in the size of the trace file. Then specify the maximum size of the trace file. When the file reaches the maximum size, the oldest tracing information is overwritten with new information.

e. Click **OK**.

In some cases, the security application and its task must be restarted in order to enable tracing.

The remote diagnostics utility enables tracing for the selected application.

► *To download a trace file of an application:*

1. Run the remote diagnostics utility and connect to the necessary device, as described in "Connecting the remote diagnostics utility to a client device (on page [652](#))".
2. In the node of the application, in the **Trace files** folder, select the required file.
3. In the left part of the remote diagnostics utility window, click **Download entire file**.

For large files the most recent trace parts can be downloaded.

You can delete the highlighted trace file. The file can be deleted after tracing is disabled.

The selected file is downloaded to the location specified in the lower part of the window.

► *To disable tracing on a remote device:*

1. Run the remote diagnostics utility and connect to the necessary device, as described in "Connecting the remote diagnostics utility to a client device (on page [652](#))".
2. In the device object tree, select the application for which you want to disable tracing.

Tracing can be enabled and disabled for applications with self-defense only if the device is connected using Administration Server tools.

3. In the left part of the remote diagnostics utility window, click **Disable tracing**.

The remote diagnostics utility disables tracing for the selected application.

Downloading application settings

► *To download application settings from a remote device:*

1. Run the remote diagnostics utility and connect to the necessary device, as described in "Connecting the remote diagnostics utility to a client device (on page [652](#))".
2. In the objects tree of the remote diagnostics utility window, select the top node with the name of the device.
3. In the left part of the remote diagnostics utility window, select the action you need from the following options:

- **Download System Info**
- **Download application settings**
- **Generate process dump file**

In the window that opens after you click this link, specify the executable file of the application for which you want to generate a dump file.

- **Start utility**

In the window that opens after you click this link, specify the executable file of the utility that you want to start, and its run settings.

The selected utility is downloaded and launched on the device.

Downloading event logs

► *To download an event log from a remote device:*

1. Run the remote diagnostics utility and connect to the necessary device, as described in "Connecting the remote diagnostics utility to a client device (on page [652](#))".
2. In the **Event log** folder of the device object tree, select the relevant log.
3. Download the selected log by clicking the **Download event log <Event log name>** link in the left part of the remote diagnostics utility window.

The selected event log is downloaded to the location specified in the lower pane.

Downloading multiple diagnostic information items

Kaspersky Security Center remote diagnostics utility allows you to download multiple items of diagnostic information including event logs, system information, trace files, and dump files.

► *To download diagnostic information from a remote device:*

1. Run the remote diagnostics utility and connect to the necessary device, as described in "Connecting the remote diagnostics utility to a client device (on page [652](#))".
2. In the left part of the remote diagnostics utility window, click **Download**.
3. Select the check boxes next to the items that you want to download.
4. Click **Start**.

Every selected item is downloaded to the location specified in the lower pane.

Starting diagnostics and downloading the results

► *To start diagnostics for an application on a remote device and download the results:*

1. Run the remote diagnostics utility and connect to the necessary device, as described in "Connecting the remote diagnostics utility to a client device (on page [652](#))".
2. In the object tree of the device, select the necessary application.
3. Start diagnostics by clicking the **Run diagnostics** link in the left part of the remote diagnostics utility window.

A diagnostics report appears in the node of the selected application in the object tree.

4. Select the newly generated diagnostics report in the objects tree and download it by clicking the **Download folder** link.

The selected report is downloaded to the location specified in the lower pane.

Starting, stopping, and restarting applications

You can start, stop, and restart applications only if you have connected the device using Administration Server tools.

► *To start, stop, or restart an application:*

1. Run the remote diagnostics utility and connect to the necessary device, as described in "Connecting the remote diagnostics utility to a client device (on page [652](#))".
2. In the object tree of the device, select the necessary application.
3. Select an action in the left part of the remote diagnostics utility window:
 - **Stop application**
 - **Restart application**
 - **Start application**

Depending on the action that you have selected, the application is started, stopped, or restarted.

UEFI protection devices

UEFI protection device is a device with Kaspersky Anti-Virus for UEFI integrated at the BIOS level. Integrated protection ensures device security from the moment the system starts, while protection on devices without integrated software begins functioning only after the security application starts. Kaspersky Security Center supports management of these devices.

► *To modify the connection settings of UEFI protection devices:*

1. In the console tree, select the node with the name of the required Administration Server.
2. In the context menu of the Administration Server, select **Properties**.
3. In the Administration Server properties window, select **Server connection settings** → **Additional ports**.

4. In the **Additional ports** section, modify the relevant settings:

- **Open port for UEFI protection devices**

UEFI protection devices can connect to the Administration Server.

- **Port for UEFI protection devices**

You can change the port number if the **Open port for UEFI protection devices** option is enabled. The default port number is 13294.

5. Click **OK**.

Settings of a managed device

► *To view the settings of a managed device:*

1. In the console tree, select the **Managed devices** folder.
2. In the workspace of the folder, select a device.
3. In the context menu of the device, select **Properties**.

The properties window of the selected device opens, with the **General** section selected.

General

The **General** section displays general information about the client device. Information is provided on the basis of data received during the last synchronization of the client device with the Administration Server:

- **Name**

In this field, you can view and modify the client device name in the administration group.

- **Description**

In this field, you can enter an additional description for the client device.

- **Windows domain**

Windows domain or workgroup, which contains the device.

- **NetBIOS name**

Windows network name of the client device.

- **DNS name**

Name of the DNS domain of the client device.

- **IP address**

Device IP address

- **Group**

Administration group, which includes the client device.

- **Last updated**

Date the databases or applications were last updated on the device.

- **Last visible**

Date and time the device was last visible on the network.

- **Connected to Administration Server**

Date and time Network Agent installed on the client device last connected to the Administration Server.

- **Do not disconnect from the Administration Server**

If this check box is selected, an uninterrupted connection is maintained between the Administration Server and the client device.

If this check box is cleared, the client device will only connect to the Administration Server to synchronize data or to transmit information.

This check box is selected by default if Administration Server is installed on the device.

If only Network Agent is installed on the device, this check box is cleared by default.

Protection

The **Protection** section provides information about the current status of anti-virus protection on the client device:

- **Device status**

Status of the client device assigned on the basis of the criteria defined by the administrator for the status of anti-virus protection on the device and the activity of the device on the network.

- **All problems**

This table contains a complete list of problems detected by the managed applications installed on the client device. Each problem is accompanied by a status, which the application suggests you assign to the device for this problem.

- **Real-time protection**

This field shows the current status of real-time protection (see section "List of managed devices. Description of columns" on page [905](#)) on the client device.

When the status changes on the device, the new status is displayed in the device properties window only after the client device is synchronized with the Administration Server.

- **Last on-demand scan**

Date and time the last virus scan was performed on the client device.

- **Total number of threats detected**

Total number of threats detected on the client device since installation of the anti-virus application (first scan), or since the last reset of the threat counter.

- **Active threats**

Number of unprocessed files on the client device.

This field ignores the number of unprocessed files on mobile devices.

- **Disk encryption status**

The current status of file encryption on the local drives of the device.

Applications

The **Applications** section lists all Kaspersky applications installed on the client device:

- **Events**

Click the button to view a list of events that have occurred on the client device when the application has been running, and to view the task results for this application.

- **Statistics**

Click this button to view current statistical information about the application.

- **Properties**

Click the button to receive information about the application and to configure the application.

Tasks

In the **Tasks** section, you can manage client device tasks: view the list of existing tasks, create new ones, remove, start, and stop tasks, modify their settings, and view execution results. The list of tasks is provided based on data received during the last session of client synchronization with the Administration Server. The Administration Server requests the task status details from the client device. If connection is not established, the status is not displayed.

Events

The **Events** section displays events logged on the Administration Server for the selected client device.

Tags

In the **Tags** section, you can manage the list of keywords that are used for finding client devices: view the list of existing tags, assign tags from the list, configure auto-tagging rules, add new tags and rename old tags, and remove tags.

System Info

The **General system info** section provides information about the application installed on the client device.

Applications registry

In the **Applications registry** section, you can view the registry of applications installed on the client device and their updates; you can also set up the display of the applications registry.

Information about installed applications is provided if Network Agent installed on the client device sends required information to the Administration Server. You can configure sending of information to the Administration Server in the properties window of Network Agent or its policy, in the **Repositories** section. Information about installed applications is provided only for devices running Windows.

Network Agent provides information about the applications based on data received from the system registry.

- **Display incompatible security applications only**

If this check box is selected, the applications list contains only those security applications that are incompatible with Kaspersky applications.

By default, this check box is cleared.

- **Show updates**

If this check box is selected, the applications list contains applications and the update packages installed for them.

By default, this check box is cleared.

- **Export to file**

Click this button to export the list of applications installed on the device to a CSV file or TXT file.

- **History**

Click this button to view events concerning installation of applications on the device. The following information is displayed:

- Date and time when the application was installed on the device
- Application name
- Application version

- **Properties**

Click this button to view the properties of the application selected in the list of applications installed on the device. The following information is displayed:

- Application name
- Application version
- Application vendor

Executable files

The **Executable files** section displays executable files found on the client device.

Hardware registry

In the **Hardware registry** section, you can view information about hardware installed on the client device. You can view this information for Windows devices and Linux devices.

Sessions

The **Sessions** section displays information about the client device owner, as well as accounts of users who have worked on the selected client device.

Information about domain users is generated based on Active Directory data. The details of local users are provided by Windows Security Account Manager installed on the client device.

- **Device owner**

The **Device owner** field displays the name of the user whom the administrator can contact when the need arises to perform certain operations on the client device.

Use the **Assign** and **Properties** buttons to select the device owner and view information about the user who has been appointed the device owner.

Use the button with the red cross to delete the current device owner.

The list displays accounts of users that work on the client device.

- **Name**

Name of the device in the Windows network.

- **Participant's name**

Name (domain or local) of the user who logged on to the system on that device.

- **Account**

Account of the user who has logged on to that device.

- **Email**

User email address.

- **Phone**

User telephone number.

Incidents

In the **Incidents** section, you can view, edit, and create incidents for the client device. Incidents can be created either automatically, through managed Kaspersky applications installed on the client device, or manually by the administrator. For example, if some users regularly move malware from their removable drives to devices, the administrator can create an incident. The administrator can provide a brief description of the case and recommended actions (such as disciplinary actions to be taken against a user) in the text of the incident, and can add a link to the user or users.

An incident for which all of the required actions have been taken is called *processed*. The presence of unprocessed incidents can be chosen as the condition for a change of the device status to *Critical* or *Warning*.

This section contains a list of incidents that have been created for the device. Incidents are classified by severity level and type. The type of an incident is defined by the Kaspersky application, which creates the incident. You can highlight processed incidents in the list by selecting the check box in the **Processed** column.

Software vulnerabilities

The **Software vulnerabilities** section provides information about vulnerabilities in third-party applications installed on client devices. You can use the search field above the list to look for vulnerabilities by name.

- **Export to file**

Click the **Export to file** button to save the list of vulnerabilities to file. By default, the application exports the list of vulnerabilities to a CSV file.

- **Show only vulnerabilities that can be fixed**

If this check box is selected, the section displays vulnerabilities that can be fixed by using a patch.

If this check box is cleared, the section displays both vulnerabilities that can be fixed by using a patch, and vulnerabilities for which no patch has been released.

By default, this check box is selected.

- **Properties**

Select a software vulnerability in the list and click the **Properties** button to view the properties of the selected software vulnerability in a separate window. In the window, you can do the following:

- Ignore software vulnerability on this managed device (in Administration Console (see section "Ignoring software vulnerabilities" on page [480](#)) or in Kaspersky Security Center 13 Web Console (see section "Settings of a managed device" on page [658](#))).
- View the list of recommended fixes for the vulnerability.
- Manually specify the software updates to fix the vulnerability (in Administration Console (see section "Selecting user fixes for vulnerabilities in third-party software" on page [481](#)) or in Kaspersky Security Center 13 Web Console (see section

- "Selecting user fixes for vulnerabilities in third-party software" on page [1253](#))).
- View vulnerability instances.
- View the list of existing tasks to fix vulnerability and create new tasks to fix vulnerability.

Available updates

This section displays a list of software updates found on this device but not installed yet.

- **Show installed updates**

If this check box is selected, the list displays both updates that have not been installed and those already installed on the client device.

By default, this check box is cleared.

Active policies

This section displays a list of Kaspersky application policies currently active on this device.

- **Export to file**

You can click the **Export to file** button to save the list of active policies to a file. By default, the application exports the list of policies to a CSV file.

Active policy profiles

- **Active policy profiles**

The list allows you to view information about the existing policy profiles, which are active on client devices. You can use the search bar above the list to find active policy profiles on the list by entering a policy name or a policy profile name.

- **Export to file**

Distribution points

This section provides a list of distribution points with which the device interacts.

- **Export to file**

Click the **Export to file** button to save to a file a list of distribution points with which the device interacts. By default, the application exports the list of devices to a CSV file.

Properties Click the **Properties** button to view and configure the distribution point with which the device interacts.

See also:

| [Adjusting the general settings of Administration Server609](#)

General policy settings

General

In the **General** section, you can modify the policy status and specify the inheritance of policy settings:

- In the **Policy status** block, you can select one of the policy modes:
 - **Active policy**

If this option is selected, the policy becomes active.

By default, this option is selected.
 - **Out-of-office policy**

If this option is selected, the policy becomes active when the device leaves the corporate network. Out-of-office policy is available only for Kaspersky Anti-Virus 6.0 for Windows Workstations MP3 or later.
 - **Inactive policy**

If this option is selected, the policy becomes inactive, but it is still stored in the **Policies** folder. If required, the policy can be activated.
- In the **Settings inheritance** settings group, you can configure the policy inheritance:
 - **Inherit settings from parent policy**

If this option is enabled, the policy setting values are inherited from the upper-level group policy and, therefore, are locked.

By default, this option is enabled.
 - **Force inheritance of settings in child policies**

If this option is enabled, after policy changes are applied, the following actions will be performed:

 - The values of the policy settings will be propagated to the policies of nested administration groups, that is, to the child policies.
 - In the **Settings inheritance** block of the **General** section in the properties window of each child policy, the **Inherit settings from parent policy** option will be automatically enabled.

If this option is enabled, the child policies settings are locked.

By default, this option is disabled.

Event configuration

The **Event configuration** section allows you to configure event logging and event notification. Events are distributed by importance level on the following tabs:

- **Critical**
- **Functional failure**
- **Warning**
- **Info**

On each tab, the list shows the types of events and the default event storage term on the Administration Server (in days). Clicking the **Properties** button lets you specify the settings of event logging and notifications about events selected in the list. By default, common notification settings (see section "Configuring event notification" on page [297](#)) specified for the entire Administration Server are used for all event types. However, you can change specific settings for the required event types.

To select multiple event types, use the SHIFT or CTRL key; to select all types, use the **Select all** button.

See also:

Control of virus outbreaks.....[611](#)

Network Agent policy settings

► *To configure the Network Agent policy:*

1. In the console tree, select the **Policies** folder.
2. In the workspace of the folder, select the Network Agent policy.
3. In the context menu of the policy, select **Properties**.

The properties window of the Network Agent policy opens.

General

In the **General** section, you can modify the policy status and specify the inheritance of policy settings:

- In the **Policy status** block, you can select one of the policy modes:
 - **Active policy**

If this option is selected, the policy becomes active.

By default, this option is selected.
 - **Out-of-office policy**

If this option is selected, the policy becomes active when the device leaves the corporate network. Out-of-office policy is available only for Kaspersky Anti-Virus 6.0 for Windows Workstations MP3 or later.
 - **Inactive policy**

If this option is selected, the policy becomes inactive, but it is still stored in the **Policies** folder. If required, the policy can be activated.
- In the **Settings inheritance** settings group, you can configure the policy inheritance:
 - **Inherit settings from parent policy**

If this option is enabled, the policy setting values are inherited from the upper-level group policy and, therefore, are locked.

By default, this option is enabled.
 - **Force inheritance of settings in child policies**

If this option is enabled, after policy changes are applied, the following actions will be performed:

 - The values of the policy settings will be propagated to the policies of nested administration groups, that is, to the child policies.
 - In the **Settings inheritance** block of the **General** section in the properties window of each child policy, the **Inherit settings from parent policy** option will be

automatically enabled.

If this option is enabled, the child policies settings are locked.

By default, this option is disabled.

Event configuration

The **Event configuration** section allows you to configure event logging and event notification. Events are distributed by importance level on the following tabs:

- **Critical**
- **Functional failure**
- **Warning**
- **Info**

The **Critical** tab is not displayed in the Network Agent policy properties.

On each tab, the list shows the types of events and the default event storage term on the Administration Server (in days). Clicking the **Properties** button lets you specify the settings of event logging and notifications about events selected in the list. By default, common notification settings (see section "Configuring event notification" on page [297](#)) specified for the entire Administration Server are used for all event types. However, you can change specific settings for the required event types.

To select multiple event types, use the SHIFT or CTRL key; to select all types, use the **Select all** button.

Settings

In the **Settings** section, you can configure the Network Agent policy:

- **Distribute files through distribution points only**

If this option is enabled, client devices retrieve updates through distribution points only, not directly from update servers.

If this option is disabled, client devices can retrieve updates from various sources: directly from update servers, from the primary Administration Server, from a local or network folder.

By default, this option is disabled.

- **Maximum size of event queue, in MB**

In this field you can specify the maximum space on the drive that an event queue can occupy.

The default value is 2 megabytes (MB).

- **Application is allowed to retrieve policy's extended data on device**

Network Agent installed on a managed device transfers information about the applied security application policy to the security application (for example, Kaspersky Endpoint Security for Windows). You can view the transferred information in the security application interface.

Network Agent transfers the following information:

- Time of the policy delivery to the managed device
- Name of the active or out-of-office policy at the moment of the policy delivery to the managed device

- Name and full path to the administration group that contained the managed device at the moment of the policy delivery to the managed device
- List of active policy profiles

You can use the information to ensure the correct policy is applied to the device and for troubleshooting purposes.
- **Protect Network Agent service against unauthorized removal or termination, and to prevent changes to the settings**

After Network Agent is installed on a managed device, the component cannot be removed or reconfigured without required privileges. The Network Agent service cannot be stopped.

By default, this option is disabled.
- **Use uninstallation password**

If this check box is selected, by clicking the **Modify** button you can specify the password for Network Agent remote uninstallation.

By default, this check box is cleared.

Repositories

In the **Repositories** section, you can select the types of objects whose details will be sent from Network Agent to Administration Server. If modification of some settings in this section is prohibited by the Network Agent policy, you cannot modify these settings. The settings in the **Repositories** section are available only on devices running Windows:

- **Details of installed applications**

If this check box is selected, information about applications installed on client devices is sent to the Administration Server.

By default, this check box is selected.
- **Include information about patches**

Information about patches of applications installed on client devices is sent to the Administration Server. Enabling this option may increase the load on the Administration Server and DBMS, as well as cause increased volume of the database.

By default, this option is enabled.
- **Details of Windows Update updates**

If this check box is selected, information about Microsoft Windows Update updates that must be installed on client devices is sent to the Administration Server.

Sometimes, even if the check box is cleared, updates are displayed in the device properties in the **Available updates** section. This might happen if, for example, the devices of the organization had vulnerabilities that could be fixed by these updates.

By default, this check box is selected.
- **Details of software vulnerabilities and corresponding updates**

If this option is enabled, information about vulnerabilities in third-party software (including Microsoft software), detected on managed devices, and about software updates to fix third-party vulnerabilities (not including Microsoft software) is sent to the Administration Server.

Selecting this option (**Details of software vulnerabilities and corresponding updates**) increases the network load, Administration Server disk load, and Network Agent resource consumption.

By default, this option is enabled.

To manage software updates of Microsoft software, use the **Details of Windows Update updates** option.

- **Hardware registry details**

Network Agent installed on a device sends information about the device hardware to the Administration Server. You can view the hardware details in the device properties.

Software updates and vulnerabilities

In the **Software updates and vulnerabilities** section, you can configure search and distribution of Windows updates, as well as enable scanning of executable files for vulnerabilities. The settings in the **Software updates and vulnerabilities** section are available only on devices running Windows:

- **Use Administration Server as a WSUS server**

If this check box is selected, Windows updates are downloaded to the Administration Server. The Administration Server provides downloaded updates to Windows Update on client devices in centralized mode through Network Agents.

If this check box is cleared, the Administration Server is not used for downloading Windows updates. In this case, client devices receive Windows updates on their own.

By default, this check box is cleared.

- Under **Allow users to manage installation of Windows Update updates**, you can limit Windows updates that users can install on their devices manually by using Windows Update.

On devices running Windows 10, if Windows Update has already found updates for the device, the new option that you select under **Allow users to manage installation of Windows Update updates** will be applied only after the updates found are installed.

Select an item in the drop-down list:

- **Allow users to install all applicable Windows Update updates**

Users can install all of the Microsoft Windows Update updates that are applicable to their devices.

Select this option if you do not want to interfere in the installation of updates.

When the user installs Microsoft Windows Update updates manually, the updates may be downloaded from Microsoft servers rather than from Administration Server. This is possible if Administration Server has not yet downloaded these updates. Downloading updates from Microsoft servers results in extra traffic.

- **Allow users to install only approved Windows Update updates**

Users can install all of the Microsoft Windows Update updates that are applicable to their devices and that are approved by you.

For example, you may want to first check the installation of updates in a test environment

and make sure that they do not interfere with the operation of devices, and only then allow the installation of these approved updates on client devices.

When the user installs Microsoft Windows Update updates manually, the updates may be downloaded from Microsoft servers rather than from Administration Server. This is possible if Administration Server has not yet downloaded these updates. Downloading updates from Microsoft servers results in extra traffic.

- **Do not allow users to install Windows Update updates**

Users cannot install Microsoft Windows Update updates on their devices manually. All of the applicable updates are installed as configured by you.

Select this option if you want to manage the installation of updates centrally.

For example, you may want to optimize the update schedule so that the network does not become overloaded. You can schedule after-hours updates, so that they do not interfere with user productivity.

- In the **Windows Update search mode** settings group, you can select the update search mode:

- **Active**

If this option is selected, Administration Server with support from Network Agent initiates a request from Windows Update Agent on the client device to the update source: Windows Update Servers or WSUS. Next, Network Agent passes information received from Windows Update Agent to Administration Server.

The option takes effect only if **Connect to the update server to update data** option of the *Find vulnerabilities and required updates* task is selected.

By default, this option is selected.

- **Passive**

If you select this option, Network Agent periodically passes Administration Server information about updates retrieved at the last synchronization of Windows Update Agent with the update source. If no synchronization of Windows Update Agent with an update source is performed, information about updates on Administration Server becomes out-of-date.

Select this option if you want to get updates from the memory cache of the update source.

- **Disabled**

If this option is selected, Administration Server does not request any information about updates.

Select this option if, for example, you want to test the updates on your local device first.

- **Scan executable files for vulnerabilities when running them**

If this check box is selected, executable files are scanned for vulnerabilities when they are run.

By default, this check box is selected.

Restart management

In the **Restart management** section, you can specify the action to be performed if the operating system of a managed device has to be restarted for correct use, installation, or uninstallation of an application. The settings in the **Restart management** section are available only on devices running Windows:

- **Do not restart the operating system**

The operating system will not be restarted.

- **Restart the operating system automatically if necessary**

If necessary, the operating system is restarted automatically.

- **Prompt user for action**

The application prompts the user to allow restarting the operating system.

By default, this option is selected.

- **Repeat the prompt every (min)**

If this check box is selected, the application prompts the user to allow restarting the operating system with the frequency specified in the field next to the check box. By default, the prompting frequency is 5 minutes.

If this check box is cleared, the application does not prompt the user to allow restarting repeatedly.

By default, this check box is selected.

- **Force restart after (min)**

If this check box is selected, after prompting the user, the application forces restart of the operating system upon expiration of the time interval specified in the field next to the check box.

If this check box is cleared, the application does not force restart.

By default, this check box is selected.

- **Wait time before forced closure of applications in blocked sessions (min)**

Applications are forced to close when the user's device goes locked (automatically after a specified interval of inactivity, or manually).

If this check box is selected, applications are forced to close on the locked device upon expiration of the time interval specified in the entry field.

If this check box is cleared, applications do not close on the locked device.

By default, this check box is cleared.

Windows Desktop sharing

In the **Windows Desktop Sharing** section, you can enable and configure the audit of the administrator's actions performed on a remote device when desktop access is shared. The settings in the **Windows Desktop Sharing** section are available only on devices running Windows:

- **Enable audit**

If this option is enabled, audit of the administrator's actions is enabled on the remote device. Records of the administrator's actions on the remote device are logged:

- In the event log on the remote device
- In a file with the syslog extension located in the Network Agent installation folder on the remote device
- In the event database of Kaspersky Security Center

Audit of the administrator's actions is available when the following conditions are met:

- The Vulnerability and Patch Management license is in use
- The administrator has the right to start shared access to the desktop of the remote device

If this option is disabled, the audit of the administrator's actions is disabled on the remote device.

By default, this option is disabled.

- **Masks of files to monitor when read**

The list contains file masks. When the audit is enabled, the application monitors the administrator's reading files that match the masks and saves information about files read. The list is available if the **Enable audit** check box is selected. You can edit file masks and add new ones to the list. Each new file mask should be specified in the list on a new line.

By default, the following file masks are specified: *.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf.

- **Masks of files to monitor when modified**

The list contains masks of files on the remote device. When audit is enabled, the application monitors changes made by the administrator in files that match masks, and saves information about those modifications. The list is available if the **Enable audit** check box is selected. You can edit file masks and add new ones to the list. Each new file mask should be specified in the list on a new line.

By default, the following file masks are specified: *.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf.

Manage patches and updates

In the **Manage patches and updates** section, you can configure download and distribution of updates, as well as installation of patches, on managed devices:

- **Automatically install applicable updates and patches for components that have the Undefined status**

If this option is enabled, Kaspersky patches that have the *Undefined* approval status are automatically installed on managed devices immediately after they are downloaded from update servers. Automatic installation of patches that have the *Undefined* status is available for Kaspersky Security Center Service Pack 2 and later.

If this option is disabled, Kaspersky patches that have been downloaded and tagged with the *Undefined* status will be installed only after you change their status to *Approved*.

By default, this option is enabled.

- **Download updates and anti-virus databases from Administration Server in advance (recommended)**

If this option is enabled, the offline model of update download is used. When the Administration Server receives updates, it notifies Network Agent (on devices where it is installed) of the updates that will be required for managed applications. When Network Agent receives information about these updates, it downloads the relevant files from the Administration Server in advance. At the first connection with Network Agent, the

Administration Server initiates an update download. After Network Agent downloads all the updates to a client device, the updates become available for applications on that device.

When a managed application on a client device attempts to access Network Agent for updates, Network Agent checks whether it has all required updates. If the updates are received from the Administration Server not more than 25 hours before they were requested by the managed application, Network Agent does not connect to the Administration Server but supplies the managed application with updates from the local cache instead. Connection with the Administration Server may not be established when Network Agent provides updates to applications on client devices, but connection is not required for updating.

If this option is disabled, the offline model of update download is not used. Updates are distributed according to the schedule of the update download task.

By default, this option is enabled.

Connectivity

The **Connectivity** section includes three nested subsections:

- **Network**
- **Connection profiles** (only for Windows)
- **Connection schedule**

In the **Network** subsection, you can configure the connection to Administration Server, enable the use of a UDP port, and specify its number. The following options are available:

- In the **Connection to Administration Server** settings group, you can configure connection to the Administration Server and specify the time interval for synchronization between client devices and the Administration Server:
 - **Compress network traffic**

If this check box is selected, the speed of data transfer by Network Agent is increased by means of a decrease in the amount of information being transferred and a consequent decreased load on the Administration Server.

The workload on the CPU of the client computer may increase.

By default, this check box is selected.

- **Open Network Agent ports in Microsoft Windows Firewall**

If this check box is selected, a UDP port, necessary for the work of Network Agent, is added to the Microsoft Windows Firewall exclusion list.

By default, this check box is selected.

- **Use SSL**

If this check box is selected, connection to the Administration Server is established through a secure port via SSL.

By default, this check box is selected.

- **Use connection gateway on distribution point (if available) under default connection settings**

If this check box is selected, the connection gateway on the distribution point is used under the settings specified in the administration group properties.

By default, this check box is selected.

- **Use UDP port**

If this check box is selected, the client device connects to the Administration Server through a UDP port.

By default, this check box is selected.

- **UDP port number**

In this field you can enter the UDP port number. The default port number is 15000.

The decimal system is used for records.

If the client device runs Windows XP Service Pack 2, the integrated firewall blocks UDP port 15000. This port should be opened manually.

In the **Connection profiles** subsection, you can specify the network location settings, configure connection profiles for Administration Server, and enable out-of-office mode when Administration Server is not available. The settings in the **Connection profiles** section are available only on devices running Windows:

- **Network location settings**

Network location settings define the characteristics of the network to which the client device is connected and specify rules for Network Agent switching from one Administration Server connection profile to another when those network characteristics are altered.

- **Administration Server connection profiles**

In this section, you can view and add profiles for Network Agent connection to the Administration Server. In this section, you can also create rules for switching Network Agent to different Administration Servers when the following events occur:

- When the client device connects to a different local network
- When the device loses connection with the local network of the organization
- When the connection gateway address is changed or the DNS server address is modified

Connection profiles are supported only for devices running Windows.

- **Enable out-of-office mode when Administration Server is not available**

If this check box is selected, in case of connection through this profile, applications installed on the client device use policy profiles for devices in out-of-office mode, as well as out-of-office policies (see section "About switching Network Agent to other Administration Servers" on page [291](#)). If no out-of-office policy has been defined for the application, the active policy will be used.

If this check box is cleared, applications will use active policies.

By default, this check box is cleared.

In the **Connection schedule** subsection, you can specify the time intervals during which Network Agent sends data to the Administration Server:

- **Connect when necessary**

If this option is selected, the connection is established when Network Agent has to send data to the Administration Server.

By default, this option is selected.

- **Connect at specified time intervals**

If this option is selected, Network Agent connects to the Administration Server at a specified time. You can add several connection time periods.

Distribution points

The **Distribution points** section includes four nested subsections:

- **Device discovery**
- **Internet connection settings**
- **KSN Proxy**
- **Updates**

In the **Device discovery** subsection, you can configure automatic polling of the network. The polling settings are available only on devices running Windows.

- In the **Network polling** settings group, you can enable automatic polling of the network and set the frequency:

- **Enable network polling**

If the check box is selected, the Administration Server automatically polls the network according to the schedule that you configured by clicking the **Set quick polling schedule** and **Set full polling schedule** links.

If this check box is cleared, the Administration Server does not poll the network.

The device discovery interval for Network Agent versions prior to 10.2 can be configured in the **Frequency of polls from Windows domains (min)** and **Frequency of network polls (min)** fields. The fields are available if the check box is selected.

By default, this check box is cleared.

- In the **IP range polling** settings group, you can enable automatic polling of IP ranges and set the polling frequency:

- **Enable IP range polling**

If the check box is selected, the Administration Server automatically polls IP ranges according to the schedule that you configured by clicking the **Set polling schedule** link.

If this check box is cleared, the Administration Server does not poll IP ranges.

The frequency of IP range polling for Network Agent versions prior to 10.2 can be configured in the **Poll interval (min)** field. The field is available if check box is selected.

By default, this check box is cleared.

- In the **Active Directory polling** settings group, you can enable automatic device discovery based on the Active Directory structure and set the frequency:

- **Enable Active Directory polling**

If the check box is selected, the Administration Server automatically polls Active Directory according to the schedule that you configured by clicking the **Set polling schedule** link.

If this check box is cleared, the Administration Server does not poll Active Directory.

The frequency of Active Directory polling for Network Agent versions prior to 10.2 can be configured in the **Poll interval (min)** field. The field is available if check box is selected.

By default, this check box is cleared.

In the **Internet connection settings** subsection, you can specify the Internet access settings:

- **Use proxy server**

If this check box is selected, in the entry fields you can configure the proxy server connection.

By default, this check box is cleared.

- **Proxy server address**

Address of the proxy server.

- **Port number**

Port number that is used for connection.

- **Bypass proxy server for local addresses**

If this check box is selected, no proxy server is used to connect to devices on the local network.

By default, this check box is cleared.

- **Proxy server authentication**

If this check box is selected, in the entry fields you can specify the credentials for proxy server authentication.

By default, this check box is cleared.

- **User name**

User account under which connection to the proxy server is established.

- **Password**

Password of the account under which the task will be run.

In the **KSN Proxy** subsection, you can configure the application to use the distribution point to forward KSN requests from the managed devices:

- **Enable KSN Proxy on distribution point side**

The KSN Proxy service is run on the device that is used as a distribution point. Use this feature to redistribute and optimize traffic on the network.

The distribution point sends the KSN statistics, which are listed in the Kaspersky Security Network statement, to Kaspersky. By default, the KSN statement is located in %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\ksneula.

By default, this option is disabled. Enabling this option takes effect only if the **Use Administration Server as proxy server** and **I agree to use Kaspersky Security Network** options are enabled (see section "Setting up access to Kaspersky Security Network" on page [786](#)) in the Administration Server properties window.

You can assign a node of an active-passive cluster to a distribution point and enable KSN Proxy on this node.

- **Forward KSN requests to Administration Server**

The distribution point forwards KSN requests from the managed devices to the Administration Server.

By default, this option is enabled.

- **Access KSN Cloud / Private KSN directly over the Internet**

The distribution point forwards KSN requests from managed devices to the KSN Cloud or Private KSN. The KSN requests generated on the distribution point itself are also sent directly to the KSN Cloud or Private KSN.

The distribution points that have Network Agent version 11 (or earlier) installed cannot access Private KSN directly. If you want to reconfigure the distribution points to send KSN requests to Private KSN, enable the **Forward KSN requests to Administration Server** option for each distribution point.

The distribution points that have Network Agent version 12 (or later) installed can access Private KSN directly.

- **TCP port**

The number of the TCP port that the managed devices will use to connect to KSN Proxy server. The default port number is 13111.

- **UDP port number**

If you need the managed devices to connect to KSN Proxy server through a UDP port, enable the **Use UDP port** option and specify a **UDP port** number. By default, this option is enabled. The default UDP port to connect to the KSN Proxy server is 15111.

In the **Updates** subsection, you can configure whether Network Agent downloads diff files:

- **Download diff files**

This option enables the downloading diff files feature (see section "Using diff files for updating Kaspersky databases and software modules" on page [412](#)).

By default, this option is enabled.

Revision history

On the **Revision history** tab, you can view the history of Network Agent policy revisions (see section "Managing object revisions" on page [719](#)). You can compare revisions, view revisions, and perform advanced operations, such as save revisions to a file, roll back to a revision, and add and edit revision descriptions.

Network Agent policy settings available for a specific operating system are given in the table below.

Table 61. Network Agent policy settings

Policy section	Windows	Mac	Linux
General	✓	✓	✓
Event configuration	✓	✓	✓
Settings	✓	✓ except the check box Use uninstallation password	✓ except the check box Use uninstallation password
Repositories	✓	-	-
Software updates and vulnerabilities	✓	-	-
Restart management	✓	-	-
Windows Desktop Sharing	✓	-	-
Manage patches and updates	✓	-	-
Network → Network	✓	✓ except the check box Open Network Agent ports in Microsoft Windows Firewall	✓ except the check box Open Network Agent ports in Microsoft Windows Firewall
Network → Connection	✓	-	-
Network → Connection Manager	✓	✓	✓
Distribution points → Device discovery	✓	-	-
Distribution points → Internet connection settings	✓	✓	✓
Distribution points → KSN Proxy	✓	-	-
Distribution points → Updates	✓	-	-
Revision history	✓	✓	✓

See also:

Scenario: Regular updating Kaspersky databases and applications[1174](#)

Managing user accounts

This section provides information about user accounts and roles supported by the application. This section contains instructions on how to create accounts and roles for users of Kaspersky Security Center. This section also contains instructions on how to manage lists of the user certificates and mobile devices and how to deliver messages to users.

In this section

Working with user accounts	678
Adding an account of an internal user	679
Editing an account of an internal user	680
Changing the number of allowed password entry attempts	681
Configuring the check of the name of an internal user for uniqueness	682
Adding a security group	683
Adding a user to a group	683
Configuring access rights to application features. Role-based access control	683
Assigning the user as a device owner	710
Delivering messages to users	710
Viewing the list of user mobile devices	711
Installing a certificate for a user	711
Viewing the list of certificates issued to a user	711
About the administrator of a virtual Administration Server	712

Working with user accounts

Kaspersky Security Center allows you to manage user accounts and groups of accounts. The application supports two types of accounts:

- Accounts of organization employees. Administration Server retrieves data of the accounts of those users when polling the organization's network.
- Accounts of internal users (see section "Working with internal users" on page [614](#)). These accounts are applied when virtual Administration Servers are used. Accounts of internal users are created (see section "Adding an account of an internal user" on page [679](#)) and used only within Kaspersky Security Center.

All user accounts can be viewed in the **User accounts** folder in the console tree. The **User accounts** folder is a subfolder of the **Advanced** folder by default.

You can perform the following actions on user accounts and groups of accounts:

- Configure users' rights of access to the application features using roles (see section "Configuring access rights to application features. Role-based access control" on page [683](#)).
- Send messages to users by email and SMS (see section "Delivering messages to users" on page [710](#)).

- View the list of the user's mobile devices (see section "Viewing the list of user mobile devices" on page [711](#)).
- Issue and install certificates on the user's mobile devices (see section "Installing a certificate for a user" on page [711](#)).
- View the list of certificates issued to the user (see section "Viewing the list of certificates issued to a user" on page [711](#)).
- Disable two-step verification (see section "Disabling two-step verification for a user account" on page [628](#)) for a user account.

Adding an account of an internal user

► *To add a new internal user account to Kaspersky Security Center:*

1. In the console tree, open the **User accounts** folder.
The **User accounts** folder is a subfolder of the **Advanced** folder by default.
2. In the workspace, click the **Add user** button.
3. In the **New user** window that opens, specify the settings of the new user account:

-  (user name)

Please be careful when entering the user name. You will not be able to change it after saving the changes.

- **Description**
- **Full name**
- **Main email**
- **Main phone**
- **Password** for the user connection to Kaspersky Security Center

The password must comply with the following rules:

- The password must be 8 to 16 characters long.
- The password must contain characters from at least three of the groups listed below:
 - Uppercase letters (A-Z)
 - Lowercase letters (a-z)
 - Numbers (0-9)
 - Special characters (@ # \$ % ^ & * - _ ! + = [] { } | : ' , . ? / \ ` ~ " () ;)
- The password must not contain any whitespaces, Unicode characters, or the combination of "." and "@", when "." is placed before "@".

To see the entered password, click and hold the **Show** button.

The number of attempts for entering the password is limited. By default, the maximum number of allowed password entry attempts is 10. You can change the allowed number of attempts to enter a password, as described in "Changing the number of allowed password entry attempts" (see section "Changing the number of allowed password entry attempts" on page [681](#)).

If the user enters an invalid password the specified number of times, the user account is blocked

for one hour. In the list of user accounts, the user icon () of a blocked account is dimmed (unavailable). You can unblock the user account only by changing the password.

- If necessary, select the **Disable account** check box to prohibit the user from connecting to the application. You can disable an account, for example, if you want to create it beforehand but activate it later.
- Select the **Request the password when account settings are modified** check box if you want to enable an additional option to protect a user account from unauthorized modification. If this option is enabled, modifying user account settings requires authorization of the user with the Modify object ACLs (see section "Access rights to application features" on page [684](#)) right of the **General features: User permissions** functional area.

4. Click **OK**.

The newly created user account is displayed in the workspace of the **User accounts** folder.

Editing an account of an internal user

► *To edit an internal user account in Kaspersky Security Center:*

1. In the console tree, open the **User accounts** folder.

The **User accounts** folder is a subfolder of the **Advanced** folder by default.

2. In the workspace, double-click the internal user account that you want to edit.
3. In the **Properties: <user name>** window that opens, change the settings of the user account:

- **Description**
- **Full name**
- **Main email**
- **Main phone**
- **Password** for the user connection to Kaspersky Security Center

The password must comply with the following rules:


- The password must be 8 to 16 characters long.
- The password must contain characters from at least three of the groups listed below:
 - Uppercase letters (A-Z)
 - Lowercase letters (a-z)
 - Numbers (0-9)
 - Special characters (@ # \$ % ^ & * - _ ! + = [] { } | : ' , . ? / \ ` ~ " () ;)

- The password must not contain any whitespaces, Unicode characters, or the combination of "." and "@", when "." is placed before "@".

To see the entered password, click and hold the **Show** button.

The number of attempts for entering the password is limited. By default, the maximum number of allowed password entry attempts is 10. You can change the allowed number of attempts to enter a password, as described in "Changing the number of allowed password entry attempts" (see section "Changing the number of allowed password entry attempts" on page [681](#)).

If the user enters an invalid password the specified number of times, the user account is blocked

for one hour. In the list of user accounts, the user icon () of a blocked account is dimmed (unavailable). You can unblock the user account only by changing the password.

- If necessary, select the **Disable account** check box to prohibit the user from connecting to the application. You can disable an account, for example, after an employee quits the company.
- Select the **Request the password when account settings are modified** option if you want to enable an additional option to protect a user account from unauthorized modification. If this option is enabled, modifying user account settings requires authorization of the user with the Modify object ACLs (see section "Access rights to application features" on page [684](#)) right of the **General features: User permissions** functional area.

4. Click **OK**.

The edited user account is displayed in the workspace of the **User accounts** folder.

Changing the number of allowed password entry attempts

The Kaspersky Security Center user can enter an invalid password a limited number of times. After the limit is reached, the user account is blocked for one hour.

By default, the maximum number of allowed attempts to enter a password is 10. You can change the number of allowed password entry attempts, as described in this section.

► *To change the number of allowed password entry attempts:*

1. Open the system registry of the device on which Administration Server is installed (for example, locally, using the regedit command in the **Start** → **Run** menu).
2. Go to the following key:
 - For a 64-bit system:
HKEY_LOCAL_MACHINE\SOFTWAREWow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags
 - For a 32-bit system:
HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags
3. If the SrvSpiPpcLogonAttempts value is not present, create it. The value type is DWORD.
By default, after Kaspersky Security Center is installed this value is not created.
4. Specify the required number of attempts in the SrvSpiPpcLogonAttempts value.
5. Click **OK** to save the changes.

6. Restart the Administration Server service.

The maximum number of allowed password entry attempts is changed.

Configuring the check of the name of an internal user for uniqueness

You can configure the check of the name of an internal user of Kaspersky Security Center for uniqueness when this name is added to the application. The check of the name of an internal user for uniqueness can only be performed on a virtual Administration Server or on the primary Administration Server for which the user account is to be created, or on all virtual Administration Servers and on the primary Administration Server. By default, the name of an internal user is checked for uniqueness on all virtual Administration Servers and on the primary Administration Server.

► *To enable the check of the name of an internal user for uniqueness on a virtual Administration Server or on the primary Administration Server:*

1. Open the system registry of the device on which Administration Server is installed (for example, locally, using the regedit command in the **Start** → **Run** menu).
2. Go to the following hive:
 - For a 64-bit system:
HKEY_LOCAL_MACHINE\SOFTWAREWow6432Node\KasperskyLab\Components\34\core\independent\KLLIM
 - For a 32-bit system:
HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\core\independent\KLLIM
3. For the LP_InterUserUniqVsScope (DWORD) key, set the 00000001 value.
The default value specified for this key is 0.
4. Restart the Administration Server service.

The name will only be checked for uniqueness on the virtual Administration Server on which the internal user was created, or on the primary Administration Server if the internal user was created on the primary Administration Server.

► *To enable the check of the name of an internal user on all virtual Administration Servers and on the primary Administration Server:*

1. Open the system registry of the device on which Administration Server is installed (for example, locally, using the regedit command in the **Start** → **Run** menu).
2. Go to the following hive:
 - For a 64-bit system:
HKEY_LOCAL_MACHINE\SOFTWAREWow6432Node\KasperskyLab\Components\34\core\independent\KLLIM
 - For a 32-bit system:
HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\core\independent\KLLIM
3. For the LP_InterUserUniqVsScope (DWORD) key, set the 00000000 value.
The default value specified for this key is 0.
4. Restart the Administration Server service.

The check of the name for uniqueness will be performed on all virtual Administration Servers and on the primary Administration Server.

Adding a security group

You can add security groups (groups of users), perform flexible configuration of groups and security group access to various application features. Security groups can be assigned names that correspond to their respective purposes. For example, the name can correspond to where users are located in the office or to the name of the company's organizational unit to which the users belong.

One user can belong to several security groups. A user account managed by a virtual Administration Server can belong only to security groups of this virtual Server and have access rights only within this virtual Server.

► *To add a security group:*

1. In the console tree select the **User accounts** folder.

The **User accounts** folder is a subfolder of the **Advanced** folder by default.

2. Click the **Add security group** button.

The **Add security group** window opens.

3. In the **Add security group** window, in the **General** section specify the name of the group.

A group name cannot be more than 255 characters long and contain special symbols such as *, <, >, ?, \, :, |. The group name must be unique.

You can enter the group description in the **Description** entry field. Filling in the **Description** field is optional.

4. Click **OK**.

The security group that you have added appears in the **User accounts** folder in the console tree. You can add users (see section "Adding a user to a group" on page [683](#)) to the newly created group.

Adding a user to a group

► *To add a user to a group:*

1. In the console tree, select the **User accounts** folder.

The **User accounts** folder is a subfolder of the **Advanced** folder by default.

2. In the list of user accounts and groups, select the group to which you want to add the user.

3. In the group properties window, select the **Group users** section and click the **Add** button.

A window with a list of users opens.

4. In the list, select a user that you want to include in the group.

5. Click **OK**.

The user is added to the group and displayed in the list of group users.

Configuring access rights to application features. Role-based access control

Kaspersky Security Center provides facilities for role-based access to the features of Kaspersky Security Center

and managed Kaspersky applications.

You can configure access rights to application features (on page [684](#)) for Kaspersky Security Center users in one of the following ways:

- By configuring the rights for each user or group of users individually.
- By creating standard user roles with a predefined set of rights and assigning those roles to users depending on their scope of duties.

User role (also referred to as a role) is a predefined set of access rights to the features of Kaspersky Security Center or managed Kaspersky applications. A role can be assigned (see section "Assigning a role to a user or a user group" on page [707](#)) to a user or a group of users.

Application of user roles is intended to simplify and shorten routine procedures of configuring users' access rights to application features. Access rights within a role are configured in accordance with the standard tasks and the users' scope of duties.

User roles can be assigned names that correspond to their respective purposes. You can create an unlimited number of roles in the application.

You can use the predefined user roles (on page [700](#)) with already configured set of rights, or create new roles (see section "Adding a user role" on page [706](#)) and configure the required rights yourself.

In this section

Access rights to application features	684
Predefined user roles.....	700
Adding a user role.....	706
Assigning a role to a user or a user group.....	707
Assigning permissions to users and groups	707
Propagating user roles to secondary Administration Servers	709

Access rights to application features

The table below shows the Kaspersky Security Center features with the access rights to manage the associated tasks, reports, settings, and perform the associated user actions.

To perform the user actions listed in the table, a user has to have the right specified next to the action.

Read, **Modify**, and **Execute** rights are applicable to any task, report, or setting. In addition to these rights, a user has to have the **Perform operations on device selections** right to manage tasks, reports, or settings on device selections.

All tasks, reports, settings, and installation packages that are missing in the table belong to the **General features: Basic functionality** functional area.

Table 62. Access rights to application features

Functional area	Right	User action: right required to perform the action	Task	Report	Other
General features: Management of administration groups	Modify	<ul style="list-style-type: none"> • Add device to an administration group: Modify • Delete device from an administration group: Modify • Add an administration group to another administration group: Modify • Delete an administration group from another administration group: Modify 	None	None	None
General features: Access objects regardless of their ACLs	Read	Get read access to all objects: Read	None	None	None

<p>General features: Basic functionality</p>	<ul style="list-style-type: none"> • Read • Modify • Execute • Perform operations on device selections 	<ul style="list-style-type: none"> • Device moving rules (create, modify, or delete) for the virtual Server: Modify, Perform operations on device selections • Get Mobile (LWNGT) protocol custom certificate: Read • Set Mobile (LWNGT) protocol custom certificate: Write • Get NLA-defined network list: Read • Add, modify, or delete NLA-defined network list: Modify • View Access Control List of groups: Read • View the Kaspersky Event Log: Read 	<ul style="list-style-type: none"> • "Download updates to the Administration Server repository" • "Deliver reports" • "Distribute installation packages" • "Install application on secondary Admi 	<ul style="list-style-type: none"> • "Report on protection status" • "Report on threats" • "Report on most heavily infected devices" • "Report on status of anti-virus databases" • "Report on errors" • "Report on network attacks" • "Summary report on mail system protection applications installed" • "Summary report on perimeter defense applications installed" • "Summary report on types of applications installed" • "Report on users of 	<p>None</p>
---	--	--	---	---	-------------

			nis trat ion Se rve rs re mo tel y"	infected devices" <ul style="list-style-type: none"> • "Report on incidents" • "Report on events" • "Report on activity of distribution points" • "Report on Secondary Administration Servers" • "Report on Device Control events" • "Report on vulnerabilities" • "Report on prohibited applications" • "Report on Web Control" • "Report on encryption status of managed devices" • "Report on encryption status of mass storage devices" 	
--	--	--	--	---	--

Functional area	Right	User action: right required to perform the action	Task	Report	Other
				<ul style="list-style-type: none"> • "Report on file encryption errors" • "Report on blockage of access to encrypted files" • "Report on rights to access encrypted devices" • "Report on effective user permissions" • "Report on rights" 	
General features: Deleted objects	<ul style="list-style-type: none"> • Read • Modify 	<ul style="list-style-type: none"> • View deleted objects in the Recycle Bin: Read • Delete objects from the Recycle Bin: Modify 	None	None	None

<p>General features: Event processing</p>	<ul style="list-style-type: none"> • Delete events • Edit event notification settings • Edit event logging settings • Modify 	<ul style="list-style-type: none"> • Change events registration settings: Edit event logging settings • Change events notification settings: Edit event notification settings • Delete events: Delete events 	<p>None</p>	<p>None</p>	<p>Setting s:</p> <ul style="list-style-type: none"> • Virus out break set tin gs: nu mb er of vir us det ect ion s req uir ed to cre ate a vir us out bre ak ev ent • Virus out bre ak set tin gs: per iod of tim e for ev alu ati on of
---	--	--	-------------	-------------	---

Functional area	Right	User action: right required to perform the action	Task	Report	Other
					virus detections <ul style="list-style-type: none"> • The maximum number of events stored in the database • Period of time for storing events from the deleted devices

Functional area	Right	User action: right required to perform the action	Task	Report	Other
General features: Operations on Administration Server	<ul style="list-style-type: none"> • Read • Modify • Execute • Modify object ACLs • Perform operations on device selections 	<ul style="list-style-type: none"> • Specify ports of Administration Server for the network agent connection: Modify • Specify ports of Activation Proxy launched on the Administration Server: Modify • Specify ports of Activation Proxy for Mobile launched on the Administration Server: Modify • Specify ports of the Web Server for distribution of standalone packages: Modify • Specify ports of the Web Server for distribution of MDM profiles: Modify • Specify SSL ports of the Administration Server for connection via Kaspersky Security Center Web Console: Modify • Specify ports of the Administration Server for mobile connection: Modify • Specify the maximum number of events stored in the Administration Server database: Modify • Specify the maximum number of events that can be sent by the Administration Server: Modify • Specify time period during which events can be sent by the Administration Server: Modify 	<ul style="list-style-type: none"> • "Backup of Administration Server database" • "Database maintenance" 	None	None

Functional area	Right	User action: right required to perform the action	Task	Report	Other
General features: Kaspersky software deployment	<ul style="list-style-type: none"> • Manage Kaspersky patches • Read • Modify • Execute • Perform operations on device selections 	Approve or decline installation of the patch: Manage Kaspersky patches	None	<ul style="list-style-type: none"> • "Report on license key usage by virtual Administration Server" • "Report on Kaspersky software versions" • "Report on incompatible applications" • "Report on versions of Kaspersky software module updates" • "Report on protection deployment" 	Installation package: "Kaspersky"
General features: Key management	<ul style="list-style-type: none"> • Export key file • Modify 	<ul style="list-style-type: none"> • Export key file: Export key file • Modify Administration Server license key settings: Modify 	None	None	None

Functional area	Right	User action: right required to perform the action	Task	Report	Other
General features: Enforced report management	<ul style="list-style-type: none"> • Read • Modify 	<ul style="list-style-type: none"> • Create reports regardless of their ACLs: Write • Execute reports regardless of their ACLs: Read 	None	None	None
General features: Hierarchy of Administration Servers	Configure hierarchy of Administration Servers	<ul style="list-style-type: none"> • Register, update, or delete secondary Administration Servers: Configure hierarchy of Administration Servers 	None	None	None
General features: User permissions	Modify object ACLs	<ul style="list-style-type: none"> • Change Security properties of any object: Modify object ACLs • Manage user roles: Modify object ACLs • Manage internal users: Modify object ACLs • Manage security groups: Modify object ACLs • Manage aliases: Modify object ACLs 	None	None	None
General features: Virtual Administration Servers	<ul style="list-style-type: none"> • Manage virtual Administration Servers • Read • Modify • Execute • Perform operations on device selections 	<ul style="list-style-type: none"> • Get list of virtual Administration Servers: Read • Get information on the virtual Administration Server: Read • Create, update, or delete a virtual Administration Server: Manage virtual Administration Servers • Move a virtual Administration Server to another group: Manage virtual Administration Servers • Set administration virtual Server permissions: Manage virtual Administration Servers 	None	"Report on results of installation of third-party software updates"	None

Functional area	Right	User action: right required to perform the action	Task	Report	Other
Mobile device management: General	<ul style="list-style-type: none"> • Connect new devices • Send only information commands to mobile devices • Send commands to mobile devices • Manage certificates • Read • Modify 	<ul style="list-style-type: none"> • Get Key Management Service restore data: Read • Delete user certificates: Manage certificates • Get user certificate public part: Read • Check if Public Key Infrastructure is enabled: Read • Check Public Key Infrastructure account: Read • Get Public Key Infrastructure templates: Read • Get Public Key Infrastructure templates by Extended Key Usage certificate: Read • Check if Public Key Infrastructure certificate is revoked: Read • Update user certificate issuance settings: Manage certificates • Get user certificate issuance settings: Read • Get packages by application name and version: Read • Set or cancel user certificate: Manage certificates • Renew user certificate: Manage certificates • Set user certificate tag: Manage certificates • Run generation of MDM installation package; cancel generation of MDM installation package: Connect new devices 	None	None	None

Functional area	Right	User action: right required to perform the action	Task	Report	Other
System management: Connectivity	<ul style="list-style-type: none"> • Start RDP sessions • Connect to existing RDP sessions • Initiate tunneling • Save files from devices to the administrator's workstation • Read • Modify • Execute • Perform operations on device selections 	<ul style="list-style-type: none"> • Create desktop sharing session: The right to create desktop sharing session • Create RDP session: Connect to existing RDP sessions • Create tunnel: Initiate tunneling • Save content network list: Save files from devices to the administrator's workstation 	None	"Report on device users"	None
System management: Hardware inventory	<ul style="list-style-type: none"> • Read • Modify • Execute • Perform operations on device selections 	<ul style="list-style-type: none"> • Get or export hardware inventory object: Read • Add, set or delete hardware inventory object: Write 	None	<ul style="list-style-type: none"> • "Report on hardware registry" • "Report on configuration changes" • "Report on hardware" 	None

Functional area	Right	User action: right required to perform the action	Task	Report	Other
System management: Network access control	<ul style="list-style-type: none"> • Read • Modify 	<ul style="list-style-type: none"> • View CISCO settings: Read • Change CISCO settings: Write 	None	None	None
System management: Operating system deployment	<ul style="list-style-type: none"> • Deploy PXE servers • Read • Modify • Execute • Perform operations on device selections 	<ul style="list-style-type: none"> • Deploy PXE servers: Deploy PXE servers • View a list of PXE servers: Read • Start or stop the installation process on PXE clients: Execute • Manage drivers for WinPE and operating system images: Modify 	"Create installation package upon reference device OS image"	None	Installation package: "OS Image"

<p>System management: Vulnerability and patch management</p>	<ul style="list-style-type: none"> • Read • Modify • Execute • Perform operations on device selections 	<ul style="list-style-type: none"> • View third-party patch properties: Read • Change third-party patch properties: Modify 	<ul style="list-style-type: none"> • "Perform Windows Update synchronization" • "Install Windows Update updates" • "Fix vulnerabilities" • "Install required updates and fix vulnerabilities" 	<p>"Report on software updates"</p>	<p>None</p>
---	--	--	---	-------------------------------------	-------------

Functional area	Right	User action: right required to perform the action	Task	Report	Other
			litie s"		
System management: Remote installation	<ul style="list-style-type: none"> • Read • Modify • Execute • Perform operations on device selections 	<ul style="list-style-type: none"> • View third-party Vulnerability and Patch Management based installation package properties: Read • Change third-party Vulnerability and Patch Management based installation package properties: Modify 	None	None	Installation packages: <ul style="list-style-type: none"> • "Custom application" • "VAPM package"

Functional area	Right	User action: right required to perform the action	Task	Report	Other
System management: Software inventory	<ul style="list-style-type: none"> • Read • Modify • Execute • Perform operations on device selections 	None	None	<ul style="list-style-type: none"> • "Report on installed applications" • "Report on applications registry history" • "Report on status of licensed applications groups" • "Report on third-party software license keys" 	None

Predefined user roles

User roles assigned to Kaspersky Security Center users provide them with sets of access rights to application features (on page [684](#)).

You can use the predefined user roles with already configured set of rights, or create new roles and configure the required rights yourself. Some of the predefined user roles available in Kaspersky Security Center can be associated with specific job positions, for example, **Auditor**, **Security Officer**, **Supervisor** (these roles are present in Kaspersky Security Center starting from the version 11). Access rights of these roles are pre-configured in accordance with the standard tasks and scope of duties of the associated positions. The table below shows how roles can be associated with specific job positions.

Table 63. Examples of roles for specific job positions

Role	Comment
Auditor	Permits all operations with all types of reports, all viewing operations, including viewing deleted objects (grants the Read and Modify permissions in the Deleted objects area). Does not permit other operations. You can assign this role to a person who performs the audit of your organization.
Supervisor	Permits all viewing operations; does not permit other operations. You can assign this role to a security officer and other managers in charge of the IT security in your organization.
Security Officer	Permits all viewing operations, permits reports management; grants limited permissions in the System management: Connectivity area. You can assign this role to an officer in charge of the IT security in your organization.

The table below shows the access rights assigned to each predefined user role.

Table 64. Access rights of predefined user roles

Role	Description
Administration Server Administrator	<p>Permits all operations in the following functional areas:</p> <ul style="list-style-type: none"> • General features: <ul style="list-style-type: none"> • Basic functionality • Event processing • Hierarchy of Administration Servers • Virtual Administration Servers • System management: <ul style="list-style-type: none"> • Connectivity • Hardware inventory • Software inventory
Administration Server Operator	<p>Grants the Read and Execute rights in all of the following functional areas:</p> <ul style="list-style-type: none"> • General features: <ul style="list-style-type: none"> • Basic functionality • Virtual Administration Servers • System management: <ul style="list-style-type: none"> • Connectivity • Hardware inventory • Software inventory
Auditor	<p>Permits all operations in the following functional areas:</p> <ul style="list-style-type: none"> • General features: <ul style="list-style-type: none"> • Access objects regardless of their ACLs • Deleted objects • Enforced report management <p>You can assign this role to a person who performs the audit of your organization.</p>

Role	Description
Installation Administrator	<p>Permits all operations in the following functional areas:</p> <ul style="list-style-type: none"> • General features: <ul style="list-style-type: none"> • Basic functionality • Kaspersky software deployment • License key management • System management: <ul style="list-style-type: none"> • Operating system deployment • Vulnerability and patch management • Remote installation • Software inventory <p>Grants Read and Execute rights in the General features: Virtual Administration Servers functional area.</p>
Installation Operator	<p>Grants the Read and Execute rights in all of the following functional areas:</p> <ul style="list-style-type: none"> • General features: <ul style="list-style-type: none"> • Basic functionality • Kaspersky software deployment (also grants the Manage Kaspersky patches right in this area) • Virtual Administration Servers • System management: <ul style="list-style-type: none"> • Operating system deployment • Vulnerability and patch management • Remote installation • Software inventory
Kaspersky Endpoint Security Administrator	<p>Permits all operations in the following functional areas:</p> <ul style="list-style-type: none"> • General features: Basic functionality • Kaspersky Endpoint Security area, including all features
Kaspersky Endpoint Security Operator	<p>Grants the Read and Execute rights in all of the following functional areas:</p> <ul style="list-style-type: none"> • General features: Basic functionality • Kaspersky Endpoint Security area, including all features
Main Administrator	<p>Permits all operations in functional areas, <i>except</i> for the following areas:</p> <ul style="list-style-type: none"> • General features: <ul style="list-style-type: none"> • Access objects regardless of their ACLs • Enforced report management

Role	Description
Main Operator	<p>Grants the Read and Execute (where applicable) rights in all of the following functional areas:</p> <ul style="list-style-type: none"> • General features: <ul style="list-style-type: none"> • Basic functionality • Deleted objects • Operations on Administration Server • Kaspersky Lab software deployment • Virtual Administration Servers • Mobile Device Management: General • System management, including all features • Kaspersky Endpoint Security area, including all features
Mobile Device Management Administrator	<p>Permits all operations in the following functional areas:</p> <ul style="list-style-type: none"> • General features: Basic functionality • Mobile Device Management: General
Mobile Device Management Operator	<p>Grants the Read and Execute rights in the General features: Basic functionality functional area.</p> <p>Grants Read and Send only information commands to mobile devices in the following functional areas:</p> <ul style="list-style-type: none"> • Mobile Device Management: General
Security Officer	<p>Permits all operations in the following functional areas:</p> <ul style="list-style-type: none"> • General features: <ul style="list-style-type: none"> • Access objects regardless of their ACLs • Enforced report management <p>Grants the Read, Modify, Execute, Save files from devices to the administrator's workstation, and Perform operations on device selections rights in the System management: Connectivity functional area.</p> <p>You can assign this role to an officer in charge of the IT security in your organization.</p>
Self Service Portal User	<p>Permits all operations in the Mobile Device Management: Self Service Portal functional area. This feature is not supported in Kaspersky Security Center 11 and later version.</p>

Role	Description
Supervisor	Grants the Read right in the General features: Access objects regardless of their ACLs and General features: Enforced report management functional area. You can assign this role to a security officer and other managers in charge of the IT security in your organization.
Vulnerability and Patch Management Administrator	Permits all operations in the General features: Basic functionality and System management (including all features) functional areas.
Vulnerability and Patch Management Operator	Grants the Read and Execute (where applicable) rights in the General features: Basic functionality and System management (including all features) functional areas.

Adding a user role

► To add a user role:

1. In the console tree, select the node with the name of the required Administration Server.
2. In the context menu of the Administration Server, select **Properties**.
3. In the Administration Server properties window, in the **Sections** pane select **User roles** and click the **Add** button.

The **User roles** section is available if the **Display security settings sections** (see section "**Adjusting the general settings of Administration Server**" on page [609](#)) option is enabled.

4. In the **New role** properties window, configure the role:
 - In the **Sections**, select **General** and specify the name of the role.
The name of a role cannot be more than 100 characters long.
 - Select the **Rights** section, and configure the set of rights by selecting the **Allow** and **Deny** check boxes next to the application features.

If you are operating on the primary Administration Server, you can enable the **Relay list of roles to secondary Administration Servers** option (see section "Propagating user roles to secondary Administration Servers" on page [709](#)).

5. Click **OK**.

The role is added.

User roles that have been created for Administration Server are displayed in the Administration Server properties window, in the **User roles** section. You can modify and delete user roles, as well as assign roles to user groups (see section "Assigning a role to a user or a user group" on page [707](#)) or selected users.

Assigning a role to a user or a user group

► *To assign a role to a user or a group of users:*

1. In the console tree, select the node with the name of the required Administration Server.
2. In the context menu of the Administration Server, select **Properties**.
3. In the Administration Server properties window, select the **Security** section.

The **Security** section is available if the **Display security settings sections** (see section "**Adjusting the general settings of Administration Server**" on page [609](#)) check box is selected in the interface settings window.

4. In the **Names of groups or users** field, select a user or a group of users to which you want to assign a role.

If the user or the group is not contained in the field, you can add it by clicking the **Add** button.

When you add a user by clicking the **Add** button, you can select the type of user authentication (Microsoft Windows or Kaspersky Security Center). Kaspersky Security Center authentication is used for selecting the accounts of internal users that are used for working with virtual Administration Servers.

5. Select the **Roles** tab and click the **Add** button.

The **User roles** window opens. This window displays user roles that have been created.

6. In the **User roles** window, select a role for the user group.
7. Click **OK**.

The role with a set of rights for working with Administration Server is assigned to the user or the user group. Roles that have been assigned are displayed on the **Roles** tab in the **Security** section of the Administration Server properties window.

Assigning permissions to users and groups

You can give users and groups permissions to use different features of Administration Server and of the Kaspersky programs for which you have management plug-ins, for example, Kaspersky Endpoint Security for Windows.

► *To assign permissions to a user or a group of users:*

1. In the console tree, do one of the following:
 - Expand the **Administration Server** node and select the subfolder with the name of the required Administration Server.
 - Select the administration group.
2. In the context menu of the Administration Server or the administration group, select **Properties**.
3. In the Administration Server properties window (or the administration group properties window) that opens, in the left **Sections** pane select **Security**.

The **Security** section is available if the **Display security settings sections** (see section "**Adjusting the general settings of Administration Server**" on page [609](#)) check box is selected in the interface settings window.

4. In the **Security** section, in the **Names of groups or users** list select a user or a group.
5. In the permissions list in the lower part of the workspace, on the **Rights** tab configure the set of rights for the user or group:
 - a. Click the plus signs (+) to expand the nodes in the list and gain access to the permissions.
 - b. Select the **Allow** and **Deny** check boxes next to the permissions that you want.

Example 1: Expand the **Access objects regardless of their ACLs** node or **Deleted objects** node, and select **Read**.

Example 2: Expand the **Basic functionality** node, and select **Write**.

6. When you have configured the set of rights, click **Apply**.

The set of rights for the user or group of users will be configured.

The permissions of the Administration Server (or the administration group) are divided into the following areas:

- General features
 - Management of administration groups (only for Kaspersky Security Center 11 or later)
 - Access objects regardless of their ACLs (only for Kaspersky Security Center 11 or later)
 - Basic functionality
 - Deleted objects (only for Kaspersky Security Center 11 or later)
 - Event processing
 - Operations on Administration Server (only in the property window of Administration Server)
 - Deploy Kaspersky applications
 - License key management
 - Enforced report management (only for Kaspersky Security Center 11 or later)
 - Hierarchy of Servers
 - User rights
 - Virtual Administration Servers
- Mobile Device Management
 - General
- System Management
 - Connectivity
 - Hardware inventory
 - Network Access Control
 - Deploy operating system
 - Manage vulnerabilities and patches

- Remote installation
- Software inventory

If neither **Allow** nor **Deny** is selected for a permission, then the permission is considered *undefined*: it is denied until it is explicitly denied or allowed for the user.

The rights of a user are the sum of:

- the user's own rights
- the rights of all the roles assigned to this user
- the rights of all the security group to which the user belongs
- the rights of all the roles assigned to the security groups to which the user belongs

If at least one of these sets of rights has **Deny** for a permission, then the user is denied this permission, even if other sets allow it or leave it undefined.

Propagating user roles to secondary Administration Servers

By default, the lists of user roles of the primary and secondary Administration Servers are independent. You can configure the application to automatically propagate the user roles created on the primary Administration Server to all of the secondary Administration Servers. The user roles can also be propagated from a secondary Administration Server to its own secondary Administration Servers.

► *To propagate user roles from the primary Administration Server to the secondary Administration Servers:*

1. Open the main application window.
2. Do one of the following:
 - In the console tree, right-click the name of the Administration Server and select **Properties** in the context menu.
 - If you have an active Administration Server policy, in the workspace of the **Policies** folder, right-click this policy and select **Properties** in the context menu.
3. In the Administration Server properties window, or in the policy settings window, in the **Sections** pane select **User roles**.

The **User roles** section is available if the **Display security settings sections** (see section "**Adjusting the general settings of Administration Server**" on page [609](#)) option is enabled.

4. Enable the **Relay list of roles to secondary Administration Servers** option.
5. Click **OK**.

The application copies the user roles of the primary Administration Server to the secondary Administration Servers.

When the **Relay list of roles to secondary Administration Servers** option is enabled and the user roles are propagated, they cannot be edited or deleted on the secondary Administration Servers. When you create a new role or edit an existing one on the primary Administration Server, the changes are automatically copied to the

secondary Administration Servers. When you delete a user role on the primary Administration Server, this role remains on the secondary Administration Servers afterward, but it can be edited or deleted.

The roles that are propagated to the secondary Administration Server from the primary Server are displayed with the lock (🔒) icon. You cannot edit these roles on the secondary Administration Server.

If you create a role on the primary Administration Server, and there is a role with the same name on its secondary Administration Server, the new role is copied to the secondary Administration Server with the index added to its name, for example, ~~1, ~~2 (the index can be random).

If you disable the **Relay list of roles to secondary Administration Servers** option, all the user roles remain on the secondary Administration Servers, but they become independent from those on the primary Administration Server. After becoming independent, the user roles on the secondary Administration Servers can be edited or deleted.

Assigning the user as a device owner

You can assign the user as a device owner to allocate a device to that user. If you have to perform some actions on the device (for example, upgrade hardware), the administrator can notify the device owner to authorize those actions.

► *To assign a user as the owner of a device:*

1. In the console tree, select the **Managed devices** folder.
2. In the workspace of the folder, on the **Devices** tab, select the device for which you need to assign an owner.
3. In the context menu of the device, select **Properties**.
4. In the device properties window, select **System Info** → **Sessions**.
5. Click the **Assign** button next to the **Device owner** field.
6. In the **User selection** window, select the user to assign as the device owner and click **OK**.
7. Click **OK**.

The device owner is assigned. By default, the **Device owner** field is filled with a value from Active Directory and is updated during every Active Directory poll (see section "Active Directory polling" on page [308](#)). You can view the list of device owners in the **Report on device owners**. You can create a report using the **New Report Wizard** (see section "Creating a report template" on page [504](#)).

Delivering messages to users

► *To send a message to a user by email:*

1. In the console tree, in the **User accounts** folder, select a user.
The **User accounts** folder is a subfolder of the **Advanced** folder by default.
2. In the user's context menu, select **Notify by email**.
3. Fill in the relevant fields in the **Send message to user** window and click the **OK** button.

The message will be sent to the email address that has been specified in the user's properties.

► *To send an SMS message to a user:*

1. In the console tree, in the **User accounts** folder, select a user.
2. In the user's context menu, select **Send an SMS**.
3. Fill in the relevant fields in the **SMS text** window and click the **OK** button.

The message will be sent to the mobile device with the number that has been specified in the user's properties.

Viewing the list of user mobile devices

► *To view a list of a user's mobile devices:*

1. In the console tree, in the **User accounts** folder, select a user.
The **User accounts** folder is a subfolder of the **Advanced** folder by default.
2. In the context menu of the user account, select **Properties**.
3. In the properties window of the user account, select the **Mobile devices** section.

In the **Mobile devices** section, you can view the list of the user's mobile devices and information about each of them. You can click the **Export to file** button to save the list of mobile devices to a file.

Installing a certificate for a user

You can install three types of certificates for a user:

- Shared certificate, which is required to identify the user's mobile device.
- Mail certificate, which is required to set up the corporate mail on the user's mobile device.
- VPN certificate, which is required to set up the virtual private network on the user's mobile device.

► *To issue a certificate to a user and then install it:*

1. In the console tree, open the **User accounts** folder and select a user account.
The **User accounts** folder is a subfolder of the **Advanced** folder by default.
2. In the context menu of the user account, select **Install certificate**.

The Certificate Installation Wizard starts. Follow the instructions of the Wizard.

After the Certificate Installation Wizard has finished, the certificate will be created and installed for the user. You can view the list of installed user certificates and export it to a file (see section "Viewing the list of certificates issued to a user" on page [711](#)).

Viewing the list of certificates issued to a user

► *To view a list of all certificates issued to a user:*

1. In the console tree, in the **User accounts** folder, select a user.
The **User accounts** folder is a subfolder of the **Advanced** folder by default.
2. In the context menu of the user account, select **Properties**.
3. In the properties window of the user account, select the **Certificates** section.

In the **Certificates** section, you can view the list of the user's certificates and information about each of them. You can click the **Export to file** button to save the list of certificates to a file.

About the administrator of a virtual Administration Server

An administrator of the enterprise network managed through a virtual Administration Server starts Kaspersky Security Center 13 Web Console under the user account specified in this window to view the details of anti-virus protection.

If necessary, several administrator accounts can be created on a virtual Server.

The administrator of a virtual Administration Server is an internal user of Kaspersky Security Center. No data on internal users is transferred to the operating system. Kaspersky Security Center authenticates internal users.

Remote installation of operating systems and applications

Kaspersky Security Center allows you to create operating system images and deploy them on client devices on the network, as well as perform remote installation of applications by Kaspersky or other vendors.

Capturing images of operating systems

Kaspersky Security Center can capture operating system images from devices and transfer those images to the Administration Server. Such images of operating systems are stored on the Administration Server in a dedicated folder. The operating system image of a reference device is captured and then created through an installation package creation task (see section "Creating installation packages of applications" on page [717](#)).

To create images of operating systems, Windows Automated Installation Kit (Windows AIK) tool package must be installed on Administration Server.

The functionality of operating system image capturing has the following features:

- An operating system image cannot be captured on a device on which Administration Server is installed.
- During capture of an operating system image, the sysprep.exe utility resets the settings of the reference device. If you want to restore the settings of the reference device, select the **Create backup copy of the device state** check box in the Operating System Image Creation Wizard.
- The image capturing process provides for a restart of the reference device.

Deploying images of operating systems on new devices

The administrator can use the images received for deployment on new networked devices on which no operating system has been installed yet. A technology named Preboot eXecution Environment (PXE) is used in this case. The administrator selects a networked device that will act as PXE server. This device must meet the following requirements:

- Network Agent must be installed on the device.

- A DHCP server cannot be active on the device because a PXE server uses the same ports as a DHCP server.
- The network segment that includes the device must not contain any other PXE servers.

The following conditions must be met to deploy an operating system: a network card must be mounted on the device, the device must be connected to the network, and the Network boot option must be selected in BIOS when booting the device.

Deployment of an operating system is performed as follows:

1. The PXE server establishes a connection with the new client device while the latter is booting up.
2. The client device becomes included in Windows Preinstallation Environment (WinPE).

Adding the device to WinPE may require configuration of the set of drivers for WinPE.

3. The client device is registered on Administration Server.
4. The administrator assigns the client device an installation package with an operating system image.

The administrator can add required drivers to the installation package with the operating system image. The administrator can also specify a configuration file with the operating system settings (answer file) that is to be applied during installation.

5. The operating system is deployed on the client device.

The administrator can manually specify the MAC addresses of client devices that have not yet been connected, and assign them the installation package with the operating system image. When the selected client devices connect to the PXE server, the operating system is automatically installed on those devices.

Deploying images of operating systems on devices where another operating system has already been installed

Deployment of images of operating systems on client devices where another operating system has already been installed is performed through the remote installation task for specific devices.

Installing applications by Kaspersky and other vendors

The administrator can create installation packages of any applications, including those specified by the user, and install the applications on client devices through the remote installation task.

In this section

Creating images of operating systems	714
Installing images of operating systems.....	714
Adding drivers for Windows Preinstallation Environment (WinPE)	715
Adding drivers to an installation package with an operating system image	716
Configuring sysprep.exe utility.....	716
Deploying operating systems on new networked devices.....	716
Deploying operating systems on client devices.....	717
Creating installation packages of applications.....	717
Issuing a certificate for installation packages of applications	718
Installing applications on client devices.....	719

Creating images of operating systems

Images of operating systems are created using the task of removing the operating system image of the reference device.

► *To create the operating system image making task:*

1. In the **Remote installation** folder of the console tree, select the **Installation packages** subfolder.
2. Click the **Create installation package** button to run the New Package Wizard.
3. In the **Select installation package type** window of the Wizard, click the **Create an installation package with the operating system image** button.
4. Follow the instructions of the Wizard.

When the Wizard finishes, an Administration Server task is created named **Create installation package upon reference device OS image**. You can view the task in the **Tasks** folder.

When the **Create installation package upon reference device OS image** task is complete, an installation package is created that you can use to deploy the operating system on client devices through a PXE server or the remote installation task. You can view the installation package in the **Installation packages** folder.

Installing images of operating systems

Kaspersky Security Center allows you to deploy WIM images of desktop and server-based Windows® operating systems on devices within an organization's network.

The following methods can be used to retrieve an operating system image that would be deployable by using Kaspersky Security Center tools:

- Import from the install.wim file included in the Windows distribution package
- Capturing an image from a reference device

Two scenarios are supported for deployment of operating system images:

- Deployment on a "clean" device, that is, without any operating system installed
- Deployment on a device running Windows

The Administration Server implicitly features a service image of Windows Preinstallation Environment (Windows PE), which is always used both for capturing operating system images, and for their deployment. All drivers required for proper functioning of all target devices must be added to WinPE. Generally, chipset drivers required for the functioning of Ethernet networking interface must be added.

The following requirements must be met in order to implement scenarios of image deployment and capture:

- Windows Automated Installation Kit (WAIK) version 2.0, or later, or Windows Assessment and Deployment Kit (WADK) must be installed on the Administration Server. If the scenario allows for installing or capturing images on Windows XP, WAIK must be installed.
- A DHCP server must be available on the network where the target device is located.
- The shared folder of the Administration Server must be open for reading from the network where the target device is located. If the shared folder is located on the Administration Server, access is required for the KIPxeUser account (this account is created automatically while running the Administration Server Installer). If the shared folder is located outside the Administration Server, access must be granted to everyone.

When selecting the operating system image to be installed, the administrator must explicitly specify the CPU architecture of the target device: x86 or x86-64.

Adding drivers for Windows Preinstallation Environment (WinPE)

► *To add drivers for Windows Preinstallation Environment (WinPE):*

1. In the **Remote installation** folder in the console tree, select the **Deploy device images** subfolder.
2. In the workspace of the **Deploy device images** folder, click the **Additional actions** button and select **Configure driver set for Windows Preinstallation Environment (WinPE)** in the drop-down list.

The **Windows Preinstallation Environment drivers** window opens.

3. In the **Windows Preinstallation Environment drivers** window click the **Add** button.

The **Select driver** window opens.

4. In the **Select driver** window, select a driver from the list.

If the necessary driver is missing from the list, click the **Add** button and specify the driver name and folder of the driver distribution package in the **Add driver** window that opens.

You can select a folder by clicking the **Browse** button.

In the **Add driver** window, click **OK**.

5. In the **Select driver** window, click **OK**.

The driver will be added to the Administration Server repository. When added to the repository, the driver is displayed in the **Select driver** window.

6. In the **Windows Preinstallation Environment drivers** window, click **OK**.

The driver will be added to Windows Preinstallation Environment (WinPE).

Adding drivers to an installation package with an operating system image

► *To add drivers to an installation package with an operating system image:*

1. In the **Remote installation** folder of the console tree, select the **Installation packages** subfolder.
2. From the context menu of an installation package with an operating system image, select **Properties**.

The installation package properties window opens.

3. In the installation package properties window, select the **Additional drivers** section.
4. Click the **Add** button in the **Additional drivers** section.

The **Select driver** window opens.

5. In the **Select driver** window, select drivers that you want to add to the installation package with the operating system image.

You can add new drivers to the Administration Server repository by clicking the **Add** button in the **Select driver** window.

6. Click **OK**.

Added drivers are displayed in the **Additional drivers** section of the properties window of the installation package with the operating system image.

Configuring sysprep.exe utility

The sysprep.exe utility is intended to prepare the device for creation of an operating system image.

► *To configure sysprep.exe utility:*

1. In the **Remote installation** folder of the console tree, select the **Installation packages** subfolder.
2. From the context menu of an installation package with an operating system image, select **Properties**.

The installation package properties window opens.

3. In the installation package properties window, select the **sysprep.exe settings** section.
4. In the **sysprep.exe settings** section, specify a configuration file to be used during deployment of the operating system on the client device:

- **Use default configuration file.** Select this option to use the answer file generated by default during capture of the operating system image.
- **Specify custom values of main settings.** Select this option to specify values for settings through the user interface.
- **Specify configuration file.** Select this option to use a custom answer file.

5. To apply the changes made, click the **Apply** button.

Deploying operating systems on new networked devices

► *To deploy an operating system on new devices that have not yet had any operating system installed:*

1. In the **Remote installation** folder in the console tree, select the **Deploy device images** subfolder.

2. Click the **Additional actions** button and select **Manage the list of PXE servers on the network** in the drop-down list.

The **Properties: Deploy device images** window opens, on the **PXE servers** section.

3. In the **PXE servers** section, click the **Add** button and, in the **PXE servers** window that opens, select the device that will be used as PXE server.

The device that you added is displayed in the PXE servers section.

4. In the **PXE servers** section select a PXE server and click the **Properties** button.
5. In the properties window of the selected PXE server, on the **PXE server connection settings** tab configure connection between Administration Server and the PXE server.
6. Boot the client device on which you want to deploy the operating system.
7. In the BIOS of the client device, select the Network boot installation option.

The client device connects to the PXE server and is then displayed in the workspace of the **Deploy device images** folder.

8. In the **Actions** section, click the **Assign installation package** link to select the installation package that will be used for the operating system installation on the selected device.

After you added the device and assigned the installation package to it, the operating system deployment starts automatically on this device.

9. To cancel the operating system deployment on the client device, click the **Cancel OS image installation** link in the **Actions** section.

► *To add devices by MAC address:*

- In the **Deploy device images** folder, click **Add device MAC address** to open the **New device** window, and specify the MAC address of the device that you want to add.
- In the **Deploy device images** folder, click **Import MAC addresses of devices from file** to select the file containing a list of MAC addresses of all devices on which you want to deploy an operating system.

Deploying operating systems on client devices

► *To deploy an operating system on client devices with another operating system already installed:*

1. In the console tree, open the **Remote installation** folder and click the **Deploy installation package on managed devices (workstations)** link to run the Protection Deployment Wizard.
2. In the **Select installation package** window of the Wizard specify an installation package with an operating system image.
3. Follow the instructions of the Wizard.

When the Wizard completes its operation, a remote installation task is created for installing the operating system on client devices. You can start or stop the task in the **Tasks** folder.

Creating installation packages of applications

► *To create an application installation package:*

1. In the **Remote installation** folder of the console tree, select the **Installation packages** subfolder.

2. Click the **Create installation package** button to run the New Package Wizard.
3. In the **Select installation package type** window of the Wizard, click one of the following buttons:
 - **Create an installation package for a Kaspersky application.** Select this option if you want to create an installation package for a Kaspersky application.
 - **Create an installation package for the specified executable file.** Select this option if you want to create an installation package for a third-party application by using an executable file. Typically, the executable file is a setup file of the application.
 - **Copy entire folder to the installation package**
 - **Specify installation parameters**
 - **Select an application from the Kaspersky database to create an installation package.** Select this option if you want to select the required third-party application from the Kaspersky database to create an installation package. The database is created automatically when you run the Download updates to the repository of the Administration Server (see section "Creating the task for downloading updates to the repository of the Administration Server" on page [413](#)) task; the applications are displayed in the list.
 - **Create an installation package with the operating system image.** Select this option if you have to create an installation package with an image of the operating system of a reference device.

When the Wizard finishes, an Administration Server task is created with the name **Create installation package upon reference device OS image**. When this task is completed, an installation package is created that you can use to deploy the operating system image through a PXE server or the remote installation task.

4. Follow the instructions of the Wizard.

When the Wizard finishes, an installation package is created that you can use to install the application on client devices. You can view the installation package by selecting **Installation packages** in the console tree.

See also:

Creating an installation package	344
Scenario: Deployment for cloud environment	821

Issuing a certificate for installation packages of applications

► *To issue a certificate for the installation package of an application:*

1. In the **Remote installation** folder of the console tree, select the **Installation packages** subfolder.
The **Remote installation** folder is a subfolder of the **Advanced** folder by default.
2. In the context menu of the **Installation packages** folder, select **Advanced**.
This opens the properties window of the **Installation packages** folder.
3. In the properties window of the **Installation packages** folder, select the **Sign stand-alone packages** section.
4. In the **Sign stand-alone packages** section, click the **Specify** button.
The **Certificate** window.

5. In the **Certificate type** field, specify the public or private certificate type:
 - If the **PKCS #12 container** value is selected, specify the certificate file and the password.
 - If the **X.509 certificate** value is selected:
 - a. Specify the private key file (one with the *.prk or *.pem extension).
 - b. Specify the private key password.
 - c. Specify the public key file (one with the *.cer extension).
6. Click **OK**.

A certificate for the installation package of the application is issued.

Installing applications on client devices

► *To install an application on client devices:*

1. In the console tree, open the **Remote installation** folder and click **Deploy installation package on managed devices (workstations)** to run the Protection Deployment Wizard.
2. In the **Select installation package** window of the Wizard specify the installation package of an application that you want to install.
3. Follow the instructions of the Wizard.

When the Wizard finishes, a remote installation task is created to install the application on client devices. You can start or stop the task in the **Tasks** folder.

Using the Protection Deployment Wizard, you can install Network Agent on client devices running Windows, Linux, and macOS.

To manage 64-bit security applications using Kaspersky Security Center on devices running Linux operating systems, you must use the 64-bit Network Agent for Linux. You can download the necessary version of Network Agent from the Technical Support website <https://support.kaspersky.com>.

Before remote installation of Network Agent on a device running Linux, you have to prepare the device (see section "Preparing a Linux device for remote installation of Network Agent" on page [355](#)).

See also:

Scenario: Deployment for cloud environment.....[821](#)

Managing object revisions

This section contains information about object revision management. Kaspersky Security Center allows you to track object modification. Every time you save changes made to an object, a *revision* is created. Each revision has a number.

Application objects that support revision management include:

- Administration Servers

- Policies
- Tasks
- Administration groups
- User accounts
- Installation packages

You can perform the following actions on object revisions:

- Compare a selected revision to the current one
- Compare selected revisions
- Compare an object to a selected revision of another object of the same type
- View a selected revision
- Roll back changes made to an object to a selected revision
- Save revisions as a .txt file

In the properties window of any object that supports revision management, the **Revision history** section displays a list of object revisions with the following details:

- Object revision number
- Date and time the object was modified
- Name of the user who modified the object
- Action performed on the object
- Description of the revision related to the change made to the object settings

By default, the object revision description is blank. To add a description to a revision, select the relevant revision and click the **Description** button. In the **Object revision description** window, enter some text for the revision description.

In this section

About object revisions.....	721
Viewing the Revision history section	721
Comparing object revisions	722
Setting storage term for object revisions and for deleted object information	723
Viewing an object revision	723
Saving an object revision to a file	724
Rolling back changes.....	724
Adding a revision description.....	725

About object revisions

You can perform the following actions on object revisions:

- Compare a selected revision to the current one
- Compare selected revisions
- Compare an object to a selected revision of another object of the same type (see section "Comparing object revisions" on page [722](#))
- View a selected revision (see section "Viewing the Revision history section" on page [721](#))
- Roll back changes made to an object to a selected revision (see section "Rolling back changes" on page [724](#))
- Save revisions as a .txt file (see section "Saving an object revision to a file" on page [724](#))

In the properties window of any object that supports revision management, the **Revision history** section displays a list of object revisions with the following details:

- Object revision number
- Date and time the object was modified
- Name of the user who modified the object
- Action performed on the object
- Description of the revision related to the change made to the object settings (see section "Adding a revision description" on page [725](#))

Viewing the Revision history section

You can compare revisions of an object to the current revision, compare different revisions selected in the list, or compare a revision of an object to a revision of another object of the same type.

► *To view the **Revision history** section of an object:*

1. In the console tree, select one of the following objects:
 - **Administration Server** node
 - **Policies** folder
 - **Tasks** folder
 - Folder of an administration group
 - **User accounts** folder
 - **Deleted objects** folder
 - **Installation packages** subfolder, which is nested in the **Remote installation** folder
2. Depending on the location of the relevant object, do one of the following:
 - If the object is in the **Administration Server** node or an administration group node, right-click the node, and in the context menu select **Properties**.
 - If the object is in the **Policies**, **Tasks**, **User accounts**, **Deleted objects**, or **Installation packages** folder, select the folder, and in the corresponding workspace select the object.

The object properties window opens.

3. In the left **Sections** pane, select **Revision history**.

The revision history is displayed in the workspace.

Comparing object revisions

You can compare past revisions of an object to the current revision, compare different revisions selected in the list, or compare a revision of an object to a revision of another object of the same type.

► *To compare revisions of an object:*

1. Select an object and proceed to the properties window of the object.
2. In the properties window, proceed to the **Revision history (see section "Viewing the Revision history section" on page 721)** section.
3. In the workspace, in the list of object revisions select the revision for comparison.

To select more than one revision of the object, use the SHIFT and CTRL keys.

4. Do one of the following:

- Click the **Compare** split button and select one of the values in the drop-down list:

- **Compare to current revision**

Select this option to compare the selected revision to the current one.

- **Compare selected revisions**

Select this option to compare two selected revisions.

- **Compare to another task**

If you work with task revisions, select **Compare to another task** to compare the selected revision to a revision of another task.

If you work with policy revisions, select **Compare to another policy** to compare the selected revision to a revision of another policy.

- Double-click the name of a revision, and in the revision properties window that opens click one of the following buttons:

- **Compare to current**

Click this button to compare the selected revision to the current one.

- **Compare to previous**

Click this button to compare the selected revision to the previous one.

A report in HTML format about comparison of the revisions is displayed in your default browser.

In this report, you can minimize some of the sections containing revision settings. To minimize a section with object revision settings, click the minimizing icon (▲) next to the section name.

Administration Server revisions include all details of changes made, except for details from the following areas:

- **Traffic** section
- **Tagging rules** section
- **Notification** section

- **Distribution points** section
- **Virus outbreak** section

No information is recorded, from the **Virus outbreak** section, about the configuration of policy activation that occurs when a Virus outbreak event is triggered.

You can compare revisions of a deleted object to a revision of an existing object, but not the reverse: you cannot compare revisions of an existing object to a revision of a deleted object.

Setting storage term for object revisions and for deleted object information

The storage term for object revisions and for information about deleted objects is the same. The default storage term is 90 days. This is enough time for the regular audit of the program.

Only users with **Modify** permission in the **Deleted objects** area (see section "Assigning permissions to users and groups" on page [707](#)) can change the storage period.

► *To change the storage term for object revisions and for information about deleted objects:*

1. In the console tree, select the Administration Server for which you want to change the storage period.
2. Right-click and in the context menu select **Properties**.
3. In the Administration Server properties window that opens, in the **Revision history repository** section enter the desired storage term (the number of days).
4. Click **OK**.

The object revisions and information about deleted objects will be stored for the number of days that you entered.

Viewing an object revision

If you need to know which modifications were made to an object over a certain period of time, you can view the revisions of this object.

► *To view the revisions of an object:*

1. Proceed to the **Revision history** (see section "**Viewing the Revision history section**" on page [721](#)) section of the object.
2. In the list of object revisions, select the revision whose settings you want to view.
3. Do one of the following:
 - Click the **View revision** button.
 - Open the revision properties window by double-clicking the revision name, and then clicking the **View revision** button.

A report in HTML format with the settings of the selected object revision is displayed. In this report, you can minimize some of the sections with object revision settings. To minimize a section with object revision settings, click the minimizing icon (▲) next to the section name.

Saving an object revision to a file

You can save an object revision as a text file, for example, in order to send it by email.

► *To save an object revision to a file:*

1. Proceed to the **Revision history** (see section "**Viewing the Revision history section**" on page [721](#)) section of the object.
2. In the list of revisions of an object, select the one whose settings you have to save.
3. Click the **Advanced** button and select the **Save to file** value in the drop-down list.

The revision is now saved as a .txt file.

Rolling back changes

You can roll back changes made to an object, if necessary. For example, you may have to revert the settings of a policy to their state on a specific date.

► *To roll back changes made to an object:*

1. Proceed to the **Revision history** (see section "**Viewing the Revision history section**" on page [721](#)) section of the object.
2. In the list of object revisions, select the number of the revision to which you have to roll back changes.
3. Click the **Advanced** button and select the **Roll back** value in the drop-down list.

The object is now rolled back to the selected revision. The list of object revisions displays a record of the action that was taken. The revision description displays information about the number of the revision to which you reverted the object.

Adding a revision description

You can add a description for the revision to simplify the search for revisions in the list.

► *To add a description for a revision:*

1. Proceed to the **Revision history** (see section "**Viewing the Revision history section**" on page [721](#)) section of the object.
2. In the list of object revisions, select the revision for which you need to add a description.
3. Click the **Description** button.
4. In the **Object revision description** window, enter some text for the revision description.
By default, the object revision description is blank.
5. Click **OK**.

Deletion of objects

This section provides information about deleting objects and viewing information about objects after they are deleted.

You can delete objects, including the following:

- Policies
- Tasks
- Installation packages
- Virtual Administration Servers
- Users
- Security groups
- Administration groups

When you delete an object, information about it remains in the database. The storage term (see section "Setting storage term for object revisions and for deleted object information" on page [723](#)) for information about the deleted objects is the same as the storage term for object revisions (the recommended term is 90 days). You can change the storage term only if you have the **Modify** permission (see section "Assigning permissions to users and groups" on page [707](#)) in the **Deleted objects** area of rights.

In this section

Deleting an object	726
Viewing information about deleted objects	726
Deleting objects permanently from the list of deleted objects	727

Deleting an object

You can delete objects such as policies, tasks, installation packages, internal users, and internal user groups if you have **Modify** permission, which is in the **Basic** functionality category of rights (see [Assigning permissions to users and groups](#) (on page [707](#)) for more information).

► *To delete an object:*

1. In the console tree, in the workspace of the required folder select an object.
2. Do one of the following:
 - Right-click the object and select **Delete**.
 - Press the **DELETE** key.

The object will be deleted, and the information about it will be stored in the database.

Viewing information about deleted objects

Information about deleted objects is stored in the **Deleted objects** folder for the same amount of time as object revisions (the recommended period is 90 days).

Only users with **Read** permission in the **Deleted objects** area of rights can view the list of deleted objects (see [Assigning permissions to users and groups](#) (on page [707](#)) for more information).

► *To view the list of deleted objects,*

In the console tree, select **Deleted objects** (by default, **Deleted objects** is a subfolder of the **Advanced** folder).

If you do not have **Read** permission in the **Deleted objects** area of rights, an empty list is displayed in the **Deleted objects** folder.

The workspace of the **Deleted objects** folder contains the following information about deleted objects:

- **Name.** The name of the object.
- **Type.** Object type, such as policy, task, or installation package.
- **Time.** Time when the object was deleted.
- **User.** Account name of the user who deleted the object.

► *To view more information about an object:*

1. In the console tree, select **Deleted objects** (by default, **Deleted objects** is a subfolder of the **Advanced** folder).
2. In the **Deleted objects** workspace, select the object that you want.

The box for working with the selected object appears on the right side of the workspace.

3. Do one of the following:

- Click the **Properties** link in the box.
- Right-click the object you selected in the workspace, and in the context menu select **Properties**.

The properties window of the object opens, displaying the following tabs:

- **General**
- **Revision history** (see section "**Managing object revisions**" on page [719](#))

Deleting objects permanently from the list of deleted objects

Only users with **Modify** permission in the **Deleted objects** area of rights can delete objects permanently from the list of deleted objects (see Assigning permissions to users and groups (on page [707](#)) for more information).

► *To delete an object from the list of deleted objects:*

1. In the console tree, select the node of the required Administration Server and then select the **Deleted objects** folder.
2. In the workspace, select the object(s) that you want to delete.
3. Do one of the following:
 - Press the **DELETE** key.
 - In the context menu of the object(s) that you selected, select **Delete**.
4. In the confirmation dialog box, click **Yes**.

The object is deleted permanently from the list of deleted objects. All information about this object (including all its revisions) is permanently removed from the database. You cannot restore this information.

Mobile Device Management

Management of mobile device protection through Kaspersky Security Center is carried out by using the Mobile Device Management feature, which requires a dedicated license. If you are intending to manage mobile devices owned by employees in your organization, you must enable Mobile Device Management.

This section provides instructions for enabling, configuring and disabling Mobile Device Management. This section also describes how to manage mobile devices connected to Administration Server.

For details about Kaspersky Security for Mobile, see *Kaspersky Security for Mobile Help*.

See also:

Scenario: Installation and initial setup of Kaspersky Security Center 13 Web Console	962
Scenario: Mobile Device Management deployment	728
About group policy for managing EAS and iOS MDM devices.....	729
Enabling Mobile Device Management	730
Modifying the Mobile Device Management settings	731
Disabling Mobile Device Management	732
Working with commands for mobile devices	733
Working with certificates	737
Adding iOS mobile devices to the list of managed devices.....	744
Adding Android mobile devices to the list of managed devices	746
Managing Exchange ActiveSync mobile devices	749
Managing iOS MDM devices	755
Managing KES devices.....	766

Scenario: Mobile Device Management deployment

This section provides a scenario for configuring the Mobile Device Management feature in Kaspersky Security Center.

Prerequisites

Make sure that you have a license that grants access to the Mobile Device Management feature.

Deployment of the Mobile Device Management feature proceeds in stages:

a. Preparing the ports

Make sure that port 13292 is available on the Administration Server. This port is required for connecting mobile devices (see section "Ports used by Kaspersky Security Center" on page [65](#)). Also, you may want to make port 17100 available. This port is only required for the activation proxy server for managed mobile devices; if managed mobile devices have Internet access, you do not have to make this port available.

b. Enabling Mobile Device Management

You can enable Mobile Device Management (see section "Enabling Mobile Device Management" on page [730](#)) when you are running the Administration Server Quick Start Wizard or later.

c. Specifying the external address of the Administration Server

You can specify the external address when you run the Administration Server Quick Start Wizard or later. If you did not select Mobile Device Management for installation and did not specify the address in the installation wizard, specify the external address in the installation package properties.

d. Adding mobile devices to the Managed devices group

Add the mobile devices to the Managed devices group so that you can manage these devices through policies. You can create a moving rule in one of the steps of the Administration Server Quick Start Wizard. You can also create the moving rule later. If you do not create such a rule, you can add mobile devices to the Managed devices group manually.

You can add mobile devices to the Managed devices group directly, or you can create a subgroup (or multiple subgroups) for them.

At any time afterward, you can connect any new mobile device to the Administration Server using the New Mobile Device Connection Wizard (see section "Adding iOS mobile devices to the list of managed devices" on page [744](#)).

e. Creating a policy for mobile devices

To manage mobile devices, create a policy (or multiple policies) for them in the corresponding group(s). You can change the settings of this policy at any time afterward.

Results

Upon completion of the scenario, you can manage Android and iOS devices using Kaspersky Security Center.

About group policy for managing EAS and iOS MDM devices

To manage iOS MDM and EAS devices, you can use the Kaspersky Device Management for iOS management plug-in, which is included in the Kaspersky Security Center distribution kit. Kaspersky Device Management for iOS allows you to create group policies for specifying the configuration settings of iOS MDM and EAS devices without using iPhone® Configuration Utility and the management profile of Exchange ActiveSync.

A group policy for managing EAS and iOS MDM devices provides the administrator with the following options:

- For managing EAS devices:
 - Configuring the device-unlocking password.
 - Configuring data storage on the device in encrypted form.
 - Configuring synchronization of corporate mail.
 - Configuring the hardware features of mobile devices, such as the use of removable drives, the camera, or Bluetooth.
 - Configuring restrictions on use of mobile applications on the device.
- For managing iOS MDM devices:
 - Configuring device password security settings.
 - Configuring restrictions on usage of hardware features of the device and restrictions on installation and removal of mobile apps.
 - Configuring restrictions on the use of pre-installed mobile apps, such as YouTube™, iTunes® Store, or Safari.
 - Configuring restrictions on media content (such as movies and TV shows) viewed, by the region where the device is located.
 - Configuring device connection to the Internet through the proxy server (Global HTTP proxy).
 - Configuring the account with which the user can access corporate apps and services (Single Sign On (SSO) technology).
 - Monitoring Internet usage (visits to websites) on mobile devices.

- Configuring wireless networks (Wi-Fi), access points (APNs), and virtual private networks (VPNs) that use different authentication mechanisms and network protocols.
- Configuring settings of the connection to AirPlay® devices for streaming photos, music, and videos.
- Configuring settings of the connection to AirPrint™ printers for wireless printing of documents from the device.
- Configuring synchronization with the Microsoft Exchange server and user accounts for using corporate email on devices.
- Configuring user credentials for synchronization with the LDAP directory service.
- Configuring user credentials for connecting to CalDAV and CardDAV services that give users access to corporate calendars and contact lists.
- Configuring settings of the iOS interface, such as fonts or icons for favorite websites, on the user's device.
- Adding new security certificates on devices.
- Configuring the Simple Certificate Enrollment Protocol (SCEP) server for automatic retrieval of certificates by the device from the Certification Authority.
- Adding custom settings for working with mobile apps.

A policy for managing EAS and iOS MDM devices is special in that it is assigned to an administration group that includes iOS MDM Server and Exchange ActiveSync Mobile Devices Server (referred to collectively as "Mobile Device Servers"). All settings specified in this policy are first applied to Mobile Device Servers and then to mobile devices managed by such servers. In the case of a hierarchical structure of administration groups, secondary Mobile Device Servers receive the policy settings from primary Mobile Device Servers and distribute them to mobile devices.

For more details on how to use the group policy for managing EAS and iOS MDM devices in Kaspersky Security Center Administration Console, please refer to the *Kaspersky Security for Mobile* documentation.

Enabling Mobile Device Management

To manage mobile devices, you must enable Mobile Device Management. If you did not enable this feature in the Quick Start Wizard (see section "Administration Server Quick Start Wizard" on page [265](#)), you can enable it later. Mobile Device Management requires a license (see section "Kaspersky Security Center licensing options" on page [320](#)).

Enabling Mobile Device Management is only available on the primary Administration Server.

► To enable Mobile Device Management:

1. In the console tree, select the **Mobile Device Management** folder.
2. In the workspace of the folder, click the **Enable Mobile Device Management** button. This button is only available if you have not enabled **Mobile Device Management** before.

The **Additional components** page of the Administration Server Quick Start Wizard is displayed.

3. Select **Enable Mobile Device Management** in order to manage mobile devices.

4. On the **Select application activation method** page, activate the application by using a key file or activation code (see section "Step 3. Selecting the application activation method" on page [267](#)).

Management of mobile devices will not be possible until you activate the Mobile Device Management feature.

5. On the **Proxy server settings to gain access to the Internet** page, select the **Use proxy server** check box if you want to use a proxy server when connecting to the Internet. When this check box is selected, the fields become available for entering settings. Specify the settings for proxy server connection (see section "Step 2. Configuring a proxy server" on page [266](#)).
6. On the **Check for updates for plug-ins and installation packages** page, select one of the following options:

- **Check whether plug-ins and installation packages are up to date**

Starting the check of up-to-date status. If the check detects outdated versions of some plug-ins or installation packages, the Wizard prompts you to download up-to-date versions to replace the outdated ones.

- **Skip check**

Continuing work without checking whether plug-ins and installation packages are up-to-date. You can select this option if, for example, you have no Internet access or if you want to proceed with the outdated version of the application for some reason.

Skipping the check of updates for plug-ins may result in improper functioning of the application.

7. On the **Latest plug-in versions available** page, download and install the latest versions of plug-ins in the language that your application version requires. Updating the plug-ins does not require a license.

After you install the plug-ins and packages, the application checks whether all plug-ins required for proper functioning of mobile devices have been installed. If outdated versions of some plug-ins are detected, the Wizard prompts you to download up-to-date versions to replace the outdated ones.

8. On the **Mobile device connection settings** page, set up the Administration Server ports (see section "Step 10. Connecting mobile devices" on page [272](#)).

When the Wizard completes, the following changes will be made:

- The Kaspersky Endpoint Security for Android policy will be created.
- The Kaspersky Device Management for iOS policy will be created.
- Ports will be opened on the Administration Server for mobile devices.

See also:

Scenario: Mobile Device Management deployment [728](#)

Modifying the Mobile Device Management settings

► To enable support of mobile devices:

1. In the console tree, select the **Mobile Device Management** folder.
2. In the workspace of the folder, click the **Connection ports for mobile devices** link.

The **Additional ports** section of the Administration Server properties window is displayed.

3. In the **Additional ports** section, modify the relevant settings:

- **SSL port for the activation proxy server**

The number of an SSL port for connection of Kaspersky Endpoint Security for Windows to activation servers of Kaspersky.

The default port number is 17000.

- **Open port for mobile devices**

A port opens for mobile devices to connect to the Licensing Server. You can define the port number and other settings in the fields below.

By default, this option is enabled.

- **Port for mobile device synchronization**

Number of the port through which mobile devices connect to the Administration Server and exchange data with it. The default port number is 13292.

You can assign a different port if port 13292 is being used for other purposes.

- **Port for mobile device activation**

The port for connection of Kaspersky Endpoint Security for Android to activation servers of Kaspersky.

The default port number is 17100.

4. Click **OK**.

Disabling Mobile Device Management

Disabling Mobile Device Management is only available on the primary Administration Server.

► *To disable Mobile Device Management:*

1. In the console tree, select the **Mobile Device Management** folder.

2. In the workspace of this folder, click the **Configure additional components** link.

The **Additional components** page of the Administration Server Quick Start Wizard is displayed.

3. Select **Do not enable Mobile Device Management** if you do not want to manage mobile devices any longer.

4. Click **OK**.

Previously connected mobile devices will not be able to connect to Administration Server. The port for mobile device connection and the port for mobile device activation will be closed automatically.

Policies that were created for Kaspersky Endpoint Security for Android and Kaspersky Device Management for iOS will not be deleted. The certificate issuance rules will not be modified. The plug-ins that have been installed will not be removed. The moving rule for mobile devices will not be deleted.

After you re-enable Mobile Device Management on managed mobile devices, you may have to reinstall mobile apps that are required for mobile device management.

Working with commands for mobile devices

This section contains information about commands for managing mobile devices supported by the application. The section provides instructions on how to send commands to mobile devices, as well as how to view the execution statuses of commands in the command log.

In this section

Commands for mobile device management	733
Using Google Firebase Cloud Messaging	735
Sending commands	736
Viewing the statuses of commands in the command log	736

Commands for mobile device management

Kaspersky Security Center supports commands for mobile device management.

Such commands are used for remote mobile device management. For example, if your mobile device is lost, you can delete corporate data from the device by using a command.

You can use commands for the following types of managed mobile devices:

- iOS MDM devices
- Kaspersky Endpoint Security (KES) devices
- EAS devices

Each device type supports a dedicated set of commands.

Special considerations for certain commands

- For all types of devices, if the **Reset to factory settings** command is successfully executed, all data is deleted from the device, and the device settings are rolled back to their factory values.
- After successful execution of the **Wipe corporate data** command on an iOS MDM device, all installed configuration profiles, provisioning profiles, the iOS MDM profile, and applications for which the **Remove together with iOS MDM profile** check box has been selected are removed from the device.
- If the **Wipe corporate data** command is successfully executed on a KES device, all corporate data, entries in Contacts, the SMS history, the call log, the calendar, the Internet connection settings, and the user accounts, except for the Google™ account, will be deleted from the device. For a KES device, all data from the memory card will also be deleted.
- Before sending the **Locate** command to a KES device, you will have to confirm that you are using this command for an authorized search for a lost device that belongs to your organization or to one of your employees. When using Kaspersky Security Center Service Pack 2 Maintenance Release 1 or earlier

versions, a mobile device that receives the **Locate** command is locked. Starting from Kaspersky Security Center 10 Service Pack 3, the device is not locked.

List of commands for mobile devices

The following table shows sets of commands for iOS MDM devices.

Table 65. Supported commands for mobile device management: iOS MDM devices

Commands	Command execution result
Lock	The mobile device is locked.
Unlock	Mobile device locking with a PIN is disabled. The previously specified PIN has been reset.
Reset to factory settings	All data is deleted from the mobile device and the settings are rolled back to their default values.
Wipe corporate data	All installed configuration profiles, provisioning profiles, the iOS MDM profile, and applications for which the Remove together with iOS MDM profile check box has been selected are removed from the device.
Synchronize device	The mobile device data is synchronized with the Administration Server.
Install profile	The configuration profile is installed on the mobile device.
Remove profile	The configuration profile is deleted from the mobile device.
Install provisioning profile	The provisioning profile is installed on the mobile device.
Remove provisioning profile	The provisioning profile is deleted from the mobile device.
Install app	The app is installed on the mobile device.
Remove app	The app is removed from the mobile device.
Enter redemption code	Redemption code entered for a paid app.
Configure roaming	Data roaming and voice roaming enabled or disabled.

The following table shows sets of commands for KES devices.

Table 66. Supported commands for mobile device management: KES devices

Command	Command execution result
Lock	The mobile device is locked.
Unlock	Mobile device locking with a PIN is disabled. The previously specified PIN has been reset.
Reset to factory settings	All data is deleted from the mobile device and the settings are rolled back to their default values.
Wipe corporate data	Corporate data, entries in Contacts, the SMS history, the call log, the calendar, the Internet connection settings, and the user accounts (except for the Google account) have been deleted. Memory card data has been wiped.
Synchronize device	The mobile device data is synchronized with the Administration Server.
Locate device	The mobile device is located and shown on Google Maps™. The mobile carrier charges a fee for sending SMS messages and for providing Internet connectivity.
Mugshot	The mobile device is locked. The photo has been taken by the front camera of the device and saved on Administration Server. Photos can be viewed in the command log. The mobile carrier charges a fee for sending SMS messages and for providing Internet connectivity.
Alarm	The mobile device sounds an alarm.

The following table shows the commands for EAS devices.

Table 67. Supported commands for mobile device management: EAS devices

Commands	Command execution result
Reset to factory settings	All data is deleted from the mobile device and the settings are rolled back to their default values.

Using Google Firebase Cloud Messaging

To ensure timely delivery of commands to KES devices managed by the Android operating system, Kaspersky Security Center uses the mechanism of push notifications. Push notifications are exchanged between KES devices and Administration Server through Google Firebase Cloud Messaging. In Kaspersky Security Center Administration Console, you can specify the Google Firebase Cloud Messaging settings to connect KES devices to the service.

To retrieve the settings of Google Firebase Cloud Messaging, you must have a Google account.

► To configure Google Firebase Cloud Messaging:

1. In the **Mobile Device Management** folder in the console tree, select the **Mobile devices** subfolder.
2. In the context menu of the **Mobile devices** folder, select **Properties**.

This opens the properties window of the **Mobile devices** folder.

3. Select the **Google Firebase Cloud Messaging settings** section.
4. In the **Sender ID** field, specify the number of a Google API project that you have received when creating one in the Google Developer Console.
5. In the **Server key** field, enter a common server key that you have created in the Google Developer Console.

At the next synchronization with Administration Server, KES devices managed by Android operating systems will be connected to Google Firebase Cloud Messaging.

You can edit the Google Firebase Cloud Messaging settings by clicking the **Reset settings** button.

Sending commands

► *To send a command to the user's mobile device:*

1. In the **Mobile Device Management** folder in the console tree, select the **Mobile devices** subfolder.

The folder workspace displays a list of managed mobile devices.

2. Select the user's mobile device to which you need to send a command.
3. In the context menu of the mobile device, select **Show command log**.
4. In the **Mobile device management commands** window, proceed to the section with the name of the command that you need to send to the mobile device, then click the **Send command** button.

Depending on the command that you have selected, clicking the **Send command** button may open the window of advanced settings of the application. For example, when you send the command for deleting a provisioning profile from a mobile device, the application prompts you to select the provisioning profile that must be deleted from the mobile device. Define the advanced settings of the command in that window and confirm your selection. After that, the command will be sent to the mobile device.

You can click the **Resend** button to send the command to the user's mobile device again.

You can click the **Remove from queue** button to cancel execution of a command that was sent if the command has not yet been executed.

The **Command log** section displays commands that have been sent to the mobile device, with the respective execution statuses. Click **Refresh** to update the list of commands.

5. Click **OK** to close the **Mobile device management commands** window.

Viewing the statuses of commands in the command log

The application saves to the command log information about all commands that have been sent to mobile devices. The command log contains information about the time and date that each command was sent to the mobile device, their respective statuses, and detailed descriptions of command execution results. For example, in case execution of a command is unsuccessful, the log displays the cause of the error. Records are stored in the command log for 30 days maximum.

Commands sent to mobile devices can have the following statuses:

- *Running*—The command has been sent to the mobile device.
- *Completed*—The command execution has successfully completed.
- *Completed with error*—The command execution has failed.

- *Deleting*—The command is being removed from the queue of commands sent to the mobile device.
- *Deleted*—The command has been successfully removed from the queue of commands sent to the mobile device.
- *Error deleting*—The command could not be removed from the queue of commands sent to the mobile device.

The application maintains a command log for each mobile device.

► *To view the log of commands sent to a mobile device:*

1. In the **Mobile Device Management** folder in the console tree, select the **Mobile devices** subfolder.

The folder workspace displays a list of managed mobile devices.

2. In the list of mobile devices, select the one for which you want to view the command log.
3. In the context menu of the mobile device, select **Show command log**.

The **Mobile device management commands** window opens. The sections of the **Mobile device management commands** window correspond to the commands that can be sent to the mobile device.

4. Select sections containing the necessary commands and view information about how the commands are sent and executed in the **Command log** section.

In the **Command log** section, you can view the list of commands that have been sent to the mobile device and details about those commands. The **Show commands** filter allows you to display in the list only commands with the selected status.

Working with certificates

This section contains information about how to work with certificates of mobile devices. The section contains instructions on how to install certificates on users' mobile devices and how to configure certificate issuance rules. The section also contains instructions on how to integrate the application with the public keys infrastructure and how to configure the support of Kerberos.

In this section

Installing a certificate	738
Step 1. Certificate type	738
Step 2. Device type.....	739
Step 3. Selecting a user.....	739
Step 4. Certificate source	739
Step 5. Certificate tag	739
Step 6. Certificate publishing settings	740
Step 7. User notification method	741
Step 8. Generating the certificate	742
Configuring certificate issuance rules.....	742
Integration with public key infrastructure	743
Enabling support of Kerberos Constrained Delegation	744

Installing a certificate

You can install the following types of certificates on a user's mobile device:

- Shared certificates for identifying the mobile device.
- Mail certificates for configuring the corporate mail on the mobile device.
- VPN certificate for configuring access to a virtual private network on the mobile device.

► *To install a certificate on a user's mobile device:*

1. In the console tree, expand the **Mobile Device Management** folder and select the **Certificates** subfolder.
2. In the workspace of the **Certificates** folder, click the **Add certificate** link to run the Certificate Installation Wizard.

Follow the instructions of the Wizard.

After the Wizard finishes, a certificate will be created and added to the list of the user's certificates; in addition, a notification will be sent to the user, providing the user with a link for downloading and installing the certificate on the mobile device. You can view the list of all certificates and export it to a file (see section "Viewing the list of certificates issued to a user" on page [711](#)). You can delete and reissue certificates, as well as view their properties.

Step 1. Certificate type

Specify the type of certificate that must be installed on the user's mobile device:

- **Mobile certificate**—for identifying the mobile device.
- **Mail certificate**—for configuring the corporate mail on the mobile device.
- **VPN certificate**—for configuring access to a virtual private network on the mobile device.

Step 2. Device type

This window is displayed only if you selected (see section "Step 1. Certificate type" on page [738](#)) **Mail certificate** or **VPN certificate** as the certificate type.

Specify the type of the operating system on the device:

- **iOS MDM device.** Select this option if you have to install a certificate on a mobile device that is connected to the iOS MDM Server by using iOS MDM protocol.
- **KES device managed by Kaspersky Security for Mobile.** Select this option if you have to install a certificate on a KES device. In this case, the certificate will be used for user identification upon every connection to the Administration Server.
- **KES device connected to Administration Server without user certificate authentication.** Select this option if you have to install a certificate on a KES device using no certificate authentication. In this case, at the final step of the Wizard, in the **User notification method** window the administrator must select the user authentication type used at every connection to the Administration Server.

Step 3. Selecting a user

In the list, select users, user groups, or Active Directory user groups for which you have to install the certificate.

In the **User selection** window, you can search for Kaspersky Security Center internal users. You can click **Add** to add an internal user.

Step 4. Certificate source

In this window, you can select the certificate source that Administration Server will use to identify the mobile device. You can specify a certificate using one of the following methods:

- Create a certificate automatically, by means of Administration Server tools, then deliver the certificate to the device.
- Specify a certificate file that was created earlier. This method is not available if multiple users were selected at the previous step.

Select the **Publish certificate** check box if you have to send to a user a notification about creation of a certificate for his or her mobile device.

If the user's mobile device has already been previously authenticated using a certificate so there is no need to specify an account name and password to receive a new certificate, clear the **Publish certificate** check box. In this case, the **User notification method** window will not be displayed.

Step 5. Certificate tag

The **Certificate tag** window is displayed if **iOS MDM device** has been selected in the **Device type**.

In the drop-down list, you can assign a tag to the certificate of the user's iOS MDM device. The certificate with the assigned tag may have specific parameters set for this tag in the Kaspersky Device Management for iOS policy properties.

The drop-down list prompts you to select the *Certificate template 1*, *Certificate template 2*, or *Certificate template 3* tag. You can configure the tags in the following sections:

- If **Mail certificate** has been selected in the **Certificate type** window, the tags for it can be configured in the properties of the Exchange ActiveSync account for mobile devices (**Managed devices** → **Policies** → Kaspersky Device Management for iOS policy properties > **Exchange ActiveSync** section → **Add** → **Advanced**).
- If **VPN certificate** has been selected in the **Certificate type** window, the tags for it can be configured in the properties of the VPN for mobile devices (**Managed devices** → **Policies** → Kaspersky Device Management for iOS policy properties → **VPN** section → **Add** → **Advanced**). You cannot configure the tags used for VPN certificates if the L2TP, PPTP, or IPSec (Cisco™) connection type is selected for your VPN.

See also:

Installing a certificate for a user [711](#)

Step 6. Certificate publishing settings

In this window, you can specify the following certificate publishing settings:

- **Do not notify the user about a new certificate**

Enable this option if you do not want to send a user a notification about creation of a certificate for the user's mobile device. In this case, the **User notification method** window will not be displayed.

This option is only applicable to devices with Kaspersky Endpoint Security for Android installed.

You might want to enable this option, for example, if the user's mobile device has already been previously authenticated by means of a certificate so there is no need to specify an account name and password to receive a new certificate.

- **Allow the device to have multiple receipts of a single certificate (only for devices with Kaspersky Endpoint Security for Android installed)**

Enable this option if you want Kaspersky Security Center to automatically resend the certificate every time it is soon to expire or when it is not found on the target device.

The certificate is automatically resent several days before the certificate expiration date. You can set the number of days in the Certificate issuance rules (see section "Configuring certificate issuance rules" on page [742](#)) window.

In some cases, the certificate cannot be found on the device. For example, this can happen when the user reinstalls the Kaspersky security application on the device or resets the device settings and data to factory defaults. In this case Kaspersky Security Center checks the device ID at the next attempt of the device to connect to the Administration Server. If the device has the same ID as it had when the certificate was issued, the application resends the certificate to the device.

Step 7. User notification method

This window is not displayed if you selected (see section "Step 2. Device type" on page 739) **iOS MDM device** as the device type or if you selected (see section "Step 6. Certificate publishing settings" on page 740) the **Do not notify the user about a new certificate** option.

In the **User notification method** window, you can configure the user notification about certificate installation on the mobile device.

In the **Authentication method** field, specify the user authentication type:

- **Credentials (domain or alias)**

In this case, the user employs the domain password or the password of a Kaspersky Security Center internal user to receive a new certificate.

- **One-time password**

In this case, the user receives a one-time password that will be sent by email or by SMS. This password must be entered to receive a new certificate.

This option changes to **Password** if you enabled (selected) the **Allow the device multiple receipts of a single certificate (only for devices with Kaspersky security applications for mobile devices installed)** option in the **Certificate publishing settings** window.

- **Password**

In this case, the password is used every time the certificate is sent to the user.

This option changes to **One-time password**, if you disabled (cleared) the **Allow the device multiple receipts of a single certificate (only for devices with Kaspersky security applications for mobile devices installed)** option in the **Certificate publishing settings** window.

This field is displayed if you selected **Mobile certificate** in the **Certificate type** window or if you selected **KES device connected to Administration Server without user certificate authentication** as the device type.

Select the user notification option:

- **Show authentication password after the Wizard finishes**

If you select this option, the user name, user name in Security Account Manager (SAM), and password for certificate retrieval for each of the selected users will be displayed at the final step of the Certificate Installation Wizard. Configuration of user notification about an installed certificate will be unavailable.

When you add certificates for multiple users, you can save the provided credentials to a file by clicking the **Export** button at the last step of the Certificate Installation Wizard.

This option is unavailable if you selected **Credentials (domain or alias)** at the **User notification method** step of the Certificate Installation Wizard.

- **Notify user of new certificate**

If you select this option, you can configure user notification about a new certificate.

- **By email**

In this group of settings, you can configure user notification about installation of a new certificate on his or her mobile device using email messages. This notification method is only available if the SMTP Server (see section "Step 8. Configuring email notifications" on page [271](#)) is enabled.

Click the **Edit message** link to view and edit the notification message, if necessary.

- **By SMS**

In this group of settings, you can configure the user notification about using SMS to install a certificate on mobile devices. This notification method is only available if SMS notification is enabled.

Click the **Edit message** link to view and edit the notification message, if necessary.

See also:

| [Installing a certificate for a user](#) **7**

Step 8. Generating the certificate

At this step, the certificate is created.

You can click **Finish** to exit the wizard.

The certificate is generated and displayed in the list of certificates in the workspace of the **Certificates** folder.

Configuring certificate issuance rules

The certificates are used for the device authentication on the Administration Server. All managed mobile devices must have certificates. You can configure how the certificates are issued.

► *To configure certificate issuance rules:*

1. In the console tree, expand the **Mobile Device Management** folder and select the **Certificates** subfolder.
2. In the workspace of the **Certificates** folder, click the **Configure certificate issuance rules** button to open the **Certificate issuance rules** window.
3. Proceed to the section with the name of a certificate type:

Issuance of mobile certificates—To configure the issuance of certificates for the mobile devices.

Issuance of mail certificates—To configure the issuance of mail certificates.

Issuance of VPN certificates—To configure the issuance of VPN certificates.

4. In the **Issuance settings** section, configure the issuance of the certificate:
 - Specify the certificate term in days.
 - Select a certificate source (**Administration Server** or **Certificates are specified manually**).
Administration Server is selected as the default source of certificates.
 - Specify a certificate template (**Default template**, **Other template**).

Configuration of templates is available if the **Integration with PKI** section features the integration with Public Key Infrastructure (on page [743](#)) enabled.

5. In the **Automatic Updates settings** section, configure automatic updates of the certificate:
 - In the **Renew when certificate is to expire in (days)** field, specify how many days before expiration the certificate must be renewed.
 - To enable automatic updates of certificates, select the **Reissue certificate automatically if possible** check box.

A mobile certificate can be renewed manually only.

6. In the **Password protection** section, enable and configure the use of a password when decrypting certificates.

Password protection is only available for mobile certificates.

- a. Select the **Prompt for password during certificate installation** check box.
 - b. Use the slider to define the maximum number of symbols in the password for encryption.
7. Click **OK**.

Integration with public key infrastructure

Integration of the application with the public key infrastructure (PKI) is required to simplify the issuance of domain certificates to users. Following integration, certificates are issued automatically.

The minimum supported PKI server version is Windows Server 2008.

You have to configure the account for integration with PKI. The account must meet the following requirements:

- Be a domain user and administrator on a device that has Administration Server installed.
- Be granted the SeServiceLogonRight privilege on the device with Administration Server installed.

To create a permanent user profile, log on at least once under the configured user account on the device with Administration Server installed. In this user's certificate repository on the Administration Server device, install the Enrollment Agent certificate provided by domain administrators.

► *To configure integration with the public keys infrastructure:*

1. In the console tree, expand the **Mobile Device Management** folder and select the **Certificates** subfolder.
2. In the workspace, click the **Integrate with public key infrastructure** button to open the **Integration with PKI** section of the **Certificate issuance rules** window.

The **Integration with PKI** section of the **Certificate issuance rules** window opens.

3. Select the **Integrate issuance of certificates with PKI** check box.
4. In the **Account** field, specify the name of the user account to be used for integration with the public key infrastructure.
5. In the **Password** field, enter the domain password for the account.

6. In the **Certificate template name in PKI system** list, select the certificate template that will be used for the issuance of certificates to domain users.

A dedicated service is run in Kaspersky Security Center under the specified user account. This service is responsible for issuing users' domain certificates. The service is run when the list of certificate templates is loaded by clicking the **Refresh list** button or when a certificate is generated.

7. Click **OK** to save the settings.

Following integration, certificates are issued automatically.

Enabling support of Kerberos Constrained Delegation

The application supports usage of Kerberos Constrained Delegation.

► *To enable support of Kerberos Constrained Delegation:*

1. In the console tree, open the **Mobile Device Management** folder.
2. In the **Mobile Device Management** folder in the console tree, select the **Mobile Device Servers** subfolder.
3. In the workspace of the **Mobile Device Servers** folder, select an iOS MDM Server.
4. In the context menu of the iOS MDM Server, select **Properties**.
5. In the properties window of the iOS MDM Server, select the **Settings** section.
6. In the **Settings** section, select the **Ensure compatibility with Kerberos constrained delegation** check box.
7. Click **OK**.

Adding iOS mobile devices to the list of managed devices

To add an iOS mobile device to the list of managed devices, a shared certificate must be delivered and installed on the device (see section "Working with certificates" on page [737](#)). Shared certificates are used by Administration Server for identifying mobile devices. A shared certificate for an iOS mobile device is delivered within an iOS MDM profile. After a shared certificate is delivered and installed on a mobile device, the device appears in the list of managed devices.

Kaspersky no longer supports Kaspersky Safe Browser.

You can add mobile devices of users to the list of managed devices by means of the New Mobile Device Connection Wizard.

► *To connect an iOS device to the Administration Server by using a shared certificate:*

1. Start the New Mobile Device Connection Wizard in one of the following ways:
 - Use the context menu in the **User accounts** folder:
 1. In the console tree, expand the **Advanced** folder and select the **User accounts** subfolder.
 1. In the workspace of the **User accounts** folder, select the users, user groups, or Active Directory user groups whose mobile devices you want to add to the list of managed devices.
 2. Right-click and in the context menu of the user account, select **Add mobile device**.

The New Mobile Device Connection Wizard starts.

- In the workspace of the **Mobile devices** folder click the **Add mobile device** button:
 1. In the console tree, expand the **Mobile Device Management** folder and select the **Mobile devices** subfolder.
 2. In the workspace of the **Mobile devices** subfolder, click the **Add mobile device** button.

The New Mobile Device Connection Wizard starts.

2. On the **Operating system** page of the Wizard, select **iOS** as the mobile device operating system type.
3. On the **Selecting iOS MDM Server** page, select the iOS MDM Server.
4. On the **Select users whose mobile devices you want to manage** page, select the users, user groups, or Active Directory user groups whose mobile devices you want to add to the list of managed devices.

This step is skipped if you start the Wizard by selecting **Add mobile device** in the context menu of the **User accounts** folder.

If you want to add a new user account into the list, click the **Add** button and enter the user account properties in the window that opens. If you want to modify or review the user account properties, select the user account from the list and click the **Properties** button.

5. On the **Certificate source** page of the Wizard, specify the method for creating the shared certificate that Administration Server will use to identify the mobile device. You can specify a shared certificate in one of the following ways:
 - **Issue certificate through Administration Server tools**

Select this option to create a new certificate by means of Administration Server tools if you did not create it previously.

If this option is selected, the iOS MDM profile will be automatically signed with a certificate generated by Administration Server.

This option is selected by default.
 - **Specify certificate file**

Select this option to specify a certificate file that was created earlier.

This method is not available if multiple users were selected at the previous step.
6. On the **User notification method** page of the Wizard, define the settings for notifying the mobile device user by SMS or email about certificate creation:
 - **Show link in Wizard**

If you select this option, a link to the installation package will be shown at the final step of the New Device Connection Wizard.

This option is not available if multiple users were selected for the device connection.

- **Send link to user**

Selecting this option allows you to configure user notification of connection of a new mobile device.

You can select the email address type, specify an additional email address, and edit the message text. You can also select the type of the user phone for sending an SMS message, specify an additional phone number, and edit the SMS message text.

If the SMTP Server has not been configured, no email messages can be sent to users. If SMS notification has not been configured, no SMS messages can be sent to users.

1. On the **Result** page, click **Finish** to close the Wizard.

The iOS MDM profile is automatically published on the Kaspersky Security Center Web Server. The mobile device user receives a notification with a link for downloading the iOS MDM profile from the Web Server. The user clicks the link. Next, the mobile device's operating system prompts the user to accept the iOS MDM profile installation. The user must agree to install the iOS MDM profile before the iOS MDM profile can be downloaded to the mobile device. After the iOS MDM profile is downloaded and the mobile device is synchronized with the Administration Server, the device is displayed in the **Mobile devices** folder, which is a subfolder of the **Mobile Device Management** folder in the console tree.

For the user to proceed to the Kaspersky Security Center Web Server by using the link, connection with the Administration Server over port 8061 must be available on the mobile device.

See also:

Scenario: Mobile Device Management deployment.....[728](#)

Adding Android mobile devices to the list of managed devices

To add an Android mobile device to the list of managed devices, Kaspersky Endpoint Security for Android and a shared certificate (see section "Working with certificates" on page [737](#)) must be delivered and installed on the mobile device. Shared certificates are used by Administration Server for identifying mobile devices. After a shared certificate is delivered and installed on a mobile device, the device appears in the list of managed devices.

You can add mobile devices of users to the list of managed devices by means of the New Mobile Device Connection Wizard. The New Mobile Device Connection Wizard provides two options for delivery and installation of a shared certificate and Kaspersky Endpoint Security for Android:

- By using a Google Play link.
- By using a link from Kaspersky Security Center Web Server.

The Kaspersky Endpoint Security for Android installation package stored for distribution on Administration Server is used for installation.

Starting the New Mobile Device Connection Wizard

► *To start the New Mobile Device Connection Wizard, do one of the following:*

- Use the context menu in the **User accounts** folder:
 1. In the console tree, expand the **Advanced** folder and select the **User accounts** subfolder.
 1. In the workspace of the **User accounts** folder, select the users, user groups, or Active Directory user groups whose mobile devices you want to add to the list of managed devices.
 2. Right-click and in the context menu of the user account, select **Add mobile device**.

The New Mobile Device Connection Wizard starts.

- In the workspace of the **Mobile devices** folder click the **Add mobile device** button:
 1. In the console tree, expand the **Mobile Device Management** folder and select the **Mobile devices** subfolder.
 2. In the workspace of the **Mobile devices** subfolder, click the **Add mobile device** button.

The New Mobile Device Connection Wizard starts.

Adding an Android mobile device by using a Google Play link

► *To install Kaspersky Endpoint Security for Android and a shared certificate on a mobile device using a Google Play link:*

1. Start the New Mobile Device Connection Wizard.
2. On the **Operating system** page of the Wizard, select **Android** as the mobile device operating system type.
3. On the **Kaspersky Endpoint Security for Android installation method** page of the Wizard, select **By using a Google Play link**.
4. On the **Select users whose mobile devices you want to manage** page of the Wizard, select the users, user groups, or Active Directory user groups whose mobile devices you want to add to the list of managed devices.

This step is skipped if the Wizard is started by selecting **Add mobile device** in the context menu of **User accounts** folder.

If you want to add a new user account into the list, click the **Add** button and enter the user account properties in the window that opens. If you want to modify or review the user account properties, select the user account in the list and click the **Properties** button.

5. On the **Certificate source** page of the Wizard, specify the method for creating the shared certificate that Administration Server will use to identify the mobile device. You can specify a shared certificate in one of the following ways:

Issue certificate through Administration Server tools

Select this option to create a new certificate by means of Administration Server tools if you did not create it previously.

If this option is selected, the certificate is automatically issued by using Administration Server tools.

This option is selected by default.

- **Specify certificate file**

Select this option to specify a certificate file that was created earlier.

This method is not available if multiple users were selected at the previous step.

6. On the **User notification method** page of the Wizard, define the settings for notifying the mobile device user by SMS or email about certificate creation:

- **Show link in Wizard**

If you select this option, a link to the installation package will be shown at the final step of the New Device Connection Wizard.

This option is not available if multiple users were selected for the device connection.

- **Send link to user**

Selecting this option allows you to configure user notification of connection of a new mobile device.

You can select the email address type, specify an additional email address, and edit the message text. You can also select the type of the user phone for sending an SMS message, specify an additional phone number, and edit the SMS message text.

If the SMTP Server has not been configured, no email messages can be sent to users. If SMS notification has not been configured, no SMS messages can be sent to users.

1. On the **Result** page, click **Finish** to close the Wizard.

After the Wizard finishes, a link and a QR code will be sent to the user's mobile device, allowing download of Kaspersky Endpoint Security for Android. The user clicks the link or scans the QR code. Next, the mobile device's operating system prompts the user to accept installation of Kaspersky Endpoint Security for Android installation. After Kaspersky Endpoint Security for Android is downloaded and installed, the mobile device connects to the Administration Server and downloads a shared certificate. After the certificate is installed on the mobile device, the device is displayed in the **Mobile devices** folder, which is a subfolder of the **Mobile Device Management** folder in the console tree.

Adding an Android mobile device using a link from Kaspersky Security Center Web Server

Kaspersky Endpoint Security for Android installation package published on the Administration Server is used for installation.

► *To install Kaspersky Endpoint Security for Android and a shared certificate on a mobile device using a link from Web Server:*

1. Start the New Mobile Device Connection Wizard.
2. On the **Operating system** page of the Wizard, select **Android** as the mobile device operating system type.
3. On the **Kaspersky Endpoint Security for Android installation method** page of the Wizard, select **By using a link from Web Server**.

In the field that appears below, select an installation package or create a new one by clicking **New**.

4. On the **Select users whose mobile devices you want to manage** page of the Wizard, select the users, user groups, or Active Directory user groups whose mobile devices you want to add to the list of managed devices.

This step is skipped if the Wizard is started by selecting **Add mobile device** in the context menu of **User accounts** folder.

If you want to add a new user account into the list, click the **Add** button and enter the user account properties in the window that opens. If you want to modify or review the user account properties, select the user account from the list and click the **Properties** button.

5. On the **Certificate source** page of the Wizard, specify the method for creating the shared certificate that Administration Server will use to identify the mobile device. You can specify a shared certificate in one of the following ways:

- **Issue certificate through Administration Server tools**

Select this option to create a new certificate by means of Administration Server tools if you did not create it previously.

If this option is selected, the certificate is automatically issued by using Administration Server tools.

This option is selected by default.

- **Specify certificate file**

Select this option to specify a certificate file that was created earlier.

This method is not available if multiple users were selected at the previous step.

6. On the **User notification method** page of the Wizard, define the settings for notifying the mobile device user by SMS or email about certificate creation:

- **Show link in Wizard**

If you select this option, a link to the installation package will be shown at the final step of the New Device Connection Wizard.

This option is not available if multiple users were selected for the device connection.

- **Send link to user**

Selecting this option allows you to configure user notification of connection of a new mobile device.

You can select the email address type, specify an additional email address, and edit the message text. You can also select the type of the user phone for sending an SMS message, specify an additional phone number, and edit the SMS message text.

If the SMTP Server has not been configured, no email messages can be sent to users. If SMS notification has not been configured, no SMS messages can be sent to users.

1. On the **Result** page, click **Finish** to close the Wizard.

The mobile app package of Kaspersky Endpoint Security for Android is automatically published on the Kaspersky Security Center Web Server. The mobile app package contains the app, the settings for connecting the mobile device to the Administration Server, and a certificate. The mobile device user will receive a notification containing a link for downloading the package from the Web Server. The user clicks the link. The operating system of the device then prompts the user to accept installation of the mobile app package. If the user agrees, the package will be downloaded to the mobile device. After the package is downloaded and the mobile device is synchronized with the Administration Server, the device is displayed in the **Mobile devices** folder, which is a subfolder of the **Mobile Device Management** folder in the console tree.

Managing Exchange ActiveSync mobile devices

This section describes advanced features for management of EAS devices through Kaspersky Security Center.

In addition to management of EAS devices by means of commands, the administrator can use the following

options:

- Create management profiles for EAS devices, assign them to users' mailboxes (on page [750](#)). *EAS device management profile* is a policy of Exchange ActiveSync that is used on a Microsoft Exchange server to manage EAS devices. In an EAS device management profile, you can configure the following groups of settings:
 - User password management settings
 - Mail synchronization settings
 - Restrictions on the use of the mobile device features
 - Restrictions on the use of mobile applications on the mobile device

Depending on the mobile device model, settings of a management profile can be applied partially. The status of an Exchange ActiveSync policy that has been applied can be viewed in the mobile device properties.

- View information about the settings of EAS device management (on page [753](#)). For example, in the mobile device properties, the administrator can view the time of the last synchronization with a Microsoft Exchange server, the EAS device ID, the Exchange ActiveSync policy name and its current status on the mobile device.
- Disconnect EAS devices from management if they are out of use (on page [753](#)).
- Define the settings of Active Directory polling by the Exchange Mobile Device Server, which allows updating the information about users' mailboxes and mobile devices.

In this section

Adding a management profile.....	750
Removing a management profile.....	751
Handling Exchange ActiveSync policies.....	752
Configuring the scan scope	752
Working with EAS devices.....	752
Viewing information about an EAS device	753
Disconnecting an EAS device from management	753
User's rights to manage Exchange ActiveSync mobile devices.....	753

Adding a management profile

To manage EAS devices, you can create EAS device management profiles and assign them to selected Microsoft Exchange mailboxes.

Only one EAS device management profile can be assigned to a Microsoft Exchange mailbox.

► *To add an EAS device management profile for a Microsoft Exchange mailbox:*

1. In the console tree, open the **Mobile Device Management** folder.
2. In the **Mobile Device Management** folder in the console tree, select the **Mobile Device Servers** subfolder.
3. In the workspace of the **Mobile Device Servers** folder, select an Exchange Mobile Device Server.
4. In the context menu of the Exchange Mobile Device Server, select **Properties**.
The Mobile Device Server properties window opens.
5. In the properties window of the **Exchange Mobile Device Server**, select the **Mailboxes** section.
6. Select a mailbox and click the **Assign profile** button.
The **Policy profiles** window opens.
7. In the **Policy profiles** window, click the **Add** button.
The **New profile** window opens.
8. Configure the profile on the tabs of the **New profile** window.
 - If you want to specify the profile name and the update interval, select the **General** tab.
 - If you want to configure the password of the mobile device user, select the **Password** tab.
 - If you want to configure synchronization with the Microsoft Exchange server, select the **Synchronization** tab.
 - If you want to configure restrictions on the mobile device features, select the **Feature Restrictions** tab.
 - If you want to configure restrictions on the use of mobile applications on the mobile device, select the **Application Restrictions** tab.
9. Click **OK**.

The new profile will be displayed in the list of profiles in the **Policy profiles** window.

If you want this profile to be automatically assigned to new mailboxes, as well as to mailboxes whose profiles have been deleted, select it in the list of profiles and click the **Set as default profile** button.

The default profile cannot be deleted. To delete the current default profile, you must assign the "default profile" attribute to a different profile.

10. In the **Policy profiles** window, click **OK**.

The management profile settings will be applied on the EAS device at the next synchronization of the device with the Exchange Mobile Device Server.

Removing a management profile

► *To remove an EAS device management profile for a Microsoft Exchange mailbox:*

1. In the console tree, open the **Mobile Device Management** folder.
2. In the **Mobile Device Management** folder in the console tree, select the **Mobile Device Servers** subfolder.
3. In the workspace of the **Mobile Device Servers** folder, select an Exchange Mobile Device Server.
4. In the context menu of the Exchange Mobile Device Server, select **Properties**.

The Mobile Device Server properties window opens.

5. In the properties window of the Exchange Mobile Device Server, select the **Mailboxes** section.
6. Select a mailbox and click the **Change profiles** button.

The **Policy profiles** window opens.

7. In the **Policy profiles** window, select the profile that you want to remove and click the red Delete button.

The selected profile will be removed from the list of management profiles. The current default profile will be applied to EAS devices managed by the profile that has been removed.

If you want to remove the current default profile, re-assign the "default profile" property to another profile, then remove the first one.

Handling Exchange ActiveSync policies

After you install Exchange Mobile Device Server, in the **Mailboxes** section of the Server properties window, you can view information about accounts of the Microsoft Exchange server that have been retrieved by polling the current domain or domain forest.

Also, in the Exchange Mobile Device Server properties window, you can use the following buttons:

- **Change profiles** allows you to open the **Policy profiles** window, which contains a list of policies retrieved from the Microsoft Exchange server. In this window, you can create, edit, or delete Exchange ActiveSync policies. The **Policy profiles** window is almost identical to the policy editing window in Exchange Management Console.
- **Assign profiles to mobile devices** allows you to assign a selected Exchange ActiveSync policy to one or several accounts.
- **Enable/disable ActiveSync** allows you to enable or disable Exchange ActiveSync HTTP for one or multiple accounts.

Configuring the scan scope

In the properties of the newly installed Exchange Mobile Device Server, in the **Settings** section, you can configure the scan scope. By default, the scan scope is the current domain in which the Exchange Mobile Device Server is installed. Selecting the **Entire domain forest** value expands the scan scope to include the entire domain forest.

Working with EAS devices

Devices retrieved by scanning the Microsoft Exchange server will be added to the common list of devices, which is located in the **Mobile Device Management** node, in the **Mobile devices** folder.

If you want the **Mobile devices** folder to display Exchange ActiveSync devices only (hereinafter referred to as EAS devices), filter the device list by clicking the **Exchange ActiveSync (EAS)** link that is located above this list.

You can manage EAS devices by means of commands. For example, the **Reset to factory settings** command allows you to remove all data from a device and reset the device settings to the factory settings. This command is useful if the device is lost or stolen, when you need to prevent corporate or personal data from falling into the hands of a third party.

If all data has been deleted from the device, it will be deleted again the next time the device connects to the Microsoft Exchange Server. The command will be reiterated until the device is removed from the list of devices. This behavior is caused by the operation principles of the Microsoft Exchange server.

To remove an EAS device from the list, in the context menu of the device, select **Delete**. If the Exchange ActiveSync account is not deleted from the EAS device, the latter will reappear on the list of devices after the next synchronization of the device with the Microsoft Exchange server.

Viewing information about an EAS device

► *To view information about an EAS device:*

1. In the **Mobile Device Management** folder in the console tree, select the **Mobile devices** subfolder.
The folder workspace displays a list of managed mobile devices.
2. In the workspace, filter EAS devices by clicking the **Exchange ActiveSync (EAS)** link.
3. From the context menu of the mobile device select **Properties**.
The properties window of the EAS device opens.

The properties window of the mobile device displays information about the connected EAS device.

Disconnecting an EAS device from management

► *To disconnect an EAS device from management by the Exchange Mobile Device Server:*

1. In the **Mobile Device Management** folder in the console tree, select the **Mobile devices** subfolder.
The folder workspace displays a list of managed mobile devices.
2. In the workspace, filter EAS devices by clicking the **Exchange ActiveSync (EAS)** link.
3. Select the mobile device that you want to disconnect from management by the Exchange Mobile Device Server.
4. In the context menu of the mobile device, select **Delete**.

The EAS device is marked for removal with a red cross icon. The mobile device is removed from the list of managed devices after it is removed from the Exchange ActiveSync Server database. To do so, the administrator must remove the user account on the Microsoft Exchange server.

User's rights to manage Exchange ActiveSync mobile devices

To manage mobile devices running under the Exchange ActiveSync protocol with Microsoft Exchange Server 2010 or Microsoft Exchange Server 2013, make sure that the user is included in a role group for which the following commandlets are allowed to execute:

- Get-CASMailbox
- Set-CASMailbox
- Remove-ActiveSyncDevice

- Clear-ActiveSyncDevice
- Get-ActiveSyncDeviceStatistics
- Get-AcceptedDomain
- Set-AdServerSettings
- Get-ActiveSyncMailboxPolicy
- New-ActiveSyncMailboxPolicy
- Set-ActiveSyncMailboxPolicy
- Remove-ActiveSyncMailboxPolicy

To manage mobile devices running under Exchange ActiveSync protocol with Microsoft Exchange Server 2007, make sure that the user has been granted administrator rights. If the rights have not been granted, execute the commandlets to assign the administrator rights to the user (see the table below).

Administrator rights required for managing Exchange ActiveSync mobile devices on Microsoft Exchange Server 2007

Access	Object	Cmdlet
Full	Branch "CN=Mobile Mailbox Policies,CN=Your Organization,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=yourdomain"	<code>Add-ADPermission -User <User or group name> -Identity "CN=Mobile Mailbox Policies,CN=<Organization name>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<Domain name>" -InheritanceType All -AccessRight GenericAll</code>
Read	Branch "CN= Your Organization,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC= yourdomain"	<code>Add-ADPermission -User <User name or group name> -Identity "CN=<Organization name>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<Domain name>" -InheritanceType All -AccessRight GenericRead</code>
Read/write	Properties msExchMobileMailboxPolicyLink and msExchOmaAdminWirelessEnable for objects in Active Directory	<code>Add-ADPermission -User <User or group name> -Identity "DC=<Domain name>" -InheritanceType All -AccessRight ReadProperty,WriteProperty -Properties msExchMobileMailboxPolicyLink, msExchOmaAdminWirelessEnable</code>
Full	Mailbox repositories for ms-Exch-Store-Admin	<code>Get-MailboxDatabase Add-ADPermission -User <user or group name> -ExtendedRights ms-Exch-Store-Admin</code>

For detailed information about how to use commandlets in Exchange Management Shell console, please refer to the Microsoft Exchange Server Technical Support website [https://technet.microsoft.com/en-us/library/bb123778\(v=exchg.150\).aspx](https://technet.microsoft.com/en-us/library/bb123778(v=exchg.150).aspx).

Managing iOS MDM devices

This section describes advanced features for management of iOS MDM devices through Kaspersky Security Center. The application supports the following features for management of iOS MDM devices:

- Define the settings of managed iOS MDM devices in centralized mode and restrict features of devices through configuration profiles. You can add or modify configuration profiles and install them on mobile devices.
- Install apps on mobile devices by means of provisioning profiles, bypassing App Store. For example, you can use provisioning profiles for installation of in-house corporate apps on users' mobile devices. A provisioning profile contains information about an app and a mobile device.
- Install apps on an iOS MDM device through the App Store. Before installing an app on an iOS MDM device, you must add that app to an iOS MDM Server.

Every 24 hours, a push notification is sent to all connected iOS MDM devices in order to synchronize data with the iOS MDM Server (see section "Installing iOS MDM Server" on page [193](#)).

For information about the configuration profile and the provisioning profile, as well as apps installed on an iOS MDM device, please refer to the properties window of the device (see section "Viewing information about an iOS MDM device" on page [764](#)).

In this section

Issuing a certificate for an iOS MDM profile	756
Adding a configuration profile	757
Installing a configuration profile on a device.....	758
Removing the configuration profile from a device	758
Adding a new device by publishing a link to a profile	759
Adding a new device through profile installation by the administrator	759
Adding a provisioning profile	760
Installing a provisioning profile to a device	760
Removing a provisioning profile from a device.....	761
Adding a managed application	762
Installing an app on a mobile device	762
Removing an app from a device	763
Configuring roaming on an iOS MDM mobile device	764
Viewing information about an iOS MDM device	764
Disconnecting an iOS MDM device from management.....	765
Sending commands to a device	765
Checking the execution status of commands sent	765

Issuing a certificate for an iOS MDM profile

You can issue a certificate for an iOS MDM profile to allow a mobile device to verify it.

► To create an iOS MDM profile certificate:

1. In the **Mobile Device Management** folder in the console tree, select the **Mobile devices** subfolder.
2. In the context menu of the **Mobile devices** folder, select **Properties**.
3. In the properties window of the folder, select the **Connection settings for iOS devices** section.
4. Click the **Browse** button under the **Select certificate file** field.

The **Certificate** window.

5. In the **Certificate type** field, specify the public or private certificate type:
 - If the **PKCS #12 container** value is selected, specify the certificate file and the password.
 - If the **X.509 certificate** value is selected:
 - a. Specify the private key file (one with the *.prk or *.pem extension).

- b. Specify the private key password.
 - c. Specify the public key file (one with the *.cer extension).
6. Click **OK**.

The iOS MDM profile certificate is issued.

Adding a configuration profile

To create a configuration profile, you can use Apple Configurator 2, which is available at the Apple Inc. website. Apple Configurator 2 works only on devices running macOS; if you do not have such devices at your disposal, you can use iPhone Configuration Utility on the device with Administration Console instead. However, Apple Inc. does not support iPhone Configuration Utility any longer.

► *To create a configuration profile using iPhone Configuration Utility and to add it to an iOS MDM Server:*

1. In the console tree, select the **Mobile Device Management** folder.
2. In the workspace of the **Mobile Device Management** folder, select the **Mobile Device Servers** subfolder.
3. In the workspace of the **Mobile Device Servers** folder, select an iOS MDM Server.
4. In the context menu of the iOS MDM Server, select **Properties**.

The Mobile Device Server properties window opens.

5. In the properties window of the iOS MDM Server, select the **Configuration profiles** section.
6. In the **Configuration profiles** section, click the **Create** button.

The **New configuration profile** window opens.

7. In the **New configuration profile** window, specify a name and ID for the profile.

The configuration profile ID should be unique; the value should be specified in Reverse-DNS format, for example, *com.companyname.identifier*.

8. Click **OK**.

iPhone Configuration Utility then starts if you have it installed.

9. Reconfigure the profile in iPhone Configuration Utility.

For a description of the profile settings and instructions on how to configure the profile, please refer to the documentation enclosed with iPhone Configuration Utility.

After you configure the profile with iPhone Configuration Utility, the new configuration profile is displayed in the **Configuration profiles** section in the properties window of the iOS MDM Server.

You can click the **Modify** button to modify the configuration profile.

You can click the **Import** button to load the configuration profile to a program.

You can click the **Export** button to save the configuration profile to a file.

The profile that you have created must be installed on iOS MDM devices (see section "Installing a configuration profile on a device" on page [758](#)).

Installing a configuration profile on a device

► *To install a configuration profile to a mobile device:*

1. In the **Mobile Device Management** folder in the console tree, select the **Mobile devices** subfolder.

The folder workspace displays a list of managed mobile devices.

2. In the workspace, filter iOS MDM devices by protocol type (*iOS MDM*).
3. Select the user mobile device on which you have to install a configuration profile.

You can select multiple mobile devices to install the profile on them simultaneously.

4. In the context menu of the mobile device, select **Show command log**.

5. In the **Mobile device management commands** window, proceed to the **Install profile** section and click the **Send command** button.

You can also send the command to the mobile device by selecting **All commands** in the context menu of that mobile device, and then selecting **Install profile**.

The **Select profiles** window opens showing a list of profiles. Select from the list the profile that you have to install on the mobile device. You can select multiple profiles to install them on the mobile device simultaneously. To select the range of profiles, use the **SHIFT** key. To combine profiles into a group, use the **CTRL** key.

6. Click **OK** to send the command to the mobile device.

When the command is executed, the selected configuration profile will be installed on the user's mobile device. If the command is successfully executed, the current status of the command in the command log will be shown as *Done*.

You can click the **Resend** button to send the command to the user's mobile device again.

You can click the **Remove from queue** button to cancel execution of a command that was sent if the command has not yet been executed.

The **Command log** section displays commands that have been sent to the mobile device, with the respective execution statuses. Click **Refresh** to update the list of commands.

7. Click **OK** to close the **Mobile device management commands** window.

The profile that you installed can be viewed and removed if necessary (see section "Removing the configuration profile from a device" on page [758](#)).

Removing the configuration profile from a device

► *To remove a configuration profile from a mobile device:*

1. In the **Mobile Device Management** folder in the console tree, select the **Mobile devices** subfolder.

The folder workspace displays a list of managed mobile devices.

2. In the workspace, filter iOS MDM devices by clicking the **iOS MDM** link.
3. Select the user's mobile device from which you have to remove the configuration profile.

You can select multiple mobile devices to remove the profile from them simultaneously.

4. In the context menu of the mobile device, select **Show command log**.

5. In the **Mobile device management commands** window, proceed to the **Remove profile** section and click the **Send command** button.

You can also send the command to the mobile device by selecting **All commands** from the context menu of the device, and then selecting **Remove profile**.

The **Remove profiles** window opens showing the list of profiles.

6. Select from the list the profile that you have to remove from the mobile device. You can select multiple profiles to remove them from the mobile device simultaneously. To select the range of profiles, use the **SHIFT** key. To combine profiles into a group, use the **CTRL** key.
7. Click **OK** to send the command to the mobile device.

When the command is executed, the selected configuration profile will be removed from the user's mobile device. If the command is executed successfully, the current status of the command will be shown as *Completed*.

You can click the **Resend** button to send the command to the user's mobile device again.

You can click the **Remove from queue** button to cancel execution of a command that was sent if the command has not yet been executed.

The **Command log** section displays commands that have been sent to the mobile device, with the respective execution statuses. Click **Refresh** to update the list of commands.

8. Click **OK** to close the **Mobile device management commands** window.

Adding a new device by publishing a link to a profile

In Administration Console, the administrator creates a new iOS MDM profile, using the New Mobile Device Connection Wizard. The Wizard performs the following actions:

- The iOS MDM profile is automatically published on the Web Server.
- The user is sent a link to the iOS MDM profile by SMS or by email. Upon receiving the link, the user installs the iOS MDM profile on the mobile device.
- The mobile device connects to the iOS MDM Server.

Due to a stricter security policy introduced by Apple, you have to set up TLS 1.1 and TLS 1.2 protocol versions when connecting a mobile device running iOS 11 to an Administration Server that has integration with Public Key Infrastructure (PKI) enabled.

See also:

Kaspersky Security Center Web Server[212](#)

Adding a new device through profile installation by the administrator

To connect a mobile device to an iOS MDM Server by installing an iOS MDM profile on that mobile device, the administrator must perform the following actions:

1. In Administration Console, open the New Device Connection Wizard.
2. Create a new iOS MDM profile by selecting the **Show certificate after the Wizard finishes** check box in the New Profile Wizard window.

3. Save the iOS MDM profile.
4. Install the iOS MDM profile on the user's mobile device through the Apple Configurator utility.

The mobile device connects to the iOS MDM Server.

Due to a stricter security policy introduced by Apple, you have to set up TLS 1.1 and TLS 1.2 protocol versions when connecting a mobile device running iOS 11 to an Administration Server that has integration with Public Key Infrastructure (PKI) enabled.

See also:

| Kaspersky Security Center Web Server[212](#)

Adding a provisioning profile

► *To add a provisioning profile to an iOS MDM Server:*

1. In the console tree, open the **Mobile Device Management** folder.
2. In the **Mobile Device Management** folder in the console tree, select the **Mobile Device Servers** subfolder.
3. In the workspace of the **Mobile Device Servers** folder, select an iOS MDM Server.
4. In the context menu of the iOS MDM Server, select **Properties**.
The Mobile Device Server properties window opens.
5. In the properties window of the **iOS MDM Server**, go to the **Provisioning profiles** section.
6. In the **Provisioning profiles** section, click the **Import** button and specify the path to a provisioning profile file.

The profile will be added to the iOS MDM Server settings.

You can click the **Export** button to save the provisioning profile to a file.

The provisioning profile that you imported can be installed on iOS MDM devices (see section "Installing a provisioning profile to a device" on page [760](#)).

Installing a provisioning profile to a device

► *To install a provisioning profile on a mobile device:*

1. In the **Mobile Device Management** folder in the console tree, select the **Mobile devices** subfolder.
The folder workspace displays a list of managed mobile devices.
2. In the workspace, filter iOS MDM devices by protocol type (*iOS MDM*).
3. Select the user's mobile device on which you have to install the provisioning profile.
You can select multiple mobile devices to install the provisioning profile simultaneously.
4. In the context menu of the mobile device, select **Show command log**.

5. In the **Mobile device management commands** window, proceed to the **Install provisioning profile** section and click the **Send command** button.

You can also send the command to the mobile device by selecting **All commands** from the context menu of that mobile device, and then selecting **Install provisioning profile**.

The **Select provisioning profiles** window opens showing a list of provisioning profiles. Select from the list the provisioning profile that you have to install on the mobile device. You can select multiple provisioning profiles to install them on the mobile device simultaneously. To select the range of provisioning profiles, use the **SHIFT** key. To combine provisioning profiles into a group, use the **CTRL** key.

6. Click **OK** to send the command to the mobile device.

When the command is executed, the selected provisioning profile will be installed on the user's mobile device. If the command is successfully executed, the current status of the command in the command log will be shown as *Completed*.

You can click the **Resend** button to send the command to the user's mobile device again.

You can click the **Remove from queue** button to cancel execution of a command that was sent if the command has not yet been executed.

The **Command log** section displays commands that have been sent to the mobile device, with the respective execution statuses. Click **Refresh** to update the list of commands.

7. Click **OK** to close the **Mobile device management commands** window.

The profile that you installed can be viewed and removed, if necessary (see section "Removing a provisioning profile from a device" on page [761](#)).

Removing a provisioning profile from a device

► *To remove a provisioning profile from a mobile device:*

1. In the **Mobile Device Management** folder in the console tree, select the **Mobile devices** subfolder.

The folder workspace displays a list of managed mobile devices.

2. In the workspace, filter iOS MDM devices by protocol type (*iOS MDM*).

3. Select the user's mobile device from which you have to remove the provisioning profile.

You can select multiple mobile devices to remove the provisioning profile from them simultaneously.

4. In the context menu of the mobile device, select **Show command log**.

5. In the **Mobile device management commands** window, proceed to the **Remove provisioning profile** section and click the **Send command** button.

You can also send the command to the mobile device by selecting **All commands** from the context menu and then selecting **Remove provisioning profile**.

The **Remove provisioning profiles** window opens showing the list of profiles.

6. Select from the list the provisioning profile that you need to remove from the mobile device. You can select multiple provisioning profiles to remove them from the mobile device simultaneously. To select the range of provisioning profiles, use the **SHIFT** key. To combine provisioning profiles into a group, use the **CTRL** key.

7. Click **OK** to send the command to the mobile device.

When the command is executed, the selected provisioning profile will be removed from the user's mobile device. Applications that are related to the deleted provisioning profile will not be operable. If the command is executed successfully, the current status of the command will be shown as *Completed*.

You can click the **Resend** button to send the command to the user's mobile device again.

You can click the **Remove from queue** button to cancel execution of a command that was sent if the command has not yet been executed.

The **Command log** section displays commands that have been sent to the mobile device, with the respective execution statuses. Click **Refresh** to update the list of commands.

8. Click **OK** to close the **Mobile device management commands** window.

Adding a managed application

Before installing an app on an iOS MDM device, you must add that app to an iOS MDM Server. An application is considered managed if it has been installed on a device through Kaspersky Security Center. A managed application can be managed remotely by means of Kaspersky Security Center.

► *To add a managed application to an iOS MDM Server:*

1. In the console tree, open the **Mobile Device Management** folder.
2. In the **Mobile Device Management** folder in the console tree, select the **Mobile Device Servers** subfolder.
3. In the workspace of the **Mobile Device Servers** folder, select an iOS MDM Server.
4. In the context menu of the iOS MDM Server, select **Properties**.

This opens the properties window of the iOS MDM Server.

5. In the properties window of the iOS MDM Server, select the **Managed applications** section.
6. Click the **Add** button in the **Managed applications** section.

The **Add an application** window opens.

7. In the **Add an application** window, in the **App name** field, specify the name of the application to be added.
8. In the **Apple ID or App Store link** field, specify the Apple ID of the application to be added, or specify a link to a manifest file that can be used to download the application.
9. If you want a managed application to be removed from the user's mobile device along with the iOS MDM profile when removing the latter, select the **Remove together with iOS MDM profile** check box.
10. If you want to block the application data backup through iTunes, select the **Block data backup** check box.
11. Click **OK**.

The added application is displayed in the **Managed applications** section of the properties window of the iOS MDM Server.

Installing an app on a mobile device

► *To install an app on an iOS MDM mobile device:*

1. In the **Mobile Device Management** folder in the console tree, select the **Mobile devices** subfolder.

The folder workspace displays a list of managed mobile devices.

2. Select the iOS MDM device on which you want to install an app.

You can select multiple mobile devices to install the application on them simultaneously.

3. In the context menu of the mobile device, select **Show command log**.

4. In the **Mobile device management commands** window, proceed to the **Install app** section and click the **Send command** button.

You can also send the command to the mobile device by selecting **All commands** in the context menu of that mobile device, and then selecting **Install app**.

The **Select apps** window opens showing a list of profiles. Select from the list the application that you have to install on the mobile device. You can select multiple applications to install them on the mobile device simultaneously. To select a range of apps, use the **SHIFT** key. To combine apps into a group, use the **CTRL** key.

5. Click **OK** to send the command to the mobile device.

When the command is executed, the selected application will be installed on the user's mobile device. If the command is successfully executed, its current status in the command log will be shown as *Completed*.

You can click the **Resend** button to send the command to the user's mobile device again. You can click the **Remove from queue** button to cancel execution of a command that was sent if the command has not yet been executed.

The **Command log** section displays commands that have been sent to the mobile device, with the respective execution statuses. Click **Refresh** to update the list of commands.

6. Click **OK** to close the **Mobile device management commands** window.

Information about the application installed is displayed in the properties of the iOS MDM mobile device (see section "Viewing information about an iOS MDM device" on page [764](#)). You can remove the application from the mobile device through the command log or the context menu of the mobile device (see section "Removing an app from a device" on page [763](#)).

Removing an app from a device

► *To remove an app from a mobile device:*

1. In the **Mobile Device Management** folder in the console tree, select the **Mobile devices** subfolder.

The folder workspace displays a list of managed mobile devices.

2. In the workspace, filter iOS MDM devices by protocol type (*iOS MDM*).
3. Select the user's mobile device from which you have to remove the app.

You can select multiple mobile devices to remove the app from them simultaneously.

4. In the context menu of the mobile device, select **Show command log**.
5. In the **Mobile device management commands** window, proceed to the **Remove app** section and click the **Send command** button.

You can also send the command to the mobile device by selecting **All commands** in the context menu of the mobile device, then selecting **Remove app**.

The **Remove apps** window opens showing a list of applications.

6. Select from the list the app that you need to remove from the mobile device. You can select multiple apps to remove them simultaneously. To select a range of apps, use the **SHIFT** key. To combine apps into a group, use the **CTRL** key.
7. Click **OK** to send the command to the mobile device.

When the command is executed, the selected app will be removed from the user's mobile device. If the command is executed successfully, the current status of the command will be shown as *Completed*.

You can click the **Resend** button to send the command to the user's mobile device again.

You can click the **Remove from queue** button to cancel execution of a command that was sent if the command has not yet been executed.

The **Command log** section displays commands that have been sent to the mobile device, with the respective execution statuses. Click **Refresh** to update the list of commands.

8. Click **OK** to close the **Mobile device management commands** window.

Configuring roaming on an iOS MDM mobile device

► *To configure roaming.*

1. In the console tree, open the **Mobile Device Management** folder.
2. In the **Mobile Device Management** folder, select the **Mobile devices** subfolder.
The folder workspace displays a list of managed mobile devices.
3. Select the iOS MDM device owned by the user for whom you have to configure roaming.
You can select multiple mobile devices to configure roaming on them simultaneously.
4. In the context menu of the mobile device, select **Show command log**.
5. In the **Mobile device management commands** window, proceed to the **Configure roaming** section and click the **Send command** button.
You can also send the command to the mobile device by selecting **All commands** → **Configure roaming** from the context menu of the device.
6. In the **Roaming settings** window, specify the relevant settings:

- **Enable voice roaming**

If this check box is selected, the voice roaming is enabled on the iOS MDM mobile device. The user of the iOS MDM mobile device can make and answer calls while in roaming.

By default, this check box is selected.

- **Enable data roaming**

If this check box is selected, the data roaming is enabled on the iOS MDM mobile device. The user of the iOS MDM mobile device can surf the Internet while in roaming.

By default, this check box is cleared.

Roaming will be configured for the selected devices.

Viewing information about an iOS MDM device

► *To view information about an iOS MDM device:*

1. In the **Mobile Device Management** folder in the console tree, select the **Mobile devices** subfolder.
The folder workspace displays a list of managed mobile devices.
2. In the workspace, filter iOS MDM devices by clicking the **iOS MDM** link.
3. Select the mobile device about which you want to view information.

4. From the context menu of the mobile device select **Properties**.

The properties window of the iOS MDM device opens.

The properties window of the mobile device displays information about the connected iOS MDM device.

Disconnecting an iOS MDM device from management

► *To disconnect an iOS MDM device from the iOS MDM Server:*

1. In the **Mobile Device Management** folder in the console tree, select the **Mobile devices** subfolder.

The folder workspace displays a list of managed mobile devices.

2. In the workspace, filter iOS MDM devices by clicking the **iOS MDM** link.
3. Select the mobile device that you have to disconnect.
4. In the context menu of the mobile device, select **Delete**.

The iOS MDM device will be marked in the list for removal. The mobile device will be automatically removed from the list of managed devices after it is removed from the iOS MDM Server database. The mobile device will be removed from the iOS MDM Server database within one minute.

After the iOS MDM device is disconnected from management, all installed configuration profiles, the iOS MDM profile, and applications for which the **Remove together with iOS MDM profile** (see section "**Adding a managed application**" on page [762](#)) check box has been selected, will be removed from the mobile device.

Sending commands to a device

► *To send a command to an iOS MDM device, the administrator must perform the following actions:*

1. In Administration Console, open the **Mobile Device Management** node.
2. Select the **Mobile devices** folder.
3. In the **Mobile devices** folder, select the mobile device to which the commands need to be sent.
4. In the context menu of the mobile device, select **Show command log**.
5. In the list that appears, select the command to be sent to the mobile device.

Checking the execution status of commands sent

► *To check the execution status of a command that has been sent to a mobile device, the administrator must perform the following actions:*

1. In Administration Console, open the **Mobile Device Management** node.
2. Select the **Mobile devices** folder.
3. In the **Mobile devices** folder, select the mobile device on which the execution status needs to be checked for the selected commands.
4. In the context menu of the mobile device, select **Show command log**.

Managing KES devices

Kaspersky Security Center supports the following KES mobile device management features:

- Centrally manage KES devices by using commands (see section "Commands for mobile device management" on page [733](#)).
- View information about the settings for management of KES devices (see section "Viewing information about a KES device" on page [767](#)).
- Install applications by using mobile app packages (see section "Creating a mobile applications package for KES devices" on page [766](#)).
- Disconnect KES devices from management (see section "Disconnecting a KES device from management" on page [767](#)).

In this section

Creating a mobile applications package for KES devices	766
Enabling two-step verification of KES devices	766
Viewing information about a KES device.....	767
Disconnecting a KES device from management	767

Creating a mobile applications package for KES devices

A Kaspersky Endpoint Security for Android license is required to create a mobile applications package for KES devices.

► *To create a mobile applications package:*

1. In the **Remote installation** folder of the console tree, select the **Installation packages** subfolder.
The **Remote installation** folder is a subfolder of the **Advanced** folder by default.
2. Click the **Additional actions** button and select **Manage mobile apps packages** in the drop-down list.
3. In the **Mobile apps package management** window, click the **New** button.
4. The Mobile Applications Package Creation Wizard starts. Follow the instructions of the Wizard.

The newly created mobile applications package is displayed in the **Mobile apps package management** window.

Enabling two-step verification of KES devices

► *To enable two-step verification of a KES device:*

1. Open the system registry of the client device that has Administration Server installed (for example, locally, using the regedit command in the **Start** → **Run** menu).
2. Go to the following hive:
 - For a 64-bit system:

HKEY_LOCAL_MACHINE\SOFTWAREWow6432Node\KasperskyLab\Components\34\core\independent\KLLIM

- For a 32-bit system:

HKLM\Software\KasperskyLab\Components\34\core\independent\KLLIM

3. Create a key with the LP_MobileMustUseTwoWayAuthOnPort13292 name.
4. Specify REG_DWORD as the key type.
5. Set the key value on 1.
6. Restart the Administration Server service.

Mandatory two-step verification of the KES device using a shared certificate will be enabled after you run the Administration Server service.

The first connection of the KES device to the Administration Server does not require a certificate.

By default, two-step verification of KES devices is disabled.

Viewing information about a KES device

► *To view information about a KES device:*

1. In the **Mobile Device Management** folder in the console tree, select the **Mobile devices** subfolder.
The folder workspace displays a list of managed mobile devices.
2. In the workspace, filter KES devices by protocol type (*KES*).
3. Select the mobile device whose information you want to view.
4. From the context menu of the mobile device select **Properties**.

The properties window of the KES device opens.

The properties window of the mobile device displays information about the connected KES device.

Disconnecting a KES device from management

To disconnect a KES device from management, the user has to remove Network Agent from the mobile device. After the user has removed Network Agent, the mobile device details are removed from the Administration Server database, and the administrator can remove the mobile device from the list of managed devices.

► *To remove a KES device from the list of managed devices:*

1. In the **Mobile Device Management** folder in the console tree, select the **Mobile devices** subfolder.
The folder workspace displays a list of managed mobile devices.
2. In the workspace, filter KES devices by protocol type (*KES*).
3. Select the mobile device that you must disconnect from management.
4. In the context menu of the mobile device, select **Delete**.

The mobile device is removed from the list of managed devices.

If Kaspersky Endpoint Security for Android has not been removed from the mobile device, that mobile device reappears in the list of managed devices after synchronization with the Administration Server.

Data encryption and protection

Data encryption reduces the risk of unintentional leakage in case your notebook, removable drive, or hard drive is stolen or lost, or upon access by unauthorized users and applications.

Kaspersky Endpoint Security for Windows provides encryption functionality. Kaspersky Endpoint Security for Windows allows you to encrypt files stored on local drives of devices and removable drives, as well as encrypt removable drives and hard drives entirely.

Encryption rules are configured through Kaspersky Security Center by defining policies. Encryption and decryption according to the existing rules are performed when applying a policy.

Availability of the encryption management feature is determined by the user interface settings (see section "Configuring the interface" on page 300).

The administrator can perform the following actions:

- Configure and perform file encryption or decryption on local drives of the device.
- Configure and perform file encryption on removable drives.
- Create rules of access to encrypted files by applications.
- Create and deliver to the user a key file for access to encrypted files if file encryption is restricted on the user's device.
- Configure and perform hard drive encryption.
- Manage user access to encrypted hard drives and removable drives (manage authentication agent accounts, create and deliver to users information on request for account name and password restoration, as well as access keys for encrypted devices).
- View encryption statuses and reports about encryption of files.

These operations are performed using tools integrated into Kaspersky Endpoint Security for Windows. For detailed instructions on how to perform operations and a description of encryption features please refer to the Kaspersky Endpoint Security for Windows Online Help <https://support.kaspersky.com/KESWin/11.6.0/en-US/127971.htm>.

Kaspersky Security Center supports encryption management functionality for devices running MAC operating systems. Encryption is configured using Kaspersky Endpoint Security for Mac tools for those application versions that support encryption functionality. For detailed instructions on how to perform operations and a description of encryption features please refer to the *Kaspersky Endpoint Security for Mac Administrator's Guide*.

In this section

Viewing the list of encrypted devices.....	769
Viewing the list of encryption events	769
Exporting the list of encryption events to a text file	770
Creating and viewing encryption reports	770
Transmitting encryption keys between Administration Servers.....	772

Viewing the list of encrypted devices

► *To view the list of devices storing encrypted information:*

1. In the console tree of Administration Server, select the **Data encryption and protection** folder.
2. Open the list of encrypted devices in one of the following ways:
 - By clicking the **Go to list of encrypted drives** link in the **Manage encrypted drives** section.
 - By selecting the **Encrypted drives** folder in the console tree.

The workspace displays information about devices on the network storing encrypted files, and about devices encrypted at the drive level. After the information on a device is decrypted, the device is automatically removed from the list.

You can sort the information in the list of devices either in ascending or descending order in any column.

The user interface settings (see section "Configuring the interface" on page [300](#)) determine whether the **Data encryption and protection** folder appears in the console tree.

Viewing the list of encryption events

When running data encryption or decryption tasks on devices, Kaspersky Endpoint Security for Windows sends Kaspersky Security Center information about events of the following types:

- Cannot encrypt or decrypt a file, or create an encrypted archive due to a lack of free disk space.
- Cannot encrypt or decrypt a file, or create an encrypted archive due to license issues.
- Cannot encrypt or decrypt a file, or create an encrypted archive due to missing access rights.
- The application has been prohibited to access an encrypted file.
- Unknown errors.

► *To view a list of events that have occurred during data encryption on devices:*

1. In the console tree of Administration Server, select the **Data encryption and protection** folder.
2. Open the list of events that occurred during encryption in one of the following ways:
 - By clicking the **Go to error list** link in the **Data encryption errors** section.

- By selecting the **Encrypted drives** folder in the console tree.

The workspace displays information about problems that have occurred during data encryption on devices.

You can take the following actions in the list of encryption events:

- Sort data records in ascending or descending order in any of the columns.
- Perform a quick search for records (by text match with a substring in any of the list fields).
- Export the list of events to a text file.

The user interface settings (see section "Configuring the interface" on page [300](#)) determine whether the **Data encryption and protection** folder appears in the console tree.

Exporting the list of encryption events to a text file

► *To export the list of encryption events to a text file:*

1. Create a list of encryption events (see section "Viewing the list of encryption events" on page [769](#)).
2. From the context menu of the events list select **Export list**.

The **Export list** window opens.

3. In the **Export list** window, specify the name of the text file with the list of events, select a folder to save it and click the **Save** button.

The list of encryption events will be saved to the file that you have specified.

Creating and viewing encryption reports

The administrator can generate the following reports:

- Report on encryption status of mass storage devices. This report contains information about the device encryption status for all groups of devices.
- Report on rights of access to encrypted devices. This report contains information about the status of user accounts that have been granted access to encrypted devices.
- Report on file encryption errors. This report contains information about errors that occurred when data encryption or decryption tasks were run on devices.
- Report on encryption status of managed devices. This report contains information about whether the encryption status of devices meets the encryption policy.
- Report on blockage of access to encrypted files. This report contains information about blocking application access to encrypted files.

► *To generate the report on encryption of devices:*

1. In the console tree, select the **Data encryption and protection** folder.
2. Do one of the following:
 - To generate the report on the encryption status of managed devices, click the **View report on encryption status of mass storage devices** link.

If you have not configured this report yet, the New Report Template Wizard will start. Follow the steps of the wizard.

- To generate the report on encryption status of mass storage devices, in the console tree select the **Encrypted drives** subfolder, and then click the **View report on encryption status of mass storage devices** button.

The report generation starts. The report appears on the **Reports** tab of the **Administration Server** node.

► *To generate the report on rights of access to encrypted devices:*

1. In the console tree, select the **Data encryption and protection** folder.
2. Do one of the following:
 - Click the **Report on rights to access encrypted drives** link in the **Manage encrypted drives** section to start the New Report Template Wizard.
 - Select the **Encrypted drives** subfolder, then click the **Report on rights to access encrypted drives** button to start the New Report Template Wizard.
3. Follow the steps of the New Report Template Wizard.

The report generation starts. The report appears on the **Reports** tab of the **Administration Server** node.

► *To generate the report on file encryption errors:*

1. In the console tree, select the **Data encryption and protection** folder.
2. Do one of the following:
 - Click the **View report on file encryption errors** link in the **Data encryption errors** section to start the New Report Template Wizard.
 - Select the **Encryption events** subfolder, then click the **Report on file encryption errors** link to start the New Report Template Wizard.
3. Follow the steps of the New Report Template Wizard.

The report generation starts. The report appears on the **Reports** tab of the **Administration Server** node.

► *To generate the report on the status of encryption of managed devices:*

1. In the console tree, select the node with the name of the required Administration Server.
2. In the workspace of the node, select the **Reports** tab.
3. Click the **New report template** button to start the New Report Template Wizard.
4. Follow the instructions of the New Report Template Wizard. In the **Selecting the report template type** window, in the **Other** section select **Report on encryption status of managed devices**.

After you have finished with the New Report Template Wizard, a new report template appears in the Administration Server node, on the **Reports** tab.

5. In the node of the relevant Administration Server on the **Reports** tab, select the report template that was created during the previous steps of the instructions.

The report generation starts. The report appears on the **Reports** tab of the **Administration Server** node.

You can also obtain information about whether the encryption statuses of devices and removable drives conform to the encryption policy by viewing information panes on the **Statistics** tab of the Administration Server node.

► *To generate the report on blockage of access to encrypted files:*

1. In the console tree, select the node with the name of the required Administration Server.
2. In the workspace of the node, select the **Reports** tab.
3. Click the **New report template** button to start the New Report Template Wizard.
4. Follow the instructions of the New Report Template Wizard. In the **Selecting the report template type** window, in the **Other** section, select **Report on blockage of access to encrypted files**.

After the New Report Template Wizard finishes, a new report template appears in the **Administration Server** node, on the **Reports** tab.

5. In the node of the **Administration Server** on the **Reports** tab, select the report template that was created during the previous steps of the instructions.

The report generation starts. The report appears on the **Reports** tab of the **Administration Server** node.

Transmitting encryption keys between Administration Servers

If the data encryption feature is enabled on a managed device, the encryption key is stored on the Administration Server. The encryption key is used to access encrypted data and to manage the encryption policy.

The encryption key must be transmitted to another Administration Server in the following cases:

- You reconfigure Network Agent on a managed device to assign the device to another Administration Server. If this device contains encrypted data, the encryption key must be transmitted to the target Administration Server. Otherwise, the data cannot be decrypted.
- You encrypt a removable drive connected to a device D1 that is managed by the Administration Server S1, and then you connect this removable drive to a device D2 managed by the Administration Server S2. To access to the data on the removable drive, the encryption key must be transmitted from the Administration Server S1 to the Administration Server S2.
- You encrypt a file on a device D1 managed by the Administration Server S1, and then you try to access the file on a device D2 managed by the Administration Server S2. To access the file, the encryption key must be transmitted from the Administration Server S1 to the Administration Server S2.

You can transmit encryption keys the following ways:

- Automatically, by enabling the **Use hierarchy of Administration Servers to obtain encryption keys** option in the properties of two Administration Servers between which an encryption key must be transmitted. If this option is disabled for one of the Administration Servers, the automatic transmission of encryption keys is not possible.

When you enable the **Use hierarchy of Administration Servers to obtain encryption keys** option in an Administration Server properties, the Administration Server sends all of the encryption keys stored in its repository to the primary Administration Server (if any) one level up in the hierarchy.

When you try to access encrypted data, the Administration Server first searches the encryption key in its own repository. If the **Use hierarchy of Administration Servers to obtain encryption keys** option is enabled and the required encryption key has not been found in the repository, the Administration Server additionally sends a request to the primary Administration Servers (if any) to provide the required encryption key. The request will be sent to all of the primary Administration Servers up to the server on the highest level of the hierarchy.

- Manually from one Administration Server to another by exporting and importing the file containing the encryption keys.

► *To enable automatic transmission of encryption keys between Administration Servers within the hierarchy:*

1. In the console tree, select the Administration Server for which you want to enable automatic transmission of encryption keys.
2. In the context menu of the Administration Server, select **Properties**.
3. In the properties window, select the **Encryption algorithm** section.
4. Enable the **Use hierarchy of Administration Servers to obtain encryption keys** option.
5. Click **OK** to apply the changes.

The encryption keys will be transmitted to primary Administration Servers (if any) at the next synchronization (the heartbeat). This Administration Server will also provide, upon request, an encryption key from its repository to a secondary Administration Server.

► *To transmit encryption keys between Administration Servers manually:*

1. In the console tree of Administration Server, select the secondary Administration Server from which you want to transmit encryption keys.
2. In the context menu of the Administration Server, select **Properties**.
3. In the properties window, select the **Encryption algorithm** section.
4. Click the **Export encryption keys from Administration Server**.
5. In the **Export encryption keys** window:
 - Click the **Browse** button, and then specify where to save the file.
 - Specify a password to protect the file from unauthorized access.

Remember the password. A lost password cannot be retrieved. If the password is lost, you have to repeat the export procedure. Therefore, make a note of the password and keep it handy.

6. Transmit the file to another Administration Server, for example, through a shared folder or removable drive.
7. On the target Administration Server, make sure that Kaspersky Security Center Administration Console is running.
8. In the console tree of Administration Server, select the target Administration Server where you want to transmit encryption keys.
9. In the context menu of the Administration Server, select **Properties**.
10. In the properties window, select the **Encryption algorithm** section.
11. Click **Import encryption keys to Administration Server**.
12. In the **Import encryption keys** window:
 - Click the **Browse** button, and then select the file containing encryption keys.
 - Specify the password.
13. Click **OK**.

The encryption keys are transmitted to the target Administration Server.

See also:

Data encryption and protection	768
--------------------------------------	---------------------

Data repositories

This section provides information about data stored on the Administration Server and used for tracking the condition of client devices and for servicing them.

The **Repositories** folder of the console tree displays the data used for tracking the statuses of client devices.

The **Repositories** folder contains the following objects:

- Updates downloaded by the Administration Server that are distributed to client devices (see section "Viewing downloaded updates" on page [424](#))
- List of equipment detected on the network
- License keys detected on client devices (see section "Kaspersky applications: licensing and activation" on page [357](#))
- Files placed in Quarantine folders on devices by security applications
- Files placed in Backup on client devices
- Files postponed for a later scan by security applications

In this section

Exporting a list of repository objects to a text file	774
Installation packages	775
Main statuses of files in the repository	775
Triggering of rules in Smart Training mode	776
Quarantine and Backup	780
Active threats	783

Exporting a list of repository objects to a text file

You can export the list of objects from the repository to a text file.

► *To export the list of objects from the repository to a text file:*

1. In the console tree, in the **Repositories** folder select the subfolder of the relevant repository.
2. In the repository subfolder, select **Export list** in the context menu.

This will open the **Export list** window, in which you can specify the name of text file and path to the folder where it was placed.

Installation packages

Kaspersky Security Center places the installation packages for applications of Kaspersky and third-party vendors in data repositories.

An *installation package* is a set of files required to install an application. An installation package contains the setup settings and initial configuration of the application being installed.

If you want to install an application on a client device, create an installation package (see section "Creating installation packages of applications" on page [717](#)) for that application, or use an existing one. The list of created installation packages is stored in the **Remote installation** folder of the console tree, the **Installation packages** subfolder.

See also:

Working with installation packages.....	344
---	---------------------

Main statuses of files in the repository

Security applications scan files on devices for known viruses and other programs that may pose a threat, assign statuses to files, and place some of them in the repository.

For example, security applications can do the following:

- Save a copy of a file to the repository before deletion
- Isolate probably infected files in the repository

The main statuses of files are presented in the table below. You can obtain more detailed information about actions to take on files in respective Help systems of security applications.

Table 68. Statuses of files in the repository

Status name	Status description
Infected	The file has a section of code of a known virus or other malware whose information is found in Kaspersky anti-virus databases.
Not infected	No known viruses or other malware were detected in the file.
Warning	The file contains a fragment of code that partially matches a snippet of code of a known threat.
Probably infected	The file contains either modified code of a known virus or code resembling a virus that is not yet known to Kaspersky.
Placed to folder by user	The user manually placed the file in the repository because the file's behavior gave rise to suspicion that it contains some threats. The user can scan the file for threats by using up-to-date databases.
False positive	A Kaspersky application assigned Infected status to a non-infected file because its code is similar to that of a virus. After a scan with up-to-date databases, the file is identified as non-infected.
Disinfected	The file was successfully disinfected.
Deleted	The file was deleted during processing.
Password-protected	The file cannot be processed because it is protected with a password.

See also:

File status icons in Administration Console913

Triggering of rules in Smart Training mode

This section provides information about the detections performed by the Adaptive Anomaly Control rules in Kaspersky Endpoint Security for Windows on client devices.

The rules detect anomalous behavior on client devices and may block it. If the rules work in Smart Training mode, they detect anomalous behavior and send reports about every such occurrence to Kaspersky Security Center Administration Server. This information is stored as a list in the **Triggering of rules in Smart Training state** subfolder of the **Repositories** folder. You can confirm detections as correct (see section "Viewing the list of detections performed using Adaptive Anomaly Control rules" on page 777) or add them as exclusions (see section "Adding exclusions from the Adaptive Anomaly Control rules" on page 779), so that this type of behavior is not considered anomalous anymore.

Information about detections is stored in the event log (see section "Using event selections" on page 1289) on the Administration Server (along with other events) and in the Adaptive Anomaly Control report (see section "Using reports" on page 1283).

For more information about Adaptive Anomaly Control, the rules, their modes and statuses, refer to Kaspersky Endpoint Security for Windows Help.

In this section

Viewing the list of detections performed using Adaptive Anomaly Control rules	777
Adding exclusions from the Adaptive Anomaly Control rules.....	779

Viewing the list of detections performed using Adaptive Anomaly Control rules

► *To view the list of detections performed by Adaptive Anomaly Control rules:*

1. In the console tree, select the node of the Administration Server that you require.
2. Select the **Triggering of rules in Smart Training state** subfolder (by default, this is a subfolder of **Advanced** → **Repositories**).

The list displays the following information about detections performed using Adaptive Anomaly Control rules:

- **Administration group**
The name of the administration group where the device belongs.
- **Device name**
The name of the client device where the rule was applied.
- **Name**
The name of the rule that was applied.
- **Status**
Excluding—If the Administrator processed this item and added it as an exclusion to the rules. This status remains till the next synchronization of the client device with the Administration Server; after the synchronization, the item disappears from the list.
Confirming—If the Administrator processed this item and confirmed it. This status remains till the next synchronization of the client device with the Administration Server; after the synchronization, the item disappears from the list.
Empty—If the Administrator did not process this item.
- **Total times rules were triggered**
The number of detects within one heuristic rule, one process and one client device. This number is counted by Kaspersky Endpoint Security.
- **User name**
The name of the client device user who run the process that generated the detect.
- **Source process path**
Path to the source process, i.e. to the process that performs the action (for more information, refer to the Kaspersky Endpoint Security help).
- **Source process hash**
SHA-256 hash of the source process file (for more information, refer to the Kaspersky Endpoint Security help).
- **Source object path**

Path to the object that started the process (for more information, refer to the Kaspersky Endpoint Security help).

- **Source object hash**

SHA-256 hash of the source file (for more information, refer to the Kaspersky Endpoint Security help).

- **Target process path**

Path to the target process (for more information, refer to the Kaspersky Endpoint Security help).

- **Target process hash**

SHA-256 hash of the target file (for more information, refer to the Kaspersky Endpoint Security help).

- **Target object path**

Path to the target object (for more information, refer to the Kaspersky Endpoint Security help).

- **Target object hash**

SHA-256 hash of the target file (for more information, refer to the Kaspersky Endpoint Security help).

- **Processed**

Date when the anomaly was detected.

► *To view properties of each information element:*

1. In the console tree, select the node of the Administration Server that you require.
2. Select the **Triggering of rules in Smart Training state** subfolder (by default, this is a subfolder of **Advanced** → **Repositories**).
3. In the **Triggering of rules in Smart Training state** workspace, select the object that you want.
4. Do one of the following:
 - Click the **Properties** link in the information box that appears on the right side of the screen.
 - Right-click, and in the context menu select **Properties**.

The properties window of the object opens, displaying information about the selected element.

You can confirm or add to exclusions (see section "Triggering of rules in Smart Training mode" on page [776](#)) any element in the list of detections of Adaptive Anomaly Control rules.

► *To confirm an element,*

Select an element (or several elements) in the list of detections and click the **Confirm** button.

The status of the element(s) will be changed to **Confirming**.

Your confirmation will contribute to the statistics used by the rules (for more information, refer to Kaspersky Endpoint Security 11 for Windows Help).

► *To add an element as an exclusion,*

Right-click an element (or several elements) in the list of detections and select **Add to exclusions** in the context menu.

The Add Exclusion Wizard (see section "Adding exclusions from the Adaptive Anomaly Control rules" on page [779](#)) starts. Follow the Wizard instructions.

If you reject or confirm an element, it will be excluded from the list of detections after the next synchronization of the client device with the Administration Server, and will no longer appear in the list.

Adding exclusions from the Adaptive Anomaly Control rules

The Add Exclusion Wizard allows you to add exclusions from the Adaptive Anomaly Control rules for Kaspersky Endpoint Security.

You can start the Wizard through one of the three procedures below.

► *To start the Add Exclusion Wizard through the Adaptive Anomaly Control node:*

1. In the console tree, select the node of the required Administration Server.
2. Select **Triggering of rules in Smart Training state** (by default, this is a subfolder of **Advanced** → **Repositories**).
3. In the workspace, right-click an element (or several elements) in the list of detections and select **Add to exclusions**.

You can add up to 1000 exclusions at a time. If you select more elements and try to add them to exclusions, an error message is displayed.

The Add Exclusion Wizard starts.

You can start the Add Exclusion Wizard from other nodes in the console tree:

- **Events** tab of the main window of the Administration Server (then the **User requests** option or **Recent events** option).
- **Report on Adaptive Anomaly Control rules state, Detections count** column.

In this section

Step 1. Selecting the application	780
Step 2. Selecting the policy (policies).....	780
Step 3. Processing of the policy (policies).....	780

Step 1. Selecting the application

This step can be skipped if you have only one Kaspersky Endpoint Security for Windows version and do not have other applications that support the Adaptive Anomaly Control rules.

The Add Exclusion Wizard shows the list of Kaspersky applications whose management plug-ins allow you to add exclusions to the policies for these applications. Select an application from this list and click **Next** to proceed to selecting the policy to which the exclusion will be added.

Step 2. Selecting the policy (policies)

The Wizard shows the list of policies (with policy profiles) for Kaspersky Endpoint Security.

Select all the policies and profiles to which you want to add exclusions and click **Next**.

Step 3. Processing of the policy (policies)

The Wizard displays a progress bar as the policies are processed. You can interrupt the processing of policies by clicking **Cancel**.

Inherited policies cannot be updated. If you do not have the rights to modify a policy, this policy will not be updated either.

When all the policies are processed (or if you interrupt the processing), a report appears. It shows which policies were updated successfully (green icon) and which policies were not updated (red icon).

This is the last step of the Wizard. Click **Finish** to close the Wizard.

Quarantine and Backup

Kaspersky anti-virus applications installed on client devices may place files in Quarantine or Backup during device scan.

Quarantine is a special repository for storing files that are probably infected with viruses and files that cannot be disinfected at the time when they are detected.

Backup is designed for storing backup copies of files that have been deleted or modified during the disinfection process.

Kaspersky Security Center creates a summarized list of files placed in Quarantine or Backup by Kaspersky applications on the devices. Network Agents on client devices transmit information about the files in Quarantine and Backup to the Administration Server. You can use Administration Console to view the properties of files stored in repositories on devices, run virus scans of those repositories, and delete files from them. The icons of the file statuses are described in the appendix (see section "File status icons in Administration Console" on page [913](#)).

Operations with Quarantine and Backup are supported for versions 6.0 or later of Kaspersky Anti-Virus for Windows Workstations and Kaspersky Anti-Virus for Windows Servers, as well as for Kaspersky Endpoint Security 10 for Windows, or later versions.

Kaspersky Security Center does not copy files from repositories to Administration Server. All files are stored in repositories on the devices. You can restore a file only on the device with the anti-virus application, which placed that file in the repository.

In this section

Enabling remote management for files in the repositories	781
Viewing properties of a file placed in repository	781
Deleting files from repositories	781
Restoring files from repositories	782
Saving a file from repositories to disk.....	782
Scanning files in Quarantine.....	782

Enabling remote management for files in the repositories

By default, you cannot manage files placed in repositories on client devices.

► *To enable remote management of files stored in repositories on client devices:*

1. In the console tree, select an administration group, for which you want to enable remote management for files in the repository.
2. In the group workspace, open the **Policies** tab.
3. On the **Policies** tab, select the policy of the security application that has placed the files in the repositories on the devices.
4. In the policy settings window in the **Data transfer to Administration Server** group of settings, select the check boxes corresponding to the repositories for which you want to enable the remote management.

The location of the **Data transfer to Administration Server** settings group in the policy properties window and the names of check boxes depend on the currently used security application.

Viewing properties of a file placed in repository

► *To view properties of a file in Quarantine or Backup:*

1. In the console tree, select the **Repositories** folder, the **Quarantine** or **Backup** subfolder.
2. In the workspace of the **Quarantine (Backup)** folder, select a file whose properties you want to view.
3. By selecting **Properties** in the context menu of the file.

Deleting files from repositories

► *To delete a file from Quarantine or Backup:*

1. In the console tree, in the **Repositories** folder, select the **Quarantine** or **Backup** subfolder.

2. In the workspace of the **Quarantine** (or **Backup**) folder select the files that you want to delete by using the **Shift** and **Ctrl** keys.
3. Delete the files in one of the following ways:
 - By selecting **Delete** in the context menu of the files.
 - By clicking the **Delete objects (Delete object)** (if you want to delete one file) link in the information box for the selected files.

The security applications that placed files in repositories on client devices will delete the same files from those repositories.

Restoring files from repositories

► *To restore a file from Quarantine or Backup:*

1. In the console tree, select the **Repositories** folder, the **Quarantine** or **Backup** subfolder.
2. In the workspace of the **Quarantine (Backup)** folder select the files that you want to restore by using the **Shift** and **Ctrl** keys.
3. Start restoration of the files in one of the following ways:
 - By selecting **Restore** in the context menu of the files.
 - By clicking the **Restore** link in the information box for the selected files.

The security applications that placed files in repositories on client devices will restore the same files to their original folders.

Saving a file from repositories to disk

Kaspersky Security Center allows you to save on a disk copies of files that a security application placed in Quarantine or Backup on a client device. Files are copied to the device with Kaspersky Security Center installed, to the specified folder.

► *To save a copy of file from Quarantine or Backup to a hard drive:*

1. In the console tree, select the **Repositories** folder, the **Quarantine** or **Backup** subfolder.
2. In the workspace of the **Quarantine (Backup)** folder, select a file that you want to copy to the hard drive.
3. Start copying in one of the following ways:
 - By selecting **Save to Disk** in the context menu of the file.
 - By clicking the **Save to Disk** link in the information box for the selected file.

The security application that placed the file in Quarantine on the client device will save a copy of that file to the specified folder.

Scanning files in Quarantine

► *To scan quarantined files:*

1. In the console tree, select the **Repositories** folder, the **Quarantine** subfolder.

2. In the workspace of the **Quarantine** folder, select the files that you want to scan by using the **SHIFT** and **CTRL** keys.
3. Start the file scan in one of the following ways:
 - By selecting **Scan** in the context menu of the file.
 - By clicking the **Scan** link in the information box for the selected files.

The application runs the on-demand scan task for security applications that have placed the selected files in Quarantine on the devices where those files are stored.

Active threats

Information about unprocessed files that have been detected on client devices is stored in the **Repositories** folder, **Active threats** subfolder.

Postponed processing and disinfection are performed by the security application upon request or after a specified event occurs. You can configure the postponed processing.

In this section

Disinfecting an unprocessed file	783
Saving an unprocessed file to disk	783
Deleting files from the "Active threats" folder	784

Disinfecting an unprocessed file

► *To start disinfection of an unprocessed file:*

1. In the console tree, in the **Repositories** folder select the **Active threats** subfolder.
2. In the workspace of the **Active threats** folder, select the file that you have to disinfect.
3. Start disinfection of the file in one of the following ways:
 - By selecting **Disinfect** in the context menu of the file.
 - By clicking the **Disinfect** link in the information box for the selected file.

The attempt to disinfect this file is then performed.

If the file is disinfecting, the security application installed on the client device restores it to its original folder. The record of the file is removed from the list in the **Active threats** folder. If the file cannot be disinfecting, the security application installed on the device deletes it from that device. The record of the file is removed from the list in the **Active threats** folder.

Saving an unprocessed file to disk

Kaspersky Security Center allows you to save to disk copies of unprocessed files found on client devices. Files are copied to the device with Kaspersky Security Center installed, to the specified folder.

► *To save a copy of an unprocessed file to disk:*

1. In the console tree, in the **Repositories** folder select the **Active threats** subfolder.
2. In the workspace of the **Active threats** folder, select the files that you have to copy to disk.
3. Start copying in one of the following ways:
 - By selecting **Save to Disk** in the context menu of the file.
 - By clicking the **Save to Disk** link in the information box for the selected file.

The security application installed on the client device on which the unprocessed file has been found saves a copy of that file to the specified folder.

Deleting files from the "Active threats" folder

► *To delete a file from the **Active threats** folder:*

1. In the console tree, in the **Repositories** folder select the **Active threats** subfolder.
2. In the workspace of the **Active threats** folder, select the files that you have to delete by using the **SHIFT** and **CTRL** keys.
3. Delete the files in one of the following ways:
 - By selecting **Delete** in the context menu of the files.
 - By clicking the **Delete objects (Delete object if you want to delete one file)** link in the information box for the selected files.

The security applications that placed the files in repositories on client devices, will delete the same files from those repositories. The records of the files are removed from the list in the **Active threats** folder.

Kaspersky Security Network (KSN)

This section describes how to use an online service infrastructure named Kaspersky Security Network (KSN). The section provides the details on KSN, as well as instructions on how to enable KSN, configure access to KSN, and view the statistics of the use of KSN proxy server.

In this chapter

About KSN	785
Setting up access to Kaspersky Security Network	786
Enabling and disabling KSN	788
Viewing the accepted KSN Statement.....	788
Viewing the KSN proxy server statistics	789
Accepting an updated KSN Statement	789
Enhanced protection with Kaspersky Security Network	791
Checking whether the distribution point works as KSN Proxy.....	791

About KSN

Kaspersky Security Network (KSN) is an online service infrastructure that provides access to the online Knowledge Base of Kaspersky, which contains information about the reputation of files, web resources, and software. The use of data from Kaspersky Security Network ensures faster responses by Kaspersky applications to threats, improves the effectiveness of some protection components, and reduces the risk of false positives. KSN allows you to use Kaspersky reputation databases to retrieve information about applications installed on managed devices.

By participating in KSN, you agree to send to Kaspersky in automatic mode information about the operation of Kaspersky applications installed on client devices that are managed through Kaspersky Security Center. Information is transferred in accordance with the current KSN access settings (see section "Setting up access to Kaspersky Security Network" on page [786](#)).

The application prompts you to join KSN while running the Quick Start Wizard. You can start or stop using KSN at any moment when using the application (see section "Enabling and disabling KSN" on page [788](#)).

You use KSN in accordance with the KSN Statement that you read and accept when you enable KSN. If the KSN Statement is updated, it is displayed to you when you update or upgrade Administration Server. You can accept the updated KSN Statement or decline it. If you decline it, you keep using KSN in accordance with the previous version of KSN Statement that you accepted before.

Client devices managed by the Administration Server interact with KSN through KSN Proxy. KSN Proxy provides the following features:

- Client devices can send requests to KSN and transfer information to KSN even if they do not have direct access to the Internet.
- The KSN proxy server caches processed data, thus reducing the load on the outbound channel and the time period spent for waiting for information requested by a client device.

You can configure the KSN proxy server in the **KSN Proxy** section of the Administration Server properties window (see section "Setting up access to Kaspersky Security Network" on page [786](#)).

Setting up access to Kaspersky Security Network

You can set up access to Kaspersky Security Network (KSN) on the Administration Server and on a distribution point.

► *To set up Administration Server access to Kaspersky Security Network (KSN):*

1. In the console tree, select the Administration Server for which you want to configure access to KSN.
2. In the context menu of the Administration Server, select **Properties**.
3. In the Administration Server properties window, in the **Sections** pane, select **KSN Proxy** → **KSN Proxy settings**.
4. In the workspace, enable the **Use Administration Server as proxy server** option to use the KSN Proxy service.

Data is sent from client devices to KSN in accordance with the Kaspersky Endpoint Security policy, which is active on those client devices. If this check box is cleared, no data will be sent to KSN from the Administration Server and client devices through Kaspersky Security Center. However, client devices can send data to KSN directly (bypassing Kaspersky Security Center), in accordance with their respective settings. The Kaspersky Endpoint Security for Windows policy, which is active on client devices, determines which data will be sent directly (bypassing Kaspersky Security Center) from those devices to KSN.

5. Enable the **I agree to use Kaspersky Security Network** option.

If this option is enabled, client devices send patch installation results to Kaspersky. When enabling this option, make sure to read and accept the terms of the KSN Statement.

If you are using Private KSN, enable the **Configure Private KSN** option and click the **Select file with KSN Proxy settings** button to download the settings of Private KSN (files with the extensions pkcs7 and pem). After the settings are downloaded, the interface displays the provider's name and contacts, as well as the creation date of the file with the settings of Private KSN.

When you enable Private KSN, pay attention to the distribution points configured to send KSN requests directly to the Cloud KSN. The distribution points that have Network Agent version 11 (or earlier) installed will continue to send KSN requests to the Cloud KSN. To reconfigure the distribution points to send KSN requests to Private KSN, enable the **Forward KSN requests to Administration Server** option for each distribution point. You can enable this option in the distribution point properties or in the Network Agent policy.

When you select the **Configure Private KSN** check box, a message appears with details about Private KSN.

The following Kaspersky applications support Private KSN:

- Kaspersky Security Center 10 Service Pack 1 or later
- Kaspersky Endpoint Security 10 Service Pack 1 for Windows or later
- Kaspersky Security for Virtualization 3.0 Agentless Service Pack 2
- Kaspersky Security for Virtualization 3.0 Service Pack 1 Light Agent

If you enable the **Configure Private KSN** option in Kaspersky Security Center, these applications receive information about supporting Private KSN. In the settings window of the application, in the **Kaspersky Security Network** subsection of the **Advanced Threat Protection** section, **KSN provider: Private KSN** is displayed. Otherwise, **KSN provider: Global KSN** is displayed.

If you use application versions earlier than Kaspersky Security for Virtualization 3.0 Agentless Service Pack 2 or earlier than Kaspersky Security for Virtualization 3.0 Service Pack 1 Light Agent when running Private KSN, we recommend that you use secondary Administration Servers for which the use of Private KSN has not been enabled.

Kaspersky Security Center does not send any statistical data to Kaspersky Security Network if Private KSN is configured in the **KSN Proxy** → **KSN Proxy settings** section of the Administration Server properties window.

If you have the proxy server settings configured in the Administration Server properties, but your network architecture requires that you use Private KSN directly, enable the **Ignore KSC proxy server settings when connecting to Private KSN** option. Otherwise, requests from the managed applications cannot reach Private KSN.

6. Configure the Administration Server connection to the KSN Proxy service:
 - Under **Connection settings**, for the **TCP port**, specify the number of the TCP port that will be used for connecting to the KSN Proxy server. The default port to connect to the KSN Proxy server is 13111.
 - If you want the Administration Server to connect to the KSN Proxy server through a UDP port, enable the **Use UDP port** option and specify a port number for the **UDP port**. By default, this option is disabled, and TCP port is used. If this option is enabled, the default UDP port to connect to the KSN Proxy server is 15111.
7. Enable the **Connect secondary Administration Servers to KSN through primary Administration Server** option.

If this option is enabled, secondary Administration Servers use the primary Administration Server as the KSN proxy server. If this option is disabled, secondary Administration Servers connect to KSN on their own. In this case, managed devices use secondary Administration Servers as KSN proxy servers.

Secondary Administration Servers use the primary Administration Server as a proxy server if in the right pane of the **KSN Proxy settings** section, in the properties of secondary Administration Servers the **Use Administration Server as a proxy server** check box is selected.

8. Click **OK**.

The KSN access settings will be saved.

You can also set up distribution point access to KSN, for example, if you want to reduce the load on the Administration Server. The distribution point that acts as a KSN proxy server sends KSN requests from managed devices to Kaspersky directly, without using the Administration Server.

► *To set up distribution point access to Kaspersky Security Network (KSN):*

1. Make sure that the distribution point is assigned manually (see section "Assigning a device a distribution point manually" on page [427](#)).
2. In the console tree, select the **Administration Server** node.
3. In the context menu of the Administration Server, select **Properties**.
4. In the Administration Server properties window, select the **Distribution points** section.
5. Select the distribution point in the list and click the **Properties** button to open its properties window.
6. In the distribution point properties window, in the **KSN Proxy** section, select **Access KSN Cloud directly over Internet**.

7. Click **OK**.

The distribution point will act as a KSN Proxy server.

Enabling and disabling KSN

► *To enable KSN:*

1. In the console tree, select the Administration Server for which you need to enable KSN.
2. In the context menu of the Administration Server, select **Properties**.
3. In the Administration Server properties window, in the **KSN Proxy** section, select the **KSN Proxy settings** subsection.
4. Select the **Use Administration Server as a proxy server**.

The KSN proxy server is enabled.

5. Select the **I agree to use Kaspersky Security Network** check box.

KSN will be enabled.

If this check box is selected, client devices send patch installation results to Kaspersky. When selecting this check box, you should read and accept the terms of the KSN Statement.

6. Click **OK**.

► *To disable KSN:*

1. In the console tree, select the Administration Server for which you need to enable KSN.
2. In the context menu of the Administration Server, select **Properties**.
3. In the Administration Server properties window, in the **KSN Proxy** section, select the **KSN Proxy settings** subsection.
4. Clear the **Use Administration Server as proxy server** check box to disable the KSN Proxy service, or clear the **I agree to use Kaspersky Security Network** check box.

If this check box is cleared, client devices will send no patch installation results to Kaspersky.

If you are using Private KSN, clear the **Configure Private KSN** check box.

KSN will be disabled.

5. Click **OK**.

Viewing the accepted KSN Statement

When you enable Kaspersky Security Network (KSN), you must read and accept the KSN Statement. You can view the accepted KSN Statement at any time.

► *To view the accepted KSN Statement:*

1. In the console tree, select the Administration Server for which you enabled KSN.
2. In the context menu of the Administration Server, select **Properties**.
3. In the Administration Server properties window, in the **KSN Proxy** section, select the **KSN Proxy settings** subsection.

4. Click the **View accepted KSN Statement** link.

In the window that opens, you can view the text of the accepted KSN Statement.

Viewing the KSN proxy server statistics

KSN proxy server is a service that ensures interaction between the Kaspersky Security Network infrastructure and client devices that are managed through the Administration Server.

Using a KSN proxy server provides you the following features:

- Client devices can send requests to KSN and transfer information to KSN even if they do not have direct access to the Internet.
- The KSN proxy server caches processed data, thus reducing the load on the outbound channel and the time period spent for waiting for information requested by a client device.

In the Administration Server properties window, you can configure the KSN proxy server and view statistics on the KSN proxy server usage.

► *To view the statistics of KSN proxy server:*

1. In the console tree, select the Administration Server for which you need to view the KSN statistics.
2. In the context menu of the Administration Server, select **Properties**.
3. In the Administration Server properties window, in the **KSN Proxy** section, select the **KSN Proxy statistics** subsection.

This section displays the statistics of the operation of KSN proxy server. If necessary, perform these additional actions:

- Click **Refresh** to update the statistics on the KSN proxy server usage.
 - Click the **Export to file** button to export the statistics to a CSV file.
 - Click the **Check KSN connection** button to check if the Administration Server is currently connected to KSN.
4. Click the **OK** button to close the Administration Server properties window.

Accepting an updated KSN Statement

You use KSN in accordance with the KSN Statement (see section "Viewing the accepted KSN Statement" on page [788](#)) that you read and accept when you enable KSN. If the KSN Statement is updated, it is displayed to you when you update or upgrade Administration Server. You can accept the updated KSN Statement or decline it. If you decline it, you keep using KSN in accordance with the version of the KSN Statement that you previously accepted.

After updating or upgrading Administration Server, the updated KSN Statement is displayed automatically. If you decline the updated KSN Statement, you still can view and accept it later.

► *To view and then accept or decline an updated KSN Statement:*

1. In the console tree, select the **Administration Server** node.
2. On the **Monitoring** tab, in the **Monitoring** section, click the **The accepted Kaspersky Security Network Statement is obsolete** link.

The **KSN Statement** window opens.

3. Carefully read the KSN Statement, and then make your decision. If you accept the updated KSN Statement, click the **I accept the terms of the License Agreement** button. If you decline the updated KSN Statement, click the **Cancel** button.

Depending on your choice, KSN keeps working in accordance with the terms of the current or updated KSN Statement. You can view the text of the accepted KSN Statement (see section "Viewing the accepted KSN Statement" on page [788](#)) in the properties of Administration Server at any time.

Enhanced protection with Kaspersky Security Network

Kaspersky offers an extra layer of protection to users through the Kaspersky Security Network. This protection method is designed to combat advanced persistent threats and zero-day attacks. Integrated cloud technologies and the expertise of Kaspersky virus analysts make Kaspersky Endpoint Security the unsurpassed choice for protection against the most sophisticated network threats.

Details on enhanced protection in Kaspersky Endpoint Security are available on the Kaspersky website.

Checking whether the distribution point works as KSN Proxy

On a managed device assigned to work as a distribution point, you can enable KSN Proxy. A managed device works as KSN Proxy when the ksnproxy service is running on the device. You can check, turn on, or turn off this service on the device locally.

► *To check whether the distribution point works as KSN Proxy:*

1. On the distribution point device, in Windows, open **Services (All Programs → Administrative Tools → Services)**.
2. In the list of services, check whether the ksnproxy service is running.

If the ksnproxy service is running, then Network Agent on the device participates in Kaspersky Security Network and works as KSN Proxy for the managed devices included in the scope of the distribution point.

If you want, you may turn off the ksnproxy service. In this case, Network Agent on the distribution point stops participating in Kaspersky Security Network. This requires local administrator rights.

Switching between Online Help and Offline Help

If you do not have Internet access, you can use the Offline Help.

► *To switch between Online Help and Offline Help:*

1. In the Kaspersky Security Center main window, in the console tree select the **Kaspersky Security Center 13**.
2. Click the **Global interface settings** link.
The settings window opens.
3. In the settings window, click **Use Offline Help**.
4. Click **OK**.

The settings are applied and saved. If you want, you can change the settings back at any time and start using Online Help at any time.

Exporting events to SIEM systems

This section explains how to export events registered by Kaspersky Security Center to external Security Information and Event Management (SIEM) systems.

About event export

Event export can be used within centralized systems that deal with security issues on an organizational and technical level, provide security monitoring services, and consolidate information from different solutions. These are SIEM systems, which provide real-time analysis of security alerts and events generated by network hardware and applications, or Security Operation Centers (SOCs).

These systems receive data from many sources, including networks, security, servers, databases, and applications. SIEM systems also provide functionality to consolidate monitored data in order to help you avoid missing critical events. In addition, the systems perform automated analysis of correlated events and alerts in order to notify the administrators of immediate security issues. Alerting can be implemented through a dashboard or can be sent through third-party channels such as email.

See also:

Event types	535
Scenario: Installation and initial setup of Kaspersky Security Center 13 Web Console	962
Events in Kaspersky Security Center	792
Event export process	794
Configuring event export in Kaspersky Security Center	795
Exporting events using Syslog	795
Exporting events using CEF and LEEF protocols	800
Exporting events directly from the database	803
Configuring event export in a SIEM system	806
Viewing export results.....	808

Events in Kaspersky Security Center

Kaspersky Security Center allows you to receive information about events that occur during the operation of Administration Server and Kaspersky applications installed on managed devices. Information about events is saved in the Administration Server database. You can export this information to external SIEM systems. Exporting event information to external SIEM systems enables administrators of SIEM systems to promptly respond to security system events that occur on managed devices or groups of devices.

In Kaspersky Security Center there are the following types of events:

- General events. These events occur in all managed Kaspersky applications. An example of a general event is Virus outbreak. General events have strictly defined syntax and semantics. General events are used, for instance, in reports and dashboards.
- Managed Kaspersky applications-specific events. Each managed Kaspersky application has its own set of events.

Each event has its own importance level. Depending on the conditions of its occurrence, an event can be assigned

various importance levels. There are four importance levels of events:

- A *critical event* is an event that indicates the occurrence of a critical problem that may lead to data loss, an operational malfunction, or a critical error.
- A *functional failure* is an event that indicates the occurrence of a serious problem, error or malfunction that occurred during operation of the application or while performing a procedure.
- A *warning* is an event that is not necessarily serious, but nevertheless indicates a potential problem in the future. Most events are designated as warnings if the application can be restored without loss of data or functional capabilities after such events occur.
- An *info* event is an event that occurs for the purpose of informing about successful completion of an operation, proper functioning of the application, or completion of a procedure.

Each event has a defined storage term, during which you can view or modify it in Kaspersky Security Center. Some events are not saved in the Administration Server database by default because their defined storage term is zero. Only events that will be stored in the Administration Server database for at least one day can be exported to external systems.

See also:

Event types	535
-------------------	---------------------

Event export process

The process of exporting events from Kaspersky Security Center to external SIEM systems involves two parties: an event sender, Kaspersky Security Center, and an event receiver, SIEM system. To successfully export events, you must configure this in your SIEM system and in the Kaspersky Security Center Administration Console. It does not matter which side you configure first. You can configure the transmission of events in the Kaspersky Security Center Administration Console and then configure the receipt of events by the SIEM system, or vice versa.

Methods for sending events from Kaspersky Security Center

There are three methods for sending events from Kaspersky Security Center to external systems:

- Sending events over the Syslog protocol to any SIEM system.

Using the Syslog protocol, you can relay any events that occur on the Kaspersky Security Center Administration Server and in Kaspersky applications that are installed on managed devices. When exporting events over the Syslog protocol, you can select exactly which types of events will be relayed to the SIEM system. The Syslog protocol is a standard message-logging protocol. For this reason, you can use the Syslog protocol to export events to any SIEM system.

- Sending events over the CEF and LEEF protocols to QRadar, Splunk, and ArcSight systems.

You can use the CEF and LEEF protocols to export general events (see section "Events in Kaspersky Security Center" on page [792](#)). When exporting events over the CEF and LEEF protocols, you do not have the capability to select specific events to export. Instead, all general events are exported. Unlike the Syslog protocol, the CEF and LEEF protocols are not universal. CEF and LEEF are intended for the appropriate SIEM systems (QRadar, Splunk, and ArcSight). Therefore, when you choose to export events over one of these protocols, you use the required parser in the SIEM system.

To export events over the CEF and LEEF protocols, the Integration with the SIEM systems feature must be activated in Administration Server by using an active license key or valid activation code (see section "Kaspersky applications: licensing and activation" on page [357](#)).

- Directly from the Kaspersky Security Center database to any SIEM system.

This method of exporting events can be used to receive events directly from public views of the database by means of SQL queries. The results of a query are saved to an XML file that can be used as input data for an external system. Only events available in public views can be exported directly from the database.

Receipt of events by the SIEM system

The SIEM system must receive and correctly parse events received from Kaspersky Security Center. For these purposes, you must properly configure the SIEM system. The configuration depends on the specific SIEM system utilized. However, there are a number of general steps in the configuration of all SIEM systems, such as configuring the receiver and the parser.

See also:

Licensing features of Kaspersky Security Center and managed applications[329](#)

Configuring event export in Kaspersky Security Center

To successfully export events, you must configure this in Kaspersky Security Center Administration Console. The Kaspersky Security Center configuration depends on which method you selected for relaying events from Kaspersky Security Center to the SIEM system.

Later sections describe how to configure Kaspersky Security Center if you chose to export events using the following methods:

- Using the Syslog protocol (see section "Exporting events using Syslog" on page [795](#))
- Using the CEF and LEEF protocols (see section "Exporting events using CEF and LEEF protocols" on page [800](#))
- Directly from the Kaspersky Security Center database (see section "Exporting events directly from the database" on page [803](#)). (A set of public views is provided in the Kaspersky Security Center database; you can find the description of these public views in the klakdb.chm (<https://media.kaspersky.com/utilities/CorporateUtilities/klakdb.zip>) document.)

Exporting events using Syslog

You can use the Syslog protocol to export to SIEM systems the events that occur in Administration Server and other Kaspersky applications installed on managed devices.

Syslog is a standard for message logging protocol. It permits separation of the software that generates messages, the system that stores them, and the software that reports and analyzes them. Each message is labeled with a facility code, indicating the software type that generates the message, and is assigned a severity level.

The Syslog protocol is defined by Request for Comments (RFC) documents published by the Internet Engineering Task Force (Internet standards). The RFC 5424 (<https://tools.ietf.org/html/rfc5424>) standard is used to export the events from Kaspersky Security Center to external systems.

In Kaspersky Security Center, you can configure export of the events to the external systems using the Syslog protocol.

The export process consists of two steps:

1. Enabling automatic event export. At this step, Kaspersky Security Center is configured so that it sends events to the SIEM system. Kaspersky Security Center starts sending events immediately after you enable automatic export.
2. Selecting the events to be exported to the external system. At this step, you select which event to export to the SIEM system.

In this section

Before you begin.....	796
Enabling automatic export	796
Selecting export events	797
Selecting events in a policy	797
Selecting events for an application.....	798

Before you begin

When setting up automatic export of events in the Kaspersky Security Center Administration Console, you must specify some of the SIEM system settings. It is recommended that you check these settings in advance in order to prepare for setting up Kaspersky Security Center.

To successfully configure automatic sending of events to a SIEM system, you must know the following settings:

- **SIEM system server address**

The IP address of the server on which the currently used SIEM system is installed. Check this value in your SIEM system settings.

- **SIEM system server port**

Port number used to establish connection between Kaspersky Security Center and your SIEM system server. You specify this value in the Kaspersky Security Center settings and in the receiver settings of your SIEM system.

Protocol Protocol used for transferring messages from Kaspersky Security Center to your SIEM system. You specify this value in the Kaspersky Security Center settings and in the receiver settings of your SIEM system.

Enabling automatic export

The first step of configuring the export of events over the Syslog protocol is to enable automatic export to Kaspersky Security Center.

► *To enable automatic export of events using the Syslog protocol:*

1. In the Kaspersky Security Center console tree, select the Administration Server whose events you want to export.
2. In the workspace of the selected Administration Server, click the **Events** tab.
3. Click the drop-down arrow next to the **Configure notifications and event export** link and select **Configure export to SIEM system** in the drop-down list.

The events properties window opens, displaying the **Event export** section.

4. In the **Event export** section, specify the following export settings:

- **Automatically export events to SIEM system database**

Select this check box to enable automatic export of events to SIEM systems. Selecting this check box enables all fields in the **Exporting events** section.

- **SIEM system**

Select the **Syslog (RFC 5424) format** option to relay events over the Syslog protocol.

- **SIEM system server address**

Specify the SIEM system server address. The address can be specified as a DNS or NetBIOS-name or as an IP-address.

- **SIEM system server port**

Specify the port number to connect to the SIEM system server. This port number must be the same as that, which your SIEM system uses to receive the events (see section **Configuring a SIEM system** for details).

- **Protocol**

Select the protocol to be used for transferring messages to the SIEM system. You can select either the TCP/IP or UDP protocol. TCP/IP is more secure because it supports confirmations on receiving the message. UDP is a simpler protocol and is suitable in situations where error checking and correction is either unnecessary or is performed within the application.

- **Maximum message size, in bytes**

Specify the maximum size (in bytes) of one message relayed to the SIEM system. Each event is relayed in one message. If the actual length of a message exceeds the specified value, the message is truncated and data may be lost. The default size is 2048 bytes. This field is available only if you selected the Syslog format in the **SIEM system** field.

5. If you want to export to the SIEM system database the events that occurred after a specified date in the past, click the **Export archive** button and specify the start date for event export. By default, the event export starts immediately after you enable it.
6. Click **OK**.

Automatic export of events is enabled.

After enabling automatic export of events, you must select which events will be exported to the SIEM system.

See also:

Selecting export events	797
-------------------------------	---------------------

Selecting export events

After enabling automatic export of events, you must select which events will be exported to the external SIEM system.

You can configure export of events to an external system based on one of the following conditions:

- *Selecting events in a policy.* If you select events to export in a policy, the SIEM system will receive the selected events that occurred in all applications managed by the specific policy. If exported events were selected in the policy, you will not be able to redefine them for an individual application managed by this policy.
- *Selecting events for an individual application.* If you select events to export for an individual application, the SIEM system will receive only the events that occurred in this application.

Later sections describe how to select events to export in a policy (see section "Selecting events in a policy" on page [797](#)) and for an individual application (see section "Selecting events for an application" on page [798](#)).

Selecting events in a policy

If you want to export events that occurred in all applications managed by a specific policy, select the events to export in the policy. In this case, you cannot select events for an individual application.

► *To select events to export in a policy:*

1. In the Kaspersky Security Center console tree, select the **Policies** node.

2. Right-click to open the context menu of the relevant policy and select **Properties**.
3. In the policy properties window that opens, select the **Event configuration** section.
4. In the list of events that appears, select one or several events that need to be exported to the SIEM system, and click the **Properties** button.

If you need to select all events, click the **Select all** button.

5. In the event properties window that appears, select the **Export to SIEM system using Syslog** check box to enable export for the selected events.

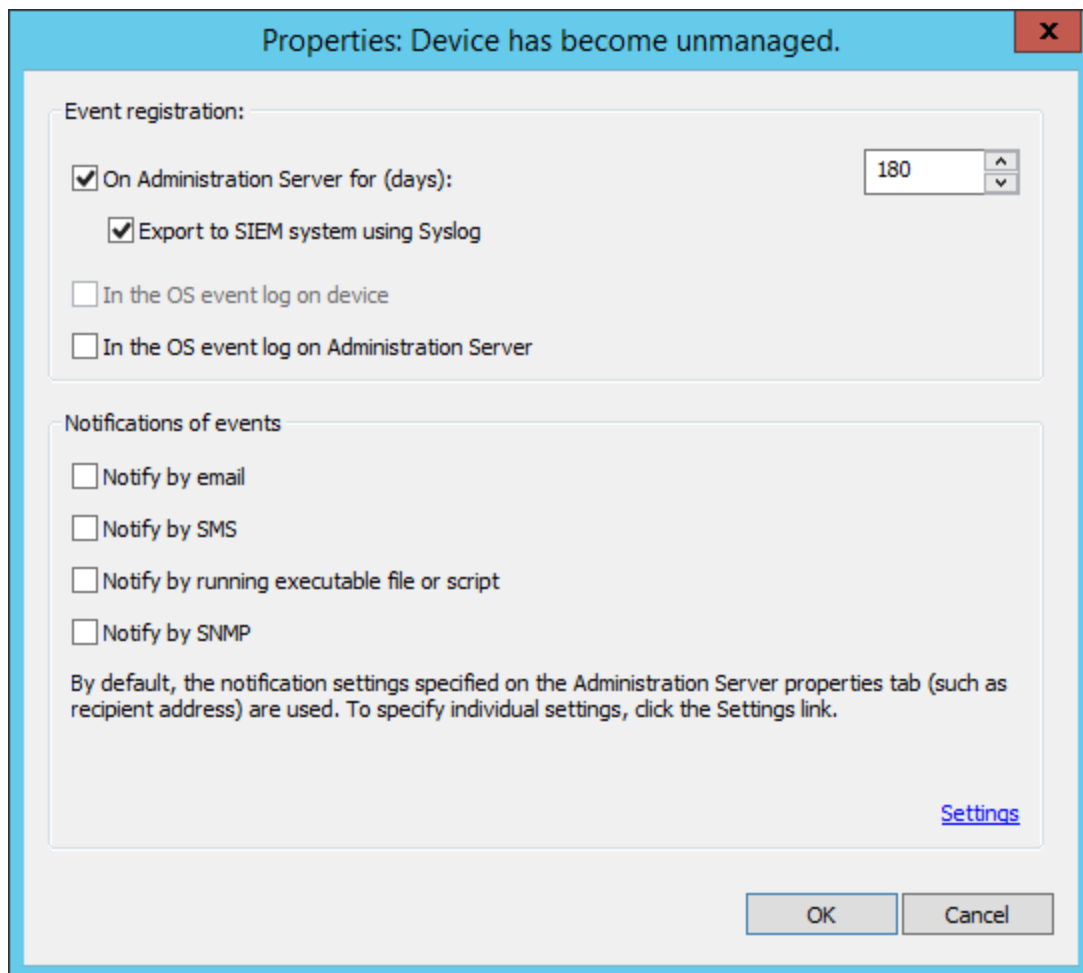


Figure 5. Administration Server event properties window

6. Click **OK** to save the changes.
7. In the policy properties window, click **OK**.

The selected events will be sent to the SIEM system over the Syslog protocol. The export will begin immediately after you enable automatic export and select the events to export. Configure the SIEM system to ensure that it can receive events from Kaspersky Security Center.

Selecting events for an application

If you want to export events that occurred in an individual application, select the events to export for the application. If previously exported events were selected in the policy, you will not be able to redefine the selected events for an individual application managed by this policy.

► *To select the events to export for an individual application:*

1. In the Kaspersky Security Center console tree, select the **Managed devices** node and go to the **Devices** tab.
2. Right-click to open the context menu of the relevant device and select **Properties**.
3. In the device properties window that opens, select the **Applications** section.
4. In the list of applications that appears, select the application whose events you need to export and click the **Properties** button.
5. In the application properties window, select the **Event configuration** section.
6. In the list of events that appears, select one or several events that need to be exported to the SIEM system, and click the **Properties** button.
7. In the event properties window that appears, select the **Export to SIEM system using Syslog** check box to enable export for the selected events.

If event properties are defined in a policy, the fields of this window cannot be edited.

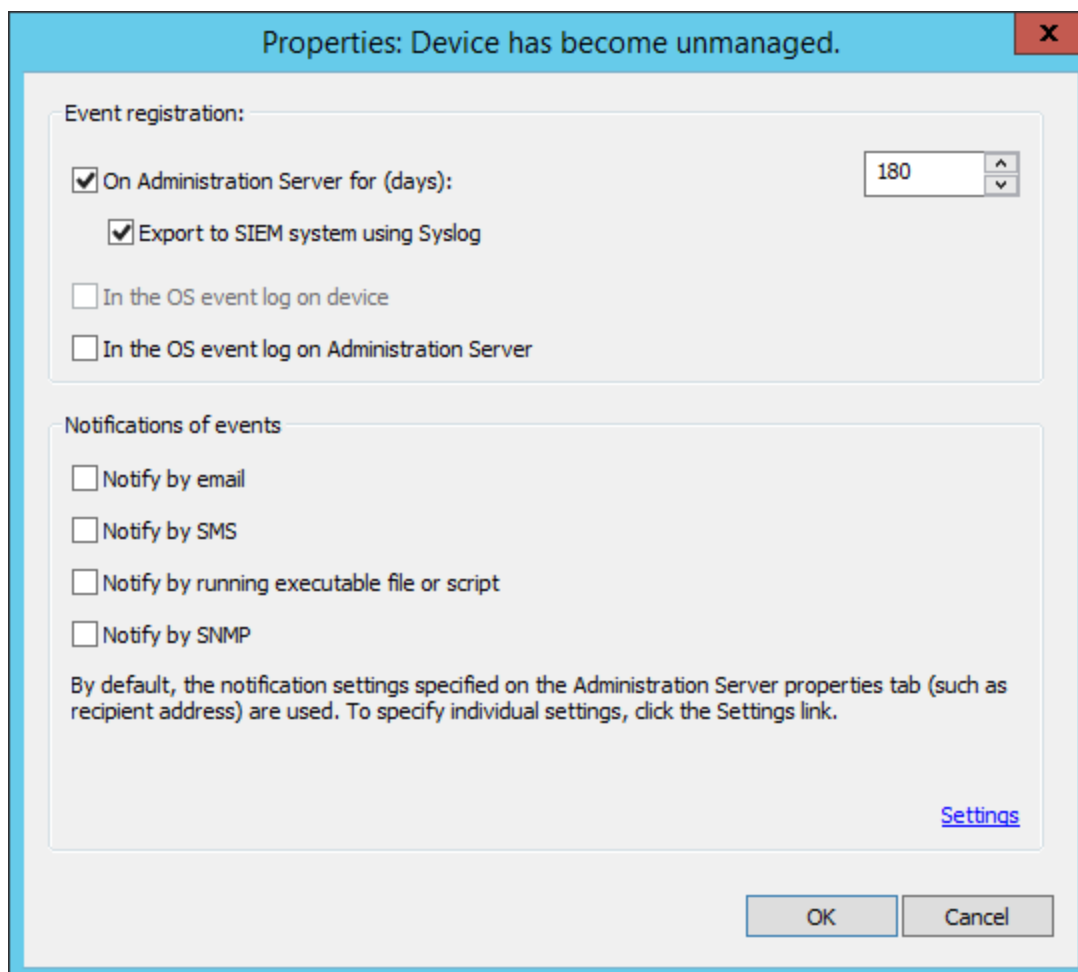


Figure 6. Event properties window

8. Click **OK** to save the changes.

9. Click **OK** in the application properties window and in the device properties window.

The selected events will be sent to the SIEM system over the Syslog protocol. The export will begin immediately after you enable automatic export and select the events to export. Configure the SIEM system to ensure that it can receive events from Kaspersky Security Center.

Exporting events using CEF and LEEF protocols

You can use the CEF and LEEF protocols to export to SIEM systems general events (see section "Events in Kaspersky Security Center" on page 792), as well as the events transferred by Kaspersky applications to the Administration Server. The set of export events is predefined, and you cannot select the events to be exported.

To export events over the CEF and LEEF protocols, the Integration with the SIEM systems feature must be activated in Administration Server by using an active license key or valid activation code (see section "Kaspersky applications: licensing and activation" on page 357).

Select the export protocol on the basis of the SIEM system used. The table below shows SIEM systems and the corresponding export protocols.

Table 69. Protocol of event export to a SIEM system

SIEM system	Export protocol
QRadar	LEEF
ArcSight	CEF
Splunk	CEF

- LEEF (Log Event Extended Format)—A customized event format for IBM® Security QRadar SIEM. QRadar can integrate, identify, and process LEEF events. LEEF events must use UTF-8 character encoding. You can find detailed information on LEEF protocol in IBM Knowledge Center (<http://www.ibm.com/support/knowledgecenter/>).
- CEF (Common Event Format)—An open log management standard that improves the interoperability of security-related information from different security and network devices and applications. CEF enables you to use a common event log format so that data can easily be integrated and aggregated for analysis by an enterprise management system.

Automatic export means that Kaspersky Security Center sends general events to the SIEM system. Automatic export of events starts immediately after you enable it. This section explains in detail how to enable automatic event export.

See also:

Licensing features of Kaspersky Security Center and managed applications	329
Before you begin.....	801
Enabling automatic export of general events	801

Before you begin

When setting up automatic export of events in Kaspersky Security Center Administration Console, you must specify some of the SIEM system settings. It is recommended that you check these settings in advance in order to prepare for setting up Kaspersky Security Center.

To successfully configure automatic sending of events to a SIEM system, you must know the following settings:

- **SIEM system server address**

The IP address of the server on which the currently used SIEM system is installed. Check this value in your SIEM system settings.

- **SIEM system server port**

Port number used to establish connection between Kaspersky Security Center and your SIEM system server. You specify this value in the Kaspersky Security Center settings and in the receiver settings of your SIEM system.

- **Protocol**

Protocol used for transferring messages from Kaspersky Security Center to your SIEM system. You specify this value in the Kaspersky Security Center settings and in the receiver settings of your SIEM system.

Enabling automatic export of general events

Automatic event export using the LEEF and CEF protocols can be enabled in Kaspersky Security Center.

Only general events (see section "Events in Kaspersky Security Center" on page [792](#)) can be exported from managed applications over the CEF and LEEF protocols. Application-specific events (see section "Events in Kaspersky Security Center" on page [792](#)) cannot be exported from managed applications over the CEF and LEEF protocols. If you need to export events of managed applications or a custom set of events that has been configured using the policies of managed applications, export the events over the Syslog protocol.

► *To enable automatic export of events using the CEF, or LEEF protocol:*

1. In the Kaspersky Security Center console tree, select the Administration Server whose events you want to export.
2. In the workspace of the selected Administration Server, click the **Events** tab.
3. Click the drop-down arrow next to the **Configure notifications and event export** link and select **Configure export to SIEM system** in the drop-down list.

The events properties window opens, displaying the **Event export** section.

4. In the **Event export** section, specify the following export settings:

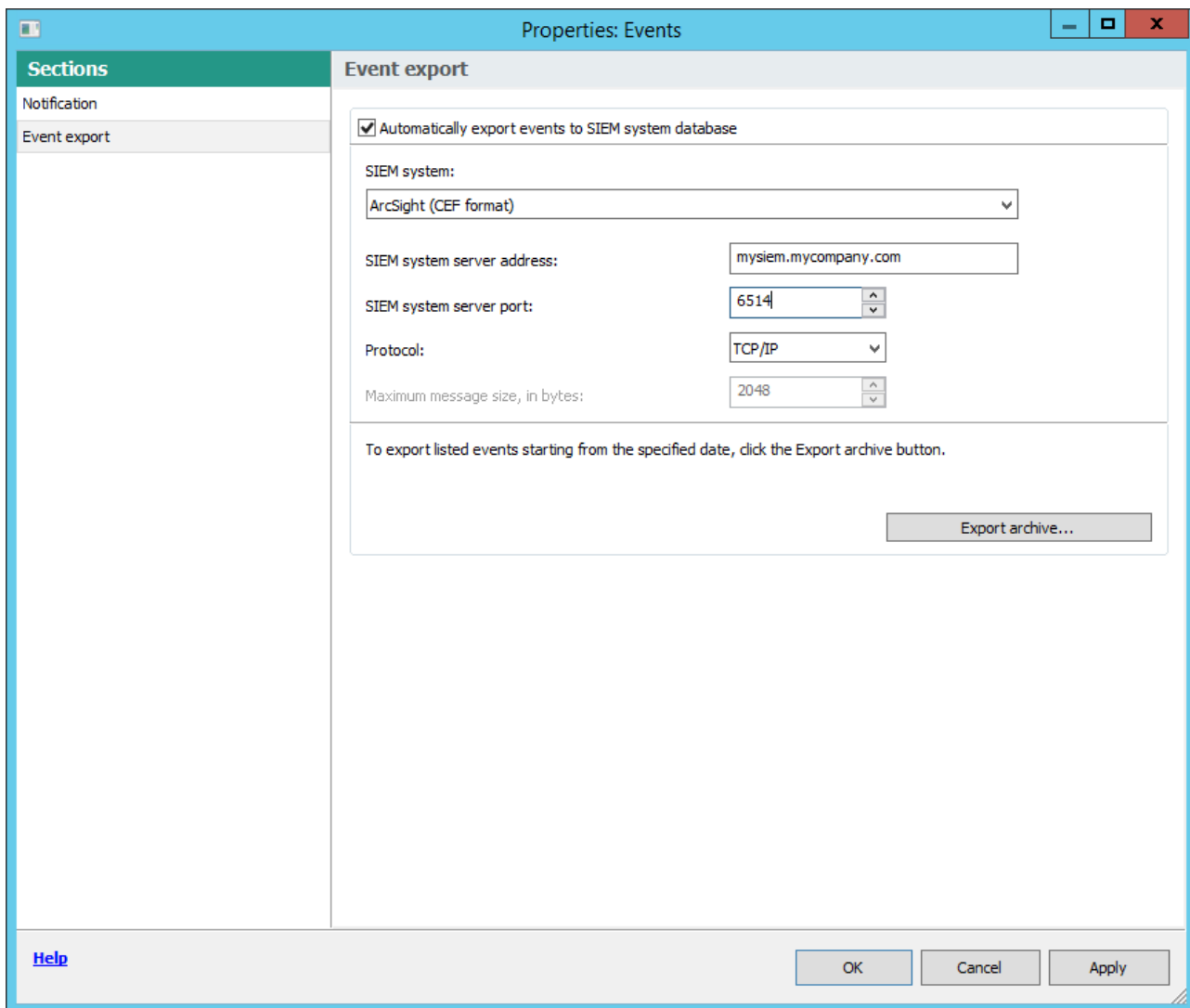


Figure 7. Event export section of the event properties window

- **Automatically export events to SIEM system database**
Select this check box to enable automatic export of events to SIEM systems. Selecting this check box enables all fields in the **Exporting events** section.
- **SIEM system**
Select the SIEM system to export the events: QRadar, Splunk, or ArcSight.
- **SIEM system server address**
Specify the SIEM system server address. The address can be specified as a DNS or NetBIOS-name or as an IP-address.
- **SIEM system server port**
Specify the port number to connect to the SIEM system server. This port number must be the same as that, which your SIEM system uses to receive the events (see section Configuring a SIEM system for details).
- **Protocol**

Select the protocol to be used for transferring messages to the SIEM system. You can select either the TCP/IP or UDP protocol. TCP/IP is more secure because it supports confirmations on receiving the message. UDP is a simpler protocol and is suitable in situations where error checking and correction is either unnecessary or is performed within the application.

5. If you want to export to the SIEM system database the events that occurred after a specified date in the past, click the **Export archive** button and specify the start date for event export. By default, the event export starts immediately after you enable it.
6. Click **OK**.

Automatic export of events will be enabled. The general events will automatically be exported to the external SIEM system.

Exporting events directly from the database

You can retrieve events directly from the Kaspersky Security Center database without having to use the Kaspersky Security Center interface. You can either query the public views directly and retrieve the event data or create your own views on the basis of existing public views and address them to collect the data you need.

Public views

For your convenience, a set of public views is provided in the Kaspersky Security Center database. You can find the description of these public views in the klakdb.chm document.

The v_akpub_ev_event public view contains a set of fields that represent the event parameters in the database. In the klakdb.chm document you can also find information on public views corresponding to other Kaspersky Security Center entities, for example, devices, applications, or users. You can use this information in your queries.

This section contains instructions for creating an SQL query by means of the klsql2 utility and a query example.

To create SQL queries or database views, you can also use any other program for working with databases. Information on how to view the parameters for connecting to the Kaspersky Security Center database, such as instance name and database name, is given in the corresponding section (see section "Viewing the Kaspersky Security Center database name" on page [805](#)).

In this section

Creating an SQL query using the klsql2 utility.....	803
Example of an SQL query in the klsql2 utility.....	804
Viewing the Kaspersky Security Center database name.....	805

Creating an SQL query using the klsql2 utility

This section describes how to download and use the klsql2 utility, and how to create an SQL query by using this utility. When you create an SQL query by means of the klsql2 utility, you do not have to provide database name and access parameters, because the query addresses Kaspersky Security Center public views directly.

► *To download and use the klsql2 utility:*

1. Download the klsql2 utility (<https://media.kaspersky.com/utilities/CorporateUtilities/klsql2.zip>) from Kaspersky website.
2. Copy and extract the downloaded klsql2.zip file to any folder on the device with Kaspersky Security Center Administration Server installed.

The klsql2.zip package includes the following files:

- klsql2.exe
 - src.sql
 - start.cmd
3. Open the src.sql file in any text editor.
 4. In the src.sql file, type the SQL query that you want, and then save the file.
 5. On the device with Kaspersky Security Center Administration Server installed, in the command line, type the following command to run the SQL query from the src.sql file and save the results to the result.xml file:

```
klsql2 -i src.sql -o result.xml
```

6. Open the newly created result.xml file to view the query results.

You can edit the src.sql file and create any query to the public views. Then, from the command line, execute your query and save the results to a file.

Example of an SQL query in the klsql2 utility

This section shows an example of an SQL query, created by means of the klsql2 utility.

The following example illustrates retrieval of the events that occurred on devices during the last seven days, and display of the events ordered by the time they occur, the most recent events are displayed first.

Example:

```
SELECT
e.nId, /* event identifier */
e.tmRiseTime, /* time, when the event occurred */
e.strEventType, /* internal name of the event type */
e.wstrEventTypeDisplayName, /* displayed name of the event */
e.wstrDescription, /* displayed description of the event */
e.wstrGroupName, /* name of the group, where the device is located */
h.wstrDisplayName, /* displayed name of the device, on which the event
occurred */
CAST((h.nIp / 16777216) & 255) AS varchar(4)) + '.' +
CAST((h.nIp / 65536) & 255) AS varchar(4)) + '.' +
CAST((h.nIp / 256) & 255) AS varchar(4)) + '.' +
CAST((h.nIp) & 255) AS varchar(4)) as strIp /* IP-address of the
device, on which the event occurred */
FROM v_akpub_ev_event e
INNER JOIN v_akpub_host h ON h.nId=e.nHostId
WHERE e.tmRiseTime>=DATEADD(Day, -7, GETUTCDATE())
ORDER BY e.tmRiseTime DESC
```

Viewing the Kaspersky Security Center database name

If you want to access Kaspersky Security Center database by means of the SQL Server, MySQL, or MariaDB database management tools, you must know the name of the database in order to connect to it from your SQL script editor.

► *To view the name of the Kaspersky Security Center database:*

1. In the Kaspersky Security Center console tree, open the context menu of the **Administration Server** folder and select **Properties**.
2. In the Administration Server properties window, in the Sections pane select **Advanced** and then **Details of current database**.
3. In the **Details of current database** section, note the following database properties (see figure below).
 - **Instance name**
Name of the current Kaspersky Security Center database instance. The default value is `.KAV_CS_ADMIN_KIT`.
 - **Database name**

Name of the Kaspersky Security Center SQL database. The default value is *KAV*.

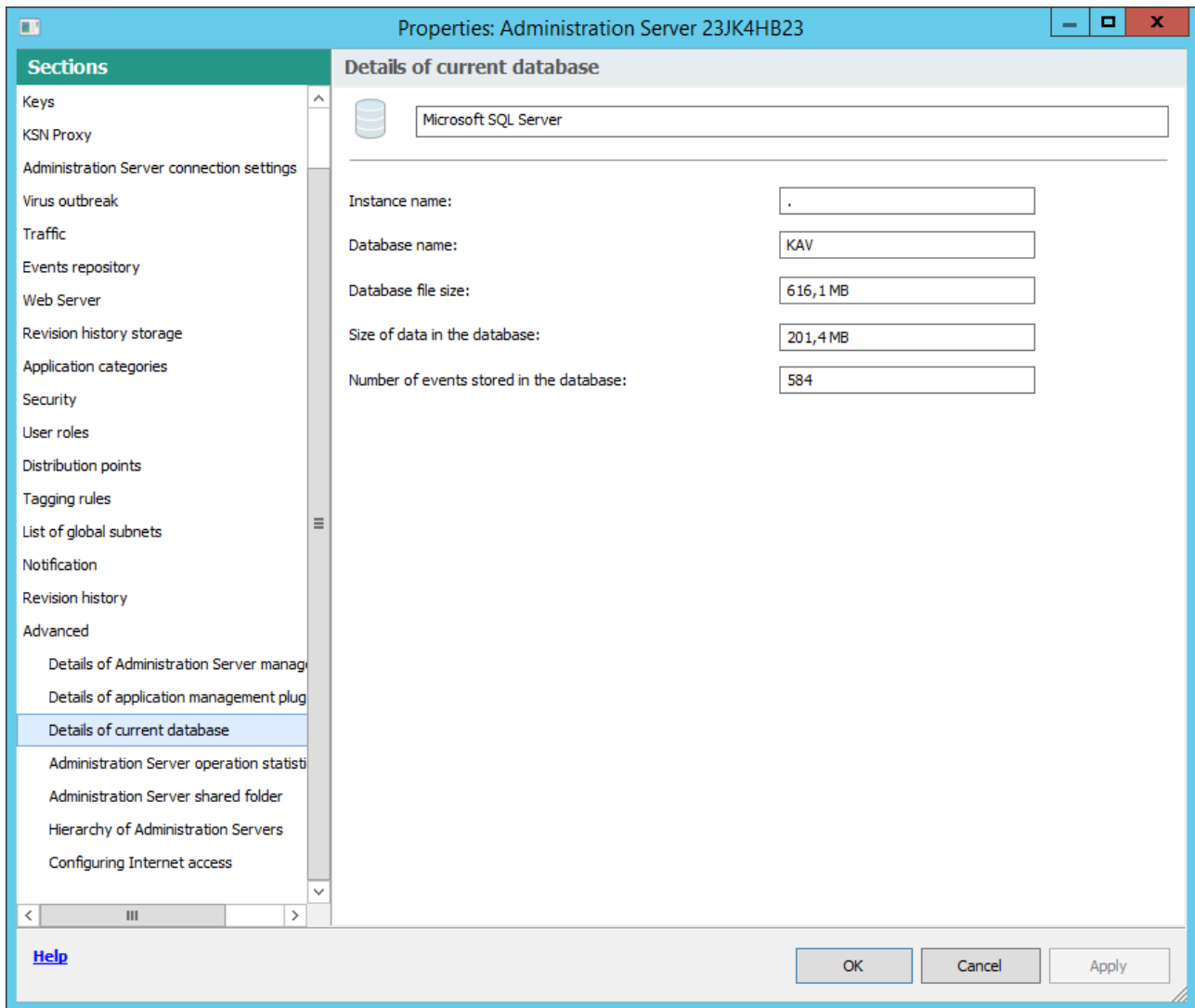


Figure 8. Section with information about the current Administration Server database

4. Click the **OK** button to close the Administration Server properties window.

Use the database name to address the database in your SQL queries.

Configuring event export in a SIEM system

The process of exporting events from Kaspersky Security Center to external SIEM systems involves two parties: an event sender—Kaspersky Security Center and an event receiver—SIEM system. You must configure the export of events in your SIEM system and in the Kaspersky Security Center Administration Console.

The settings that you specify in the SIEM system depend on the particular system that you are using. Generally, for all SIEM systems you must set up a receiver and, optionally, a message parser to parse received events.

Setting up the receiver

To receive events sent by Kaspersky Security Center, you must set up the receiver in your SIEM system. In

general, the following settings must be specified in the SIEM system:

- **Export protocol or input type**

It is the message transfer protocol, either TCP/IP or UDP. This protocol must be the same as the protocol you specified in Kaspersky Security Center.

- **Port**

Port number to connect to Kaspersky Security Center. This port must be the same as the port you specified in Kaspersky Security Center.

- **Message protocol or source type**

The protocol used to export events to the SIEM system. It can be one of the standard protocols: Syslog, CEF, or LEEF. The SIEM system selects the message parser according to the protocol you specify.

Depending on the SIEM system used, you may have to specify some additional receiver settings.

The following figure shows the receiver setup screen in ArcSight.

The screenshot shows the 'Edit Receiver' configuration page in the ArcSight Logger interface. The page has a navigation bar at the top with 'hp ArcSight Logger' and tabs for 'Summary', 'Analyze', 'Dashboards', 'Configuration', and 'System Admin'. Below the navigation bar, the title 'Edit Receiver' is displayed. A note states: 'If a source type that you need does not exist in the Source Type dropdown list below, go to the [Source Types](#) page to add it.' The configuration fields are: 'Name' (text input: tcp cef), 'IP/Host' (dropdown: All), 'Port' (text input: 616), 'Encoding' (dropdown: UTF-8), 'Source Type' (dropdown: CEF), and 'Enable' (checkbox: checked). At the bottom, there are 'Save' and 'Cancel' buttons.

Figure 9. Receiver setup in ArcSight

Message parsers

Exported events are passed to SIEM systems as messages. These messages must be properly parsed so that information on the events can be used by the SIEM system. Message parsers are a part of the SIEM system; they are used to split the contents of the message into the relevant fields, such as event ID, severity, description, parameters and so on. This enables the SIEM system to process events received from Kaspersky Security Center so that they can be stored in the SIEM system database.

Each SIEM system has a set of standard message parsers. Kaspersky also provides message parsers for some SIEM systems, for example, for QRadar and ArcSight. You can download these message parsers from the

websites of the corresponding SIEM systems. When configuring the receiver, you can select to use one of the standard message parsers or a message parser from Kaspersky.

Viewing export results

You can control for successful completion of the event export procedure. To do this, check whether messages with export events are received by your SIEM system.

If the events sent from Kaspersky Security Center are received and properly parsed by your SIEM system, configuration on both sides is done properly. Otherwise, check the settings you specified in Kaspersky Security Center against the configuration in your SIEM system.

The figure below shows the events exported to ArcSight. The first event is expanded, so that you can see that it is a critical Administration Server event: "*Device status is Critical*".

The representation of export events in the SIEM system varies according to the SIEM system you use.

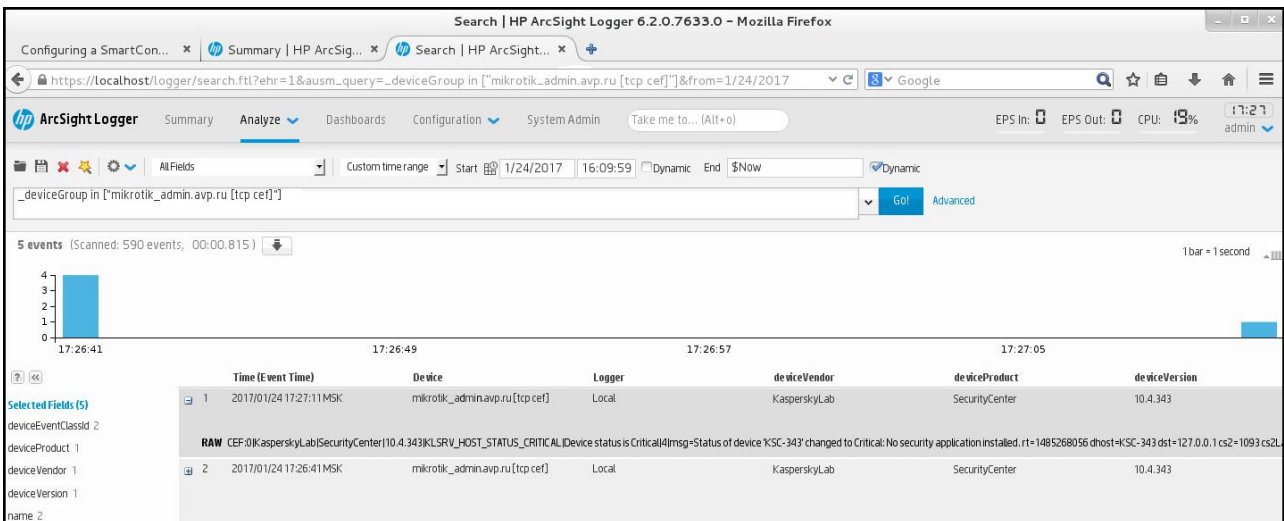


Figure 10. Example of events

Using SNMP for sending statistics to third-party applications

This section describes how to get information from Administration Server by using Simple Network Management Protocol (SNMP) in Windows. Kaspersky Security Center contains SNMP agent, which transfers statistics of Administration Server performance to side applications using OIDs.

This section also contains information on resolving problems that you might encounter while using SNMP for Kaspersky Security Center.

In this chapter

SNMP agent and object identifiers	809
Getting a string counter name from an object identifier.....	809
Values of object identifiers for SNMP	810
Troubleshooting	818

SNMP agent and object identifiers

For Kaspersky Security Center, SNMP agent is implemented as a dynamic library `kl SNMPag.dll`, which is registered by the installer during Administration Server installation. SNMP agent works inside the `snmp.exe` process (that is a Windows service). Third-party applications use SNMP to receive statistics, which comes in the form of counters, on Administration Server performance.

Each counter has a unique *object identifier* (also referred to as OID). An object identifier is a sequence of numbers divided by dots. The object identifiers of Administration Server start with the 1.3.6.1.4.1.23668.1093 prefix. The OID of the counter is a concatenation of that prefix with a suffix describing the counter. For example, the counter with the OID value of 1.3.6.1.4.1.23668.1093.1.1.4 has the suffix with value of 1.1.4.

You can use an SNMP client (such as Zabbix) to monitor the state of your system. In order to get the information, you can search for a value of OID that corresponds to the information and enter that value into your SNMP client. Then your SNMP client will return you another value that characterizes the status of your system.

The list of counters and counter types is in the `adminkit.mib` file on the Administration Server. *MIB* stands for Management Information Base. You can import and parse `.mib` files via the MIB Viewer application that is designed for requesting and displaying the counter values.

Getting a string counter name from an object identifier

In order to use an object identifier (OID) for transferring information to third-party applications, you may need to get a string counter name from that OID.

► *To get a string counter name from an OID:*

1. Open the `adminkit.mib` file, that is located on the Administration Server, in a text editor.
2. Locate the namespace describing the first value (from left to right).

For example, for 1.1.4 OID suffix would be "counters" (::= { kladminkit 1 }).

3. Locate the namespace describing the second value.

For example, for 1.1.4 OID suffix would be `counters 1`, which stands for `deployment`.

4. Locate the namespace describing the third value.

For example, for 1.1.4 OID suffix would be `deployment 4`, which stands for `hostsWithAntivirus`.

The string counter name is the concatenation of these values, for example, `<MIB base namespace>.counters.deployment.hostsWithAntivirus`, and it corresponds to the OID with the value of 1.3.6.1.4.1.23668.1093.1.1.4.

Values of object identifiers for SNMP

The table below shows the values and descriptions of the objects identifiers, or OID, that are used for transferring information on Administration Server performance to third-party applications.

Table 70. Values and descriptions of object identifiers for SNMP

Value of object identifier	Numeric data type	OID	Description
deploymentStatus	INTEGER { ok(0), info(1), warning(2), critical(3) }	.1.3.6.1.4.1.2366 8.1093.1.1.1	Deployment status. The status can be one of the following: <ul style="list-style-type: none"> • Info. License is not valid for N devices anymore. • Warning. One of the following: <p>There are M devices with Kaspersky applications installed on a total of N devices in Administration Server groups (N > M). License L expires on N devices in M days. Task T of installing applications has been successfully finished on N devices, reboot is needed for M devices.</p> • Critical. License expired for N devices. • OK. None of the above.
noAntivirusSoftware	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.2366 8.1093.1.1.2.1	The reason <code>deploymentStatus</code> shows that the Administration Server group contains too many devices without managed applications. Value equals 1 in case a few devices were found without managed applications, and 0 otherwise.
remoteInstallTaskFailed	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.2366 8.1093.1.1.2.2	The reason <code>deploymentStatus</code> shows that the task of the remote installation has failed on some devices. The number of those devices can be obtained via <code>hostsRemoteInstallFailed</code> .
licenceExpiring	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.2366 8.1093.1.1.2.3	The reason <code>deploymentStatus</code> shows that there are some devices with a license expiring in the next 7 days. The number of those devices can be obtained via <code>hostsLicenseExpiring</code> .

Value of object identifier	Numeric data type	OID	Description
licenceExpired	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.2366 8.1093.1.1.2.4	The reason <code>deploymentStatus</code> shows that there are some devices with an expired license. You can obtain the number of those devices via <code>hostsLicenseExpired</code> .
hostsInGroups	Counter32	.1.3.6.1.4.1.2366 8.1093.1.1.3	Number of devices in Administration Server groups.
hostsWithAntivirus	Counter32	.1.3.6.1.4.1.2366 8.1093.1.1.4	Number of devices in Administration Server groups with managed applications installed.
hostsRemoteInstallFailed	Counter32	.1.3.6.1.4.1.2366 8.1093.1.1.5	Number of devices on which the task of the remote installation failed.
licenceExpiringSerial	OCTET STRING	.1.3.6.1.4.1.2366 8.1093.1.1.6	ID of a license key that expires soon (in less than 7 days).
licenceExpiredSerial	OCTET STRING	.1.3.6.1.4.1.2366 8.1093.1.1.7	ID of the expired license key.
licenceExpiringDays	Unsigned32	.1.3.6.1.4.1.2366 8.1093.1.1.8	Number of days before a license expires.
hostsLicenceExpiring	Counter32	.1.3.6.1.4.1.2366 8.1093.1.1.9	Number of devices with a license that expires soon (in less than 7 days).
hostsLicenceExpired	Counter32	.1.3.6.1.4.1.2366 8.1093.1.1.10	Number of devices with an expired license.
updatesStatus	INTEGER { ok(0), info(1), warning(2), critical(3) }	.1.3.6.1.4.1.2366 8.1093.1.2.1	Current status of Anti-virus bases. The status can be one of the following: <ul style="list-style-type: none"> • Info. Administration Server has not been updated in more than 1 day, and less than 1 day had passed since application installation. • Warning. Administration Server has not been updated in more than 1 day. • Critical. Administration Server has not been updated in more than 2 days. • OK. None of the above.

Value of object identifier	Numeric data type	OID	Description
serverNotUpdated	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.2366 8.1093.1.2.2.1	This reason shows that Administration Server was not updated for a log time. The amount of time considered long is specified in <code>updatesStatus</code> .
notUpdatedHosts	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.2366 8.1093.1.2.2.2	This reason shows that some devices were not updated for a long time (7 days or more for Critical and 3 days for Warning). You can obtain the number of those devices via <code>hostsNotUpdated</code> .
lastServerUpdate Time	OCTET STRING	.1.3.6.1.4.1.2366 8.1093.1.2.3	Last time when Anti-virus bases were updated on Administration Server.
hostsNotUpdated	Counter32	.1.3.6.1.4.1.2366 8.1093.1.2.4	Number of devices containing Anti-virus bases that are not updated.
protectionStatus	INTEGER { ok(0), warning(1), critical(2) }	.1.3.6.1.4.1.2366 8.1093.1.3.1	Status of real-time protection. One of the following: <ul style="list-style-type: none"> • Warning. One of the following: A security breach is detected on a device that belongs to the Administration Server group. Encryption errors made some devices change protection status. Full scan has not been performed for a long time. • Critical. Anti-virus protection is not working on some devices in Administration Server groups. • OK. None of the above.
antivirusNotRunning	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.2366 8.1093.1.3.2.1	This reason shows that a security application is not running on some devices. You can obtain the number of those devices via <code>hostsAntivirusNotRunning</code> .

Value of object identifier	Numeric data type	OID	Description
realtimeNotRunning	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.2366 8.1093.1.3.2.2	This reason shows that real-time protection is not running on some devices. You can obtain the number of those devices via <code>hostsRealtimeNotRunning</code> .
notCuredFound	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.2366 8.1093.1.3.2.4	This reason shows that there are devices containing non-disinfected objects. You can obtain the number of those devices via <code>hostsNotCuredObject</code> .
tooManyThreats	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.2366 8.1093.1.3.2.5	This reason shows that there are threats found on some devices. You can obtain the number of those devices via <code>hostsTooManyThreats</code> .
virusOutbreak	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.2366 8.1093.1.3.2.6	This reason shows the virus outbreak status of the system. Value equals 1 if a certain amount of viruses were found during a certain amount of time, and 0 otherwise. Amount of viruses and amount of time are specified on Administration Server, by using the <code>Virus attack</code> settings.
hostsAntivirusNotRunning	Counter32	.1.3.6.1.4.1.2366 8.1093.1.3.3	Number of devices with security applications not running.
hostsRealtimeNotRunning	Counter32	.1.3.6.1.4.1.2366 8.1093.1.3.4	Number of devices with real-time protection not running.
hostsRealtimeLevelChanged	Counter32	.1.3.6.1.4.1.2366 8.1093.1.3.5	Number of devices with real-time protection level not acceptable.
hostsNotCuredObject	Counter32	.1.3.6.1.4.1.2366 8.1093.1.3.6	Number of devices containing non-disinfected objects.
hostsTooManyThreats	Counter32	.1.3.6.1.4.1.2366 8.1093.1.3.7	Number of devices containing threats.

Value of object identifier	Numeric data type	OID	Description
fullscanStatus	INTEGER { ok(0), info(1), warning(2), critical(3) }	.1.3.6.1.4.1.2366 8.1093.1.4.1	Status of Anti-virus full scan. One of the following: <ul style="list-style-type: none"> • Info. Less 7 days have passed since the moment of application installation. • Warning. Anti-virus full scan hasn't been performed for more than 7 days since the moment of application installation. • Critical. Anti-virus full scan hasn't been performed for more than 14 days since the moment of application installation. • OK. None of the above.
notScannedLately	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.2366 8.1093.1.4.2.1	This reason shows that some devices have not been scanned for a certain amount of time. You can obtain the number of those devices via <code>hostsNotScannedLately</code> . The amount of time is specified in <code>fullScanStatus</code> .
hostsNotScannedLately	Counter32	.1.3.6.1.4.1.2366 8.1093.1.4.3	Number of devices that have not been scanned for a certain amount of time. The amount of time is specified in <code>fullScanStatus</code> .
logicalNetworkStatus	INTEGER { ok(0), warning(1), critical(2) }	.1.3.6.1.4.1.2366 8.1093.1.5.1	Status of the logical network of Administration Server. One of the following: <ul style="list-style-type: none"> • Warning. If there are devices with a warning status that can't be accessed or if there are devices that do not belong to any Administration Server group. • Critical. If there are devices whose control has been lost by Administration Server, or if there are devices with a critical status and that cannot be accessed. • OK. None of the above.

Value of object identifier	Numeric data type	OID	Description
notConnectedLongTime	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.2366 8.1093.1.5.2.1	This reason shows that some devices have not been connected to Administration Server for a long time (7 days or more for a device of Warning status and 4 days for a device of Critical status). You can obtain the number of those devices via <code>hostsNotConnectedLongTime</code> .
controlLost	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.2366 8.1093.1.5.2.2	This reason shows that there are devices whose control has been lost by Administration Server. You can obtain the number of those devices via <code>hostsControlLost</code> .
hostsFound	Counter32	.1.3.6.1.4.1.2366 8.1093.1.5.3	Number of devices found by Administration Server that do not belong to any Administration Server groups.
groupsCount	Counter32	.1.3.6.1.4.1.2366 8.1093.1.5.4	Number of groups at Administration Server.
hostsNotConnectedLongTime	Counter32	.1.3.6.1.4.1.2366 8.1093.1.5.5	Number of devices that have not been connected to Administration Server for a long time. The amount of time considered long is specified in <code>notConnectedLongTime</code> .
hostsControlLost	Counter32	.1.3.6.1.4.1.2366 8.1093.1.5.6	Number of devices that are not controlled by Administration Server.

Value of object identifier	Numeric data type	OID	Description
eventsStatus	INTEGER { ok(0), warning(1), critical(2) }	.1.3.6.1.4.1.2366 8.1093.1.6.1	Status of events subsystem. One of the following: <ul style="list-style-type: none"> • Warning. One of the following: <p>Devices of Administration Server group have not been searching for Windows updates for a long time.</p> <p>There are devices with status problems.</p> • Critical. One of the following: <p>There is an event of "Critical" importance on at least one device.</p> <p>There is an event of "Error" importance on at least one device.</p> <p>There is an event of task completing unsuccessfully on at least one device.</p> <p>Devices of Administration Server group have not been searching for Windows updates for a long time.</p> <p>There are devices with status problems.</p> • OK. None of the above.
criticalEventOccurred	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.2366 8.1093.1.6.2.1	The reason <code>eventsStatus</code> shows that there are some critical events on Administration Server. You can obtain the number of those events via <code>criticalEventsCount</code> . Value equals 1 if there is at least one critical event on any device, and 0 otherwise.
criticalEventsCount	Counter32	.1.3.6.1.4.1.2366 8.1093.1.6.3	Number of critical events on Administration Server.

Troubleshooting

This section lists solutions for a few typical issues that you might encounter while using the SNMP service.

Third-party application can not connect to the SNMP service

Make sure that SNMP support is installed in Windows. SNMP support is disabled by default.

► *To allow SNMP support in Windows 10:*

1. Navigate to **Control Panel**.
2. Open the **Add or Remove Programs** menu.
3. Click **Turn Windows features on or off**.
4. In the Windows features list, navigate to the SNMP feature, and then click **OK**.
5. Navigate to **Control Panel** → **Administrative Tools** → **Services**.
6. Choose the SNMP service and run it.
7. Check if listening works by testing it with `netstat`, for a standard UDP-port.

SNMP support is allowed in Windows 10.

SNMP service is working, yet the third-party application cannot get any values

Allow SNMP agent tracing and make sure that a non-empty file is created. This means that the SNMP agent is properly registered and functioning. After this, allow connections from the SNMP service in the side service settings. If a side service operates on the same host as the SNMP agent, the list of IP addresses should contain either the IP address of that host or `loopback 127.0.0.1`.

An SNMP service that communicates with agents should be running in Windows. You can specify the paths to SNMP agents in the Windows Registry via `regedit`.

- For Windows 10:
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\ExtensionAgents]
- For Windows Vista and Windows Server 2008:
[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SNMP\Parameters\ExtensionAgents]

You can allow SNMP agent tracing via `regedit` as well.

- For x86:
[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\SNMP\Debug]
- For x64:
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\SNMP\Debug]
"TraceLevel"=dword:00000004
"TraceDir"="C:\\"

Values do not match the statuses of Administration Console

In order to reduce the load at Administration Server, the caching of values is implemented for the SNMP agent. The latency between the cache being actualized and the values being changed on the Administration Server may cause mismatches between the values returned by the SNMP agent and the actual ones. When working with third-party applications, you should consider that possible latency.

Working in a cloud environment

This section provides information about Kaspersky Security Center deployment and maintenance in cloud environments, such as Amazon Web Services, Microsoft Azure, or Google Cloud.

The addresses of web pages cited in this document were correct as of March 2021.

See also:

Scenario: Installation and initial setup of Kaspersky Security Center 13 Web Console	962
About work in a cloud environment	820
Scenario: Deployment for cloud environment.....	821
Prerequisites for deploying Kaspersky Security Center in a cloud environment.....	825
Hardware requirements for the Administration Server in a cloud environment.....	826
Licensing options in a cloud environment.....	826
Database options for work in a cloud environment	827
Working in Amazon Web Services cloud environment.....	828
Working in Microsoft Azure cloud environment	842
Working in Google Cloud.....	849
Prerequisites for client devices in a cloud environment necessary for work with Kaspersky Security Center	852
Cloud Environment Configuration Wizard	853
Checking configuration	864
Cloud device group.....	865
Network segment polling	865
Installing applications on devices in a cloud environment.....	870
Viewing the properties of cloud devices	872
Synchronization with cloud	873
Using deployment scripts for deploying security applications	876
Deployment of Kaspersky Security Center in Yandex.Cloud	877

About work in a cloud environment

Kaspersky Security Center 13 not only works with on-premises devices, but also provides special features for working in a cloud environment. Kaspersky Security Center works with the following virtual machines:

- Amazon EC2 instances (hereinafter, also referred to as *instances*). An Amazon EC2 instance is a virtual machine that is created on the basis of the Amazon Web Services (AWS) platform. Kaspersky Security Center uses *AWS API* (Application Programming Interface).
- Microsoft Azure virtual machines. Kaspersky Security Center uses Azure API.
- Google Cloud virtual machines instances. Kaspersky Security Center uses Google API.

You can deploy Kaspersky Security Center on an instance or a virtual machine to manage protection of devices in a cloud environment and to use special features of Kaspersky Security Center for work in a cloud environment. These features include:

- Using API tools to poll devices in a cloud environment
- Using API tools to install Network Agent and security applications on devices in a cloud environment
- Searching devices based on whether they belong to a specific cloud segment

You can also use an instance or a virtual machine on which a Kaspersky Security Center Administration Server is deployed to protect on-premises devices (for example, if a cloud server turns out to be easier for you to service and maintain than a physical one). If this is the case, you work with the Administration Server in the same way that you would if the Administration Server were installed on an on-premises device.

In a Kaspersky Security Center that has been deployed from a paid Amazon Machine Image (AMI) (in AWS) or a usage-based monthly billed SKU (in Azure), Vulnerability and Patch Management (including integration with SIEM systems) is automatically activated; Mobile Device Management cannot be activated.

The Administration Server is installed together with Administration Console. Kaspersky Security for Windows Server is also automatically installed on the device on which the Administration Server is installed.

You can use Cloud Environment Configuration Wizard (on page [853](#)) to configure Kaspersky Security Center, taking into account the specifics of working in a cloud environment.

See also:

Scenario: Deployment for cloud environment.....[821](#)

Scenario: Deployment for cloud environment

This section describes the deployment of Kaspersky Security Center for working in cloud environments such as Amazon Web Services, Microsoft Azure, and Google Cloud.

After you finish the deployment scenario, Kaspersky Security Center Administration Server (see section "Administration Server" on page [44](#)) and Administration Console are started and configured with the default parameters. Anti-Virus protection managed by Kaspersky Security Center is deployed on the selected Amazon EC2 instances or Microsoft Azure virtual machines. You can then fine-tune the configuration of Kaspersky Security Center, create a complex structure of administration groups, and create various policies and tasks for groups.

The deployment of Kaspersky Security Center for working in cloud environments consists of the following parts:

1. Preparation work
2. Deploying Administration Server

3. Installing Kaspersky anti-virus applications on virtual devices that need to be protected
4. Configuring the update download settings
5. Configuring the settings for managing reports about the protection status of devices

The Cloud Environment Configuration Wizard (on page [853](#)) is intended for performing the initial configuration. It starts automatically the first time that Kaspersky Security Center is deployed from a ready-to-use image. You can manually start the Wizard at any time. In addition, you can manually perform all of the actions that the Wizard performs.

We recommend that you plan for a minimum of one hour for deploying Kaspersky Security Center Administration Server in the cloud environment and at least one working day for protection deployment in the cloud environment.

Deployment of Kaspersky Security Center in the cloud environment proceeds in stages:

a. Planning the configuration of cloud segments

Learn how Kaspersky Security Center works in a cloud environment (see section "About work in Amazon Web Services cloud environment" on page [829](#)). Plan where Administration Server will be deployed (inside or outside of the cloud environment); and determine how many cloud segments you plan to protect. If you are planning to deploy Administration Server outside of the cloud environment or if you are planning to protect more than 5000 devices, you will need to install Administration Server manually.

To work with Google Cloud, you can only install Administration Server manually.

b. Planning the resources

Make sure that you have everything that is required for deployment (see section "Prerequisites for deploying Kaspersky Security Center in a cloud environment" on page [825](#)).

c. Subscribing to Kaspersky Security Center as a ready-to-use image

Select one of the ready-to-use AMIs at AWS Marketplace or select a Usage-based monthly billed SKU at Azure Marketplace, pay for it according to marketplace rules if necessary (or use the BYOL model), and then use the image to deploy an Amazon EC2 instance / Microsoft Azure virtual machine with Kaspersky Security Center installed.

This stage is necessary only if you plan to deploy Administration Server on an instance / virtual machine within a cloud environment and you are also planning to deploy protection for no more than 5000 devices. Otherwise, this stage is not necessary and instead you manually have to install Administration Server, Administration Console, and the DBMS (see section "Main installation scenario" on page [59](#)).

This step is unavailable for Google Cloud.

d. Determining the location of the DBMS

Determine where your DBMS will be (see section "Database options for work in a cloud environment" on page [827](#)).

If you plan to use a database outside the cloud environment, make sure that you have a working database.

If you plan to use Amazon Relational Database Service (RDS), create a database with RDS in the AWS cloud environment.

If you plan to use Microsoft Azure SQL DBMS, create a database with the Azure Database service in the Microsoft Azure cloud environment (see section "Working with Azure SQL" on page [846](#)).

If you plan to use Google MySQL, create a database in the Google Cloud (see section "Working with Google Cloud SQL for MySQL instance" on page [850](#)) (Please refer to <https://cloud.google.com/sql/docs/mysql> <https://cloud.google.com/sql/docs/mysql> for details).

e. Installing Administration Server and Administration Console (Microsoft Management Console based and/or web-based) on selected devices manually

Install Administration Server, Administration Console, and the DBMS on the selected devices, as described in the basic deployment scenario for Kaspersky Security Center (see section "Main installation scenario" on page [59](#)).

This stage is necessary if you plan to place Administration Server outside of a cloud environment or if you plan to deploy protection for more than 5000 devices. Then make sure that your Administration Server meets hardware requirements (see section "Hardware requirements for the Administration Server in a cloud environment" on page [826](#)). Otherwise, this stage is not necessary and a subscription to Kaspersky Security Center as a ready-to-use image in AWS Marketplace, Azure Marketplace, or Google Cloud is sufficient.

f. Ensuring that Administration Server has the permissions to work with cloud APIs

In AWS, go to the AWS Management Console and create an IAM role (see section "Creating an IAM role for the Administration Server" on page [830](#)) or an IAM user account (see section "Creating an IAM user account for work with Kaspersky Security Center" on page [833](#)). The created IAM role (or IAM user account) will allow Kaspersky Security Center to work with the AWS API: Poll cloud segments and deploy protection.

In Azure, create a subscription and an Application ID with password (see section "Creating a subscription, Application ID, and password" on page [843](#)). Kaspersky Security Center uses these credentials to work with the AWS API: Poll cloud segments and deploy protection.

In Google Cloud, register a project, get your project ID and a private key (see section "Creating client email, project ID, and private key" on page [849](#)). Kaspersky Security Center uses these credentials to poll cloud segments by using the Google API.

g. Creating an IAM role for protected instances (for AWS only)

In the AWS Management Console, create an IAM role (see section "Creating an IAM role for installation of applications on Amazon EC2 instances" on page [834](#)) that defines the set of permissions for executing requests to AWS. This newly created role will be subsequently assigned to new instances. The IAM role is required in order to use Kaspersky Security Center to install applications on instances.

h. Preparing a database by using Amazon Relational Database Service or Microsoft Azure SQL

If you plan to use Amazon Relational Database Service (RDS (see section "Working with Amazon RDS" on page [835](#))), create an Amazon RDS database instance and an S3 bucket on which the database backup will be stored. You can skip this stage if you want a database on the same EC2 instance where Administration Server is installed or if you want your database to be located somewhere else (see section "Database options for work in a cloud environment" on page [827](#)).

If you plan to use Microsoft Azure SQL, create a storage account (see section "Creating Azure storage account" on page [846](#)) and a database (see section "Creating Azure SQL database and SQL Server" on page [847](#)) in Microsoft Azure.

If you plan to use Google MySQL, configure your database in the Google Cloud. (Please refer to <https://cloud.google.com/sql/docs/mysql> <https://cloud.google.com/sql/docs/mysql> for details.)

i. Licensing Kaspersky Security Center for working in the cloud environment

Make sure that you have licensed (see section "Licensing options in a cloud environment" on page [826](#)) Kaspersky Security Center to work in the cloud environment and provide an activation code or key file so that the application can add it to license storage. This stage can be completed in the Cloud Environment Configuration Wizard (see section "Step 1. Selecting the application activation method" on page [855](#)).

This stage is required if you are using Kaspersky Security Center installed from a free ready-to-use AMI based on the BYOL model or if you are manually installing Kaspersky Security Center without the use of AMIs. In each of these cases, you will need a license for Kaspersky Security for Virtualization or a license for Kaspersky Hybrid Cloud Security, to activate Kaspersky Security Center.

If you are using Kaspersky Security Center installed from a ready-to-use image, this stage is not necessary and the corresponding window of the Cloud Environment Configuration Wizard is not displayed.

j. Authorization in the cloud environment

Provide Kaspersky Security Center with your AWS, Azure, or Google Cloud credentials so that Kaspersky Security Center can operate with the necessary permissions. This stage can be completed in the Cloud Environment Configuration wizard (see section "Step 3. Authorization in the cloud environment" on page [856](#)).

k. Polling a cloud segment so that Administration Server can receive information about devices in the cloud segment

Start cloud segment polling (see section "Network segment polling" on page [865](#)). In the AWS environment, Kaspersky Security Center will receive the addresses and names of all instances that can be accessed, based on the permissions of the IAM role or IAM user. In the Microsoft Azure environment, Kaspersky Security Center will receive the addresses and names of all virtual machines that can be accessed, based on the permissions of the Reader role.

You can then use Kaspersky Security Center to install Kaspersky applications and software from other vendors on the detected instances or virtual machines.

Kaspersky Security Center regularly starts a poll, which means that new instances or virtual machines are automatically detected.

l. Combining all network devices into the Cloud administration group

Move the discovered instances or virtual machines into the **Managed devices\Cloud** administration group so that they can become available for centralized management. If you want to assign devices to subgroups, for example, depending on which operating system is installed on them, you can create several administration groups within the **Managed devices\Cloud** group. You can enable automatic moving (see section "Creating rules for moving devices to administration groups automatically" on page [313](#)) of all devices that will be detected during routine polls to the **Managed devices\Cloud** group.

m. Using Network Agent to connect networked devices to Administration Server

Install Network Agent on devices in the cloud environment (see section "Installing applications on devices in a cloud environment" on page [870](#)). Network Agent is the Kaspersky Security Center component that provides for communication between devices and Administration Server. Network Agent settings are configured automatically by default.

You can install Network Agent on each device locally (see section "Installing applications on client devices" on page [719](#)). You can also install Network Agent on devices remotely using Kaspersky Security Center (see section "Creating installation packages of applications" on page [717](#)). Or, you can skip this stage and install Network Agent together with the latest versions of the security applications.

n. Installing the latest versions of security applications on networked devices

Select the devices on which you want to install security applications, and then install the latest versions of security applications on those devices (see section "Installing applications on client devices" on page [719](#)). You can perform the installation either remotely using Kaspersky Security Center on Administration Server or locally.

Kaspersky Endpoint Security for Linux is intended for instances and virtual machines running Linux.

Kaspersky Security for Windows Server is intended for instances and virtual machines running Windows.

o. Configuring update settings

The **Find vulnerabilities and required updates** task is created automatically when Cloud Environment Configuration Wizard is run. You can also create the task manually (see section "Scanning applications for

vulnerabilities" on page [464](#)). This task automatically finds and downloads required application updates for subsequent installation to network devices using Kaspersky Security Center tools.

It is recommended to complete the following stage after Cloud Environment Configuration Wizard finishes:

p. Configuring report management

You can view reports (see section "Working with reports" on page [504](#)) on the **Monitoring** tab in the workspace of the **Administration Server** node. You can also receive reports by email. Reports on the **Monitoring** tab are available by default. To configure the receipt of reports by email, specify the email addresses that should receive reports, and then configure the format of reports.

Results

Upon completion of the scenario, you can make sure (see section "Checking configuration" on page [864](#)) that the initial configuration was successful:

- You can connect to Administration Server through Administration Console or Kaspersky Security Center 13 Web Console.
- The latest versions of Kaspersky security applications are installed and running on managed devices.
- Kaspersky Security Center has created the default policies and tasks for all managed devices.

Prerequisites for deploying Kaspersky Security Center in a cloud environment

Before starting deployment of Kaspersky Security Center in the Amazon Web Services or Microsoft Azure cloud environment, make sure that you have the following:

- Internet access
- One of the following accounts:
 - Amazon Web Services account (for work with AWS)
 - Microsoft account (for work with Azure)
 - Google account (for work with Google Cloud)
- One of the following:
 - License for Kaspersky Security for Virtualization
 - License for Kaspersky Hybrid Cloud Security
 - Funds to purchase such a license (Kaspersky Security for Virtualization or Kaspersky Hybrid Cloud Security)
 - Funds to pay for a ready-to-use image at the Azure Marketplace
- Guides for the latest versions of Kaspersky Endpoint Security for Linux and Kaspersky Security for Windows Server

See also:

Scenario: Deployment for cloud environment	821
--	---------------------

Hardware requirements for the Administration Server in a cloud environment

For deployment in cloud environments, the requirements for Administration Server and database server are the same as the requirements for physical Administration Server (depending on how many devices you want to manage). Please refer to the documentation of the cloud environment for details.

See also:

Scenario: Deployment for cloud environment.....[821](#)

Licensing options in a cloud environment

Work in a cloud environment is outside the basic functionality of Kaspersky Security Center and therefore requires a dedicated license.

Two Kaspersky Security Center licensing options are available for working in a cloud environment:

- Paid AMI (in Amazon Web Services) or Usage-based monthly billed SKU (in Microsoft Azure).
This grants a license for Kaspersky Security Center as well as licenses for Kaspersky Endpoint Security for Linux and Kaspersky Security for Windows Server. You have to pay according to Amazon Marketplace or Azure Marketplace rules.

This model lets you have not more than 200 client devices for one Administration Server.

- A free-of-charge, ready-to-use image using a proprietary license, according to the Bring Your Own License (BYOL) model.

For Kaspersky Security Center licensing in AWS or Azure, you must have a license for one of the following applications:

- Kaspersky Security for Virtualization
- Kaspersky Hybrid Cloud Security

The BYOL model lets you have up to 100 000 client devices for one Administration Server. This model also lets you manage devices outside the AWS (or Azure) cloud environment.

You can choose the BYOL model in the following cases:

- you already own a valid license for Kaspersky Security for Virtualization,
- or you already own a valid license for Kaspersky Hybrid Cloud Security,
- or you are willing to purchase a license immediately before deployment of Kaspersky Security Center.

At the stage of initial setup (see section "Step 1. Selecting the application activation method" on page [855](#)), Kaspersky Security Center prompts you for an activation code or key file.

If you choose BYOL, you will not have to pay for Kaspersky Security Center through Azure Marketplace or AWS Marketplace.

In both cases, Vulnerability and Patch Management is automatically activated, and Mobile Device Management cannot be activated.

You may encounter an error when trying to activate the feature Support of the cloud environment using the license for Kaspersky Hybrid Cloud Security.

Upon subscribing to Kaspersky Security Center, you get an Amazon Elastic Compute Cloud (Amazon EC2) instance or a Microsoft Azure virtual machine with Kaspersky Security Center Administration Server. The installation packages for Kaspersky Security for Windows Server and Kaspersky Endpoint Security for Linux are available on the Administration Server. You can install these applications on devices in the cloud environment. You do not have to license these applications.

If a managed device is not visible to the Administration Server for more than a week, the application (Kaspersky Security for Windows Server or Kaspersky Endpoint Security for Linux) on the device will shift to limited functionality mode. To activate the application again, you have to make the device on which the application is installed visible to the Administration Server again.

See also:

Scenario: Deployment for cloud environment.....[821](#)

Database options for work in a cloud environment

You must have a database to work with Kaspersky Security Center. When deploying Kaspersky Security Center in AWS, in Microsoft Azure, or Google Cloud, you have three options:

- Create a local database on the same device with the Administration Server. Kaspersky Security Center comes with a SQL Server Express database that can support up to 5000 managed devices. Choose this option if SQL Server Express Edition is enough for your needs.
- Create a database with the Relational Database Service (RDS) in the AWS cloud environment, or with the Azure Database service in the Microsoft Azure cloud environment (see section "Working with Azure SQL" on page [846](#)). Choose this option if you want a DBMS other than SQL Express. Your data will be transferred inside the cloud environment, where it will remain, and you will not have any extra expenses. If you already work with Kaspersky Security Center on premises and have some data in your database, you can transfer your data to the new database.

For work on Google Cloud Platform, you can only use Cloud SQL for MySQL.

- Use an existing database server. Choose this option if you already have a database server and want to use it for Kaspersky Security Center. If this server is outside the cloud environment, your data will be transferred over the internet, which might result in extra expenses.

The procedure of Kaspersky Security Center deployment in the cloud environment has a special step for creating (choosing) a database.

See also:

Scenario: Deployment for cloud environment.....	821
---	---------------------

Working in Amazon Web Services cloud environment

This section tells you how to prepare for working with Kaspersky Security Center in Amazon Web Services.

The addresses of web pages cited in this document were correct as of March 2021.

In this section

About work in Amazon Web Services cloud environment.....	829
Creating IAM roles and IAM user accounts for Amazon EC2 instances	829
Working with Amazon RDS	835

About work in Amazon Web Services cloud environment

You can purchase Kaspersky Security Center at AWS Marketplace in the form of an Amazon Machine Image (AMI), which is a ready-to-use image of a preconfigured virtual machine. You can subscribe to a paid AMI or BYOL AMI and, based on that image, create an Amazon EC2 instance with Kaspersky Security Center Administration Server installed.

To work with the AWS platform and, in particular, to purchase apps at AWS Marketplace and create instances, you need an Amazon Web Services account. You can create a free account at <https://aws.amazon.com>. You can also use an existing Amazon account.

If you subscribed to an AMI available at AWS Marketplace, you receive an instance with your ready-to-use Kaspersky Security Center. You do not have to install the application yourself. In this case, Kaspersky Security Center Administration Server is installed on the instance without your involvement. After installation, you can start Administration Console and connect to Administration Server to begin working with Kaspersky Security Center.

To learn more about an AMI and how AWS Marketplace works, please visit the AWS Marketplace Help page (<https://aws.amazon.com/marketplace/help>). For more information about working with the AWS platform, using instances, and related concepts, please refer to the Amazon Web Services documentation <https://aws.amazon.com/documentation/>.

The addresses of web pages cited in this document were correct as of March 2021.

See also:

Scenario: Deployment for cloud environment.....	821
Hardware and software requirements	31

Creating IAM roles and IAM user accounts for Amazon EC2 instances

This section describes the actions that must be performed to ensure correct operation of the Administration Server. These actions include work with the AWS Identity and Access Management (IAM) roles and user accounts. Also described are the actions that must be taken on client devices to install Network Agent on them and then install Kaspersky Security for Windows Server and Kaspersky Endpoint Security for Linux.

You can prepare EC2 instances manually, or you can use a script to do it automatically.

In this section

Ensuring that the Kaspersky Security Center Administration Server has the permissions to work with AWS	830
Creating an IAM role for the Administration Server	830
Creating an IAM user account for work with Kaspersky Security Center	833
Creating an IAM role for installation of applications on Amazon EC2 instances.....	834

Ensuring that the Kaspersky Security Center Administration Server has the permissions to work with AWS

The standards for operating in the Amazon Web Services cloud environment prescribe (см. раздел <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html> - <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html>) that a special IAM role (see section "Creating an IAM role for the Administration Server" on page [830](#)) be assigned to the Administration Server instance for working with AWS services. An IAM role is an IAM entity that defines the set of permissions for execution of requests to AWS services. The IAM role provides the permissions for cloud segment polling and installation of applications on instances.

After you create an IAM role and assign it to the Administration Server, you will be able to deploy protection of instances by using this role, without providing any additional information to Kaspersky Security Center.

However, it may be advisable to not create an IAM role for the Administration Server in the following cases:

- The devices whose protection you plan to manage are EC2 instances within the Amazon Web Services cloud environment but the Administration Server is outside of the environment.
- You plan to manage the protection of instances not only within your cloud segment but also within other cloud segments that were created under a different account in AWS. In this case, you will need an IAM role only for the protection of your cloud segment. An IAM role will not be needed to protect another cloud segment.

In these cases, instead of creating an IAM role you will need to create an *IAM user account* (see section "Creating an IAM user account for work with Kaspersky Security Center" on page [833](#)), that will be used by Kaspersky Security Center to work with AWS services. Before starting to work with the Administration Server, create an IAM user account with an *AWS IAM access key* (hereinafter also referred to as *IAM access key*).

Creation of an IAM role or IAM user account requires the AWS Management Console <https://console.aws.amazon.com>. To work with the AWS Management Console, you will need a user name and password from an account in AWS.

See also:

Scenario: Deployment for cloud environment.....	821
---	---------------------

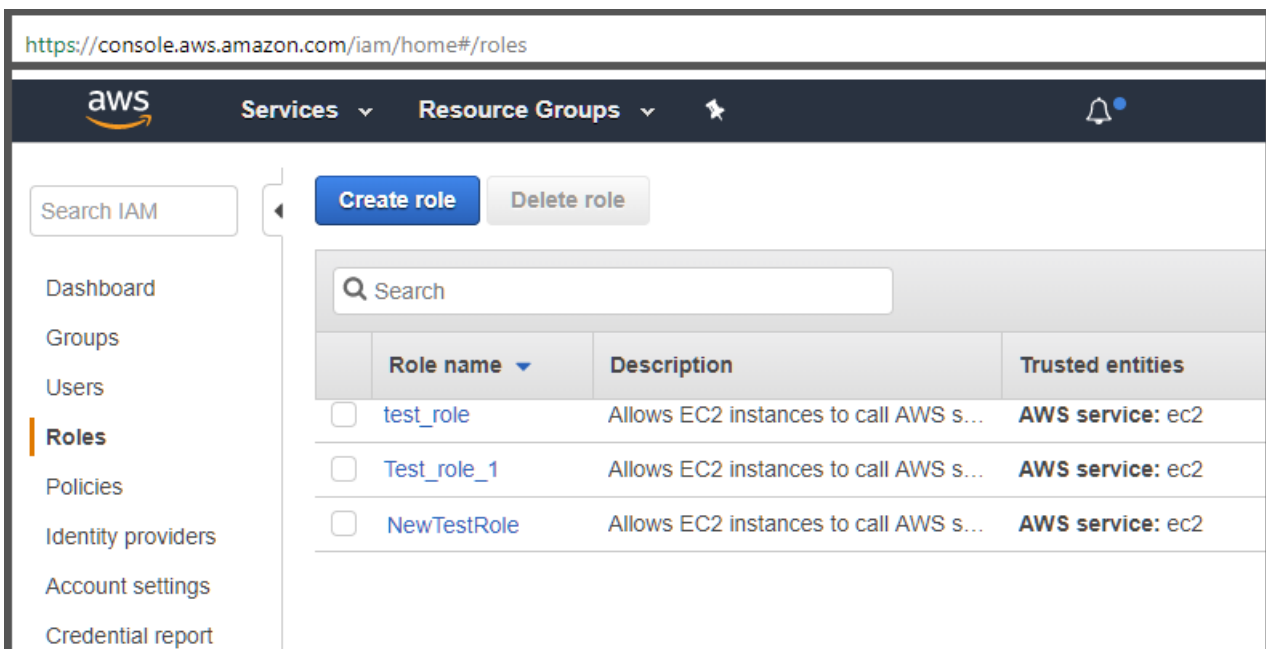
Creating an IAM role for the Administration Server

Before you deploy the Administration Server, in the AWS Management Console (см. раздел AWS console - <https://console.aws.amazon.com/iam>) create an IAM role with permissions required for installation of applications on instances. For more details, see AWS Help https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html sections about IAM roles.

► *To create an IAM role for the Administration Server:*

1. Open the AWS Management Console (см. раздел IAM console - <https://console.aws.amazon.com/iam/home>) and log in under your AWS account.
2. Proceed to the **Roles** section.
3. Click the **Create Role** button.
4. In the list of services that appears, select **EC2** and then in the **Select Your Use Case** list select **EC2** again.
5. Click the **Next: Permissions** button.
6. In the list that opens, select the following check box(es):
 - Next to **AmazonEC2ReadOnlyAccess**, if you plan to only run cloud segment polling and do not plan to install applications on EC2 instances using AWS API.
 - Next to **AmazonEC2ReadOnlyAccess** and **AmazonSSMFullAccess**, if you plan to run cloud segment polling and install applications on EC2 instances using AWS API. In this case, you will also need to assign an IAM role with the AmazonEC2RoleforSSM permission (see section "Creating an IAM role for installation of applications on Amazon EC2 instances" on page [834](#)) to the protected EC2 instances.
7. Click the **Next: Review** button.
8. Enter a name and a description for the IAM role and click the **Create role** button (see the figure below).

The role that you created appears in the list of roles with the name and description that you entered.



You will need to assign this role to the EC2 instance that you will use as the Administration Server.

The newly created role is available for all applications on the Administration Server. Therefore, any application running on the Administration Server has the capability to poll cloud segments or install applications on EC2 instances within a cloud segment.

The addresses of web pages cited in this document were correct as of March 2021.

See also:

Creating an IAM user account for work with Kaspersky Security Center	833
Step 3. Authorization in the cloud environment	856
Scenario: Deployment for cloud environment.....	821

Creating an IAM user account for work with Kaspersky Security Center

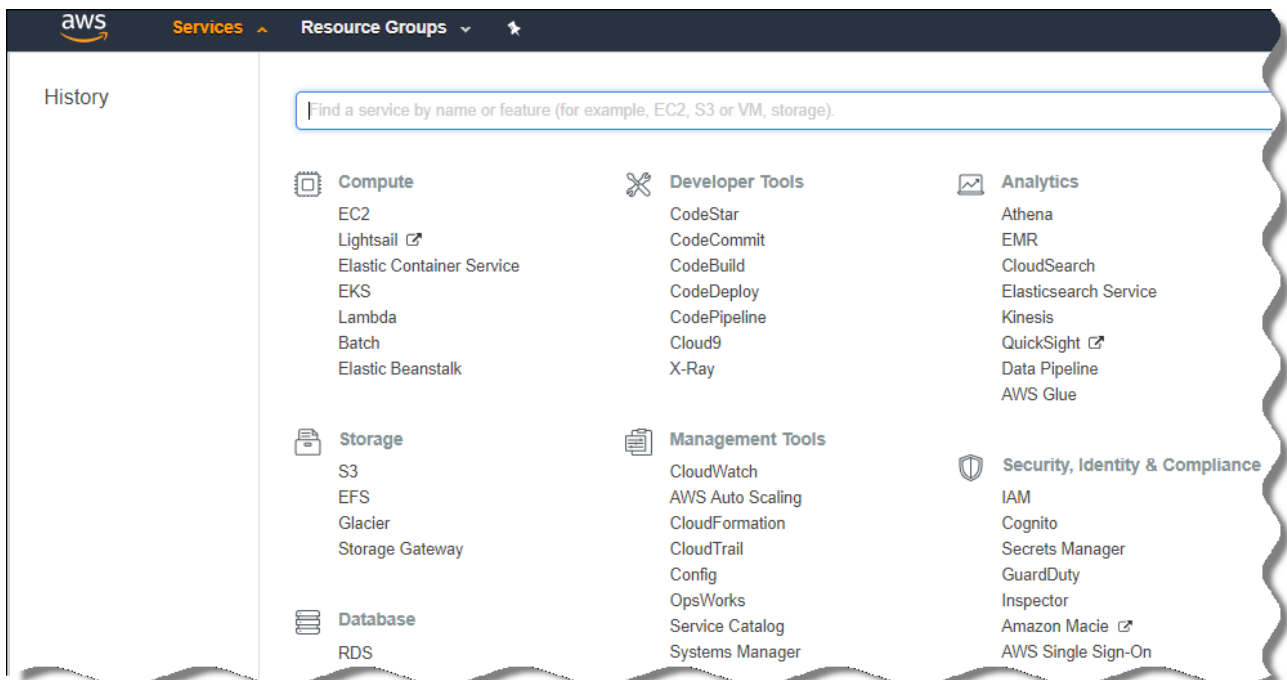
An IAM user account is required for working with Kaspersky Security Center if the Administration Server has not been assigned an IAM role with permissions for device discovery and installation of applications on instances. The same account, or a different account, is also required for backing up the Administration Server data task if you use an S3 bucket. You can create one IAM user account with all the necessary permissions, or you can create two separate user accounts.

An *IAM access key* that you will need to provide to Kaspersky Security Center during initial configuration is automatically created for the IAM user. An IAM access key consists of an access key ID and a secret key. For more details about the IAM service, please refer to the following AWS reference pages:

- <http://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html>
<https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html>.
- http://docs.aws.amazon.com/IAM/latest/UserGuide/IAM_UseCases.html#UseCase_EC2
https://docs.aws.amazon.com/IAM/latest/UserGuide/IAM_UseCases.html#UseCase_EC2.

► *To create an IAM user account with the necessary permissions:*

1. Open the AWS Management Console (см. раздел AWS console - <https://console.aws.amazon.com/iam>) and sign in under your account.
2. In the list of AWS services, select **IAM** (as shown in the figure below).



A window opens containing a list of user names and a menu that lets you work with the tool.

3. Navigate through the areas of the console dealing with user accounts, and add a new user name or names.
4. For the user(s) you add, specify the following AWS properties:
 - Access type: **Programmatic Access**.
 - Permissions boundary not set.
 - Permissions:

- **ReadOnlyAccess**—If you plan to run only cloud segment polling and do not plan to install applications on EC2 instances using AWS API.
- **ReadOnlyAccess** and **AmazonSSMFullAccess**—If you plan to run cloud segment polling and install applications on EC2 instances using AWS API. In this case, you must assign an IAM role with the AmazonEC2RoleforSSM permission (see section "Creating an IAM role for installation of applications on Amazon EC2 instances" on page [834](#)) to the protected EC2 instances.

After you add permissions, view them for accuracy. In case of a mistaken selection, go back to the previous screen and make the selection again.

5. After you create the user account, a table appears containing the IAM access key of the new IAM user. The access key ID is displayed in the **Access key ID** column. The secret key is displayed as asterisks in the **Secret access key** column. To view the secret key, click **Show**.

The newly created account is displayed in the list of IAM user accounts that corresponds to your account in AWS.

When deploying Kaspersky Security Center in a cloud segment, you must specify that you are using an IAM user account and provide the access key ID and secret access key to Kaspersky Security Center.

The addresses of web pages cited in this document were correct as of March 2021.

See also:

Creating an IAM role for the Administration Server.....	830
Step 3. Authorization in the cloud environment.....	856
Scenario: Deployment for cloud environment.....	821

Creating an IAM role for installation of applications on Amazon EC2 instances

Before you start protection deployment on EC2 instances by using Kaspersky Security Center, create in the AWS Management Console (см. раздел AWS console - <https://console.aws.amazon.com/iam>) an IAM role with permissions required for installation of applications on instances. For more details, see AWS Help sections AWS Help https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html about IAM roles.

The IAM role is required so that you can assign it to all EC2 instances on which you plan to install security applications by using Kaspersky Security Center. If you do not assign an instance the IAM role with the necessary permissions, installation of applications on this instance using AWS API tools will result in an error.

To work with the AWS Management Console, you will need a user name and password from an account in AWS.

► *To create an IAM role for installing applications on instances:*

1. Open the AWS Management Console (см. раздел IAM console - <https://console.aws.amazon.com/iam/home>) and log in under your AWS account.
2. In the menu on the left, select **Roles**.
3. Click the **Create Role** button.
4. In the list of services that appears, select **EC2** and then in the **Select Your Use Case** list select **EC2** again.

5. Click the **Next: Permissions** button.
6. In the list that opens, select the check box next to **AmazonEC2RoleforSSM**.
7. Click the **Next: Review** button.
8. Enter a name and a description for the IAM role and click the **Create role** button.

The role that you created appears in the list of roles with the name and description that you entered.

Hereinafter, you can use the newly created IAM role to create new EC2 instances that you intend to protect through Kaspersky Security Center, as well as associate it with existing instances.

The addresses of web pages cited in this document were correct as of March 2021.

See also:

Scenario: Deployment for cloud environment.....[821](#)

Working with Amazon RDS

This section describes which actions must be taken to prepare a database of Amazon Relational Database Service (RDS) for Kaspersky Security Center, place it in an option group, create an IAM role for working with an RDS database, prepare an S3 bucket for storage, and migrate an existing database to RDS.

Amazon RDS is a web service that helps AWS users to set up, operate, and scale a relational database in the AWS cloud environment. If you want, you can use an Amazon RDS database to work with Kaspersky Security Center.

You can work with the following databases:

- Microsoft SQL Server
- SQL Express Edition
- Aurora MySQL 5.7
- Standard MySQL 5.7

See also:

Scenario: Deployment for cloud environment.....	821
Creating an Amazon RDS instance.....	836
Creating option group for Amazon RDS instance	837
Modifying the option group	838
Modifying permissions for IAM role for Amazon RDS database instance	839
Preparing Amazon S3 bucket for database.....	840
Migrating the database to Amazon RDS	840

Creating an Amazon RDS instance

If you want to use Amazon RDS as the DBMS, you have to create an Amazon RDS database instance. This section describes how to select SQL Express Edition; if you want to work with Aurora MySQL 5.7 or Standard MySQL 5.7, you must select one of those engines.

► *To create an Amazon RDS database instance:*

1. Open the AWS Management Console at <https://console.aws.amazon.com> and sign in under your account.
2. Using the AWS interface, create a database with the following settings:
 - Engine: Microsoft SQL Server, SQL Express Edition
 - DB engine version: SQL Server 2014 12.00.5546.0v1
 - DB instance class: db.t2.medium
 - Storage type: General purpose
 - Allocated storage: minimum 50 GiB
 - Security group: the same group where the EC2 instance with Kaspersky Security Center Administration Server will be located

Create an identifier, username and password for your RDS instance.

You may leave default settings in all the other fields. Or, change the default settings if you want to customize your Amazon RDS instance. To get help, refer to the AWS information pages.

3. At the last step, AWS displays the results of the process. If you want to view the details of your Amazon RDS instance, press **View DB instance details**. If you want to proceed to the next action, start creating an option group for your Amazon RDS instance (see section "Creating option group for Amazon RDS instance" on page [837](#)).

The creation of a new Amazon RDS instance may take up to several minutes. After the instance is created, you can use it for work with Kaspersky Security Center data.

The addresses of web pages cited in this document were correct as of March 2021.

See also:

Scenario: Deployment for cloud environment.....821

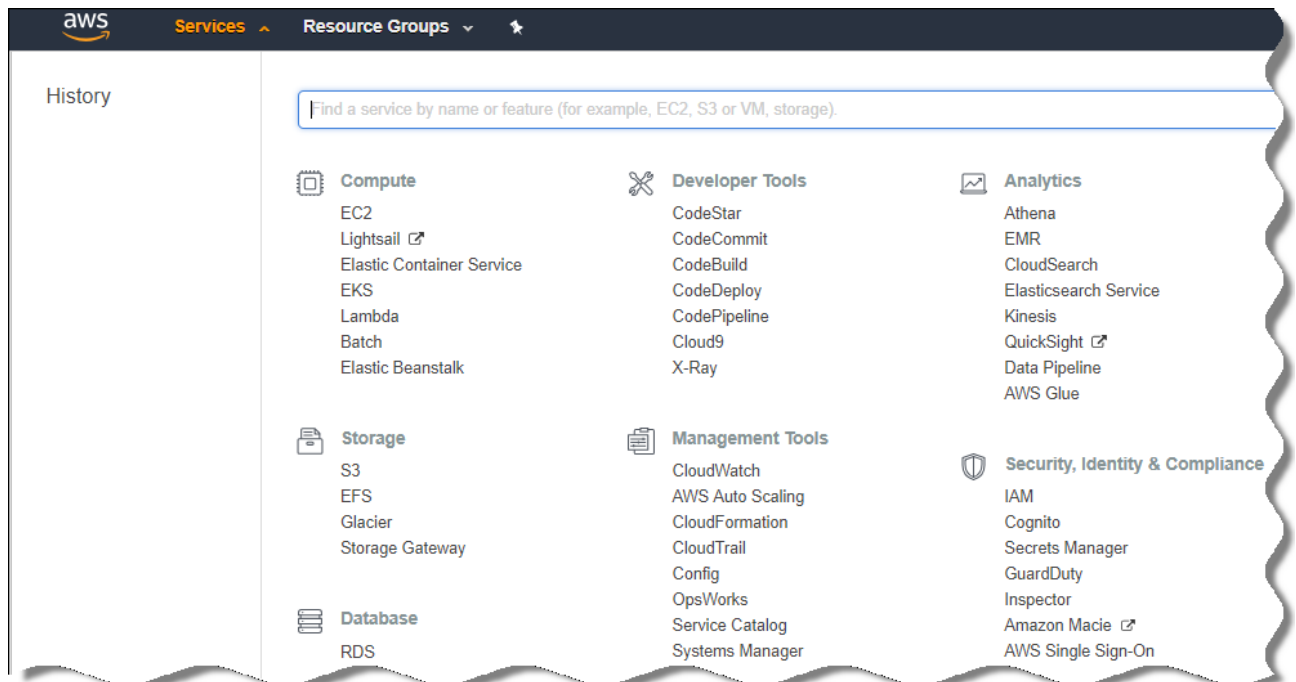
Creating option group for Amazon RDS instance

You need to place your Amazon RDS instance into an option group.

► To create an option group for your Amazon RDS instance:

1. Make sure that you are in the AWS Management Console (<https://console.aws.amazon.com> <https://console.aws.amazon.com>) and signed in under your account.
2. In the menu line, click **Services**.

The list of available services appears (see figure below).



3. In the list, click **RDS**.
4. In the left pane, click **Option groups**.
5. Click the **Create group** button.
6. Create an option group with the following settings, if you chose SQL Server at the stage of creating the Amazon RDS instance (see section "Creating an Amazon RDS instance" on page 836):
 - Engine: SQLserver-ex
 - Major engine version: 12.00

If you chose a different SQL database at the stage of creating the Amazon RDS instance, then choose a corresponding engine.

The group is created. You can see it in the list of your groups.

After creating the option group, place your Amazon RDS instance into this option group.

The addresses of web pages cited in this document were correct as of March 2021.

See also:

- Scenario: Deployment for cloud environment.....[821](#)
- Hardware requirements for the Administration Server in a cloud environment.....[826](#)

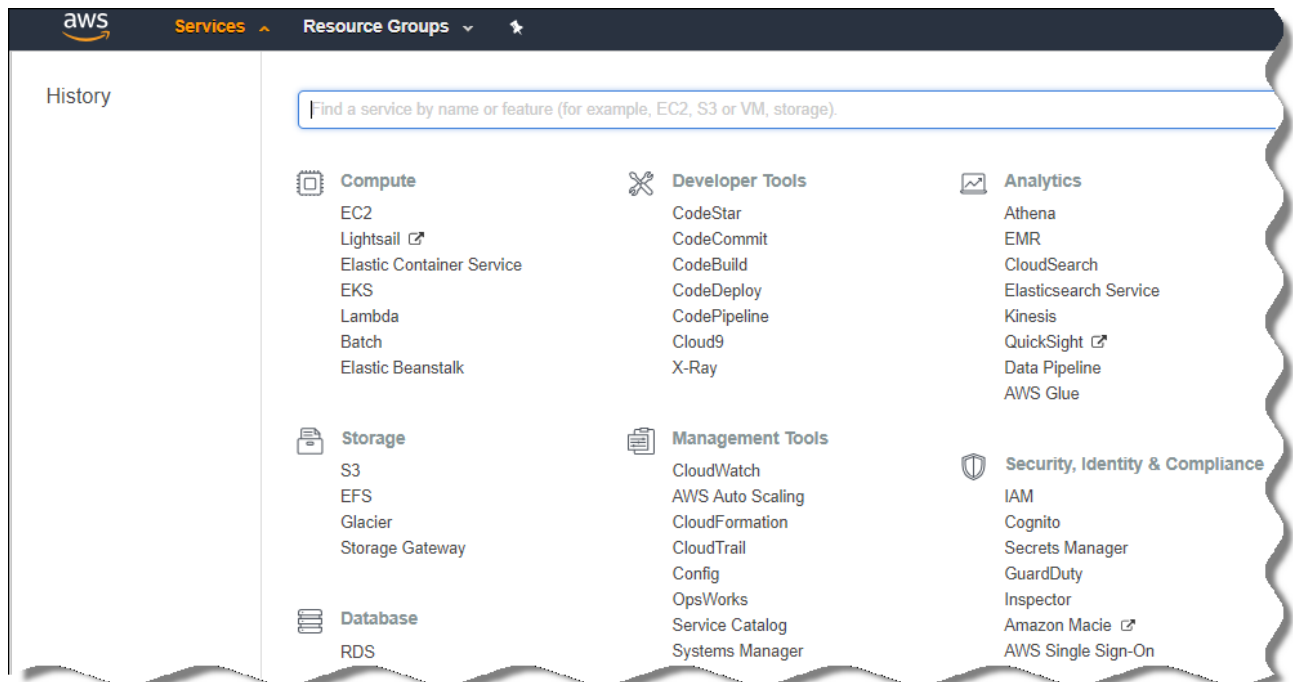
Modifying the option group

The default configuration of the option group in which you placed the Amazon RDS instance is not enough for working with the Kaspersky Security Center database. You have to add options to the option group and create a new IAM role for working with the database.

► *To modify the option group and create a new IAM role:*

1. Make sure that you are in the AWS Management Console (<https://console.aws.amazon.com> <https://console.aws.amazon.com>) and signed in under your account.
2. In the menu line, click **Services**.

The list of available services appears (see figure below).



3. In the list, select RDS.
4. In the left pane, click **Option groups**.

The list of option groups is displayed.

5. Select the option group in which you placed your Amazon RDS instance and click the **Add option** button. The **Add option** window opens.
 6. In the IAM role section, select the **Create a new role / Yes** option and enter a name for the new IAM role. The role is created with a default set of permissions. Later, you will have to change its permissions (see section "Modifying permissions for IAM role for Amazon RDS database instance" on page [839](#)).
 7. In the S3 bucket section, do one of the following:
 - If you haven't created an Amazon S3 bucket instance for the data backup, select the **Create a new S3 bucket** link and create a new S3 bucket, using the AWS interface (see section "Preparing Amazon S3 bucket for database" on page [840](#)).
 - If you already have created an Amazon S3 bucket instance for the Administration Server data backup task, select your S3 bucket from the drop-down menu.
 8. Finish adding options by clicking the **Add option** button at the bottom of the page.
- You have modified the option group and created a new IAM role for working with the RDS database.

The addresses of web pages cited in this document were correct as of March 2021.

See also:

Scenario: Deployment for cloud environment.....	821
---	---------------------

Modifying permissions for IAM role for Amazon RDS database instance

After you add options to the option group (see section "Modifying the option group" on page [838](#)), you must assign required permissions to the IAM role that you created for working with the Amazon RDS database instance.

► *To assign required permissions to the IAM role that you created for work with the Amazon RDS database instance:*

1. Make sure that you are in the AWS Management Console (<https://console.aws.amazon.com> <https://console.aws.amazon.com>) and have signed in under your account.
2. In the list of services, select **IAM**.
A window opens containing a list of user names and a menu that lets you work with the tool.
3. In the menu, select **Roles**.
4. In the list of IAM roles displayed in the workspace, select the role that you created when adding option to the option group (see section "Modifying the option group" on page [838](#)).
5. Using the AWS interface, delete the **sqlNativeBackup-<date>** policy.
6. Using the AWS interface, attach the **AmazonS3FullAccess** policy to the role.

The IAM role is assigned the required permissions to work with Amazon RDS.

The addresses of web pages cited in this document were correct as of March 2021.

See also:

Scenario: Deployment for cloud environment [821](#)

Preparing Amazon S3 bucket for database

If you plan to use Amazon Relational Database System (Amazon RDS) database, you have to create an Amazon Simple Storage Service (Amazon S3) bucket instance where the regular Backup of the database will be stored. For information about Amazon S3 and about S3 buckets, refer to the Amazon help pages. For more information about creating an Amazon S3 instance, refer to Amazon S3 help page <https://docs.aws.amazon.com/AmazonS3/latest/user-guide/create-bucket.html>.

► To create an Amazon S3 bucket:

1. Make sure that AWS Management Console <https://console.aws.amazon.com/> is open and you are signed in under your account.
2. In the list of AWS services, select S3.
3. Navigate the console to create a bucket, following the instructions of the wizard.
4. Select the same region where your Administration Server is located (or will be located).
5. When the wizard finishes, make sure that the new bucket appears in the list of buckets.

A new S3 bucket is created and appears in your list of buckets. You have to specify this bucket when adding options to the option group (see section "Modifying the option group" on page [838](#)). You will also have to specify the address of your S3 bucket to Kaspersky Security Center when the Kaspersky Security Center creates the *Backup of Administration Server data* task (see section "Step 7. Creating an initial protection configuration" on page [861](#)).

The addresses of web pages cited in this document were correct as of March 2021.

See also:

Database options for work in a cloud environment [827](#)

Scenario: Deployment for cloud environment [821](#)

Migrating the database to Amazon RDS

You can migrate your Kaspersky Security Center database from an on-premises device to an Amazon S3 instance that supports Amazon RDS. To do this, you need an S3 bucket (see section "Preparing Amazon S3 bucket for database" on page [840](#)) for an RDS database and an IAM user account with AmazonS3FullAccess permission for this S3 bucket (see section "Creating an IAM user account for work with Kaspersky Security Center" on page [833](#)).

► *To perform the migration of the database:*

1. Make sure that you have created an RDS instance (see section "Creating an Amazon RDS instance" on page [836](#)) (refer to Amazon RDS reference pages https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_SQLServer.html for more information).
2. On your physical Administration Server (on-premises), run the Kaspersky Backup utility to back up Administration Server data.
You must make sure that the file is named backup.zip.
3. Copy the backup.zip file to the EC2 instance on which Administration Server is installed.

Make sure that you have enough disk space on the EC2 instance on which Administration Server is installed. In the AWS environment, you can add disk space to your instance to accommodate the process of database migration.

4. On the AWS Administration Server, start the Kaspersky Backup utility again in interactive mode (see section "Data backup and recovery in interactive mode" on page [619](#)).
The Backup and Restore Wizard starts.
5. At the **Select action** step, select **Restore Administration Server data** and click **Next**.
6. At the **Restore settings** step, click the **Browse** button next to the **Folder for storage of backup copies**.
7. In the **Sign In to Online Storage** window that opens, fill in the following fields and then click **OK**:
 - **S3 bucket name**
The name of your S3 bucket (see section "Preparing Amazon S3 bucket for database" on page [840](#)).
 - **Backup folder**
Specify the location of the storage folder that is meant for backup.
 - **Access key ID**
AWS IAM access key ID that belongs to the IAM user who has the permissions to use the S3 bucket (the AmazonS3FullAccess permission).
 - **Secret key**
AWS IAM secret key that belongs to the IAM user who has the permissions to use the S3 bucket (the AmazonS3FullAccess permission).
8. Select the **Migrate from local backup** option. The **Browse** button becomes available.
9. Click the **Browse** button to choose the folder on the AWS Administration Server where you copied the backup.zip file.
10. Click **Next** and complete the procedure.

Your data will be restored to the RDS database using your S3 bucket. You can use this database for further work with Kaspersky Security Center in the AWS environment.

The addresses of web pages cited in this document were correct as of March 2021.

See also:

Scenario: Deployment for cloud environment [821](#)

Working in Microsoft Azure cloud environment

This section provides information about Kaspersky Security Center deployment and maintenance in a cloud environment provided by Microsoft Azure, as well as details of protection deployment on virtual machines in this cloud environment.

In a Kaspersky Security Center that has been deployed from a Usage-based monthly billed SKU, Vulnerability and Patch Management is automatically activated, and Mobile Device Management cannot be activated.

See also:

Hardware and software requirements	31
About work in Microsoft Azure	843
Creating a subscription, Application ID, and password	843
Assigning a role to the Azure Application ID	844
Deploying Administration Server in Microsoft Azure and selecting database	845
Working with Azure SQL.....	846

About work in Microsoft Azure

To work with the Microsoft Azure platform and, in particular, to purchase apps at the Azure Marketplace and create virtual machines, you will need an Azure subscription. Before you deploy the Administration Server, create an Azure Application ID with permissions required for installation of applications on virtual machines.

If you purchase a Kaspersky Security Center image at the Azure Marketplace, you can deploy a virtual machine with your ready-to-use Kaspersky Security Center Administration Server. You must select settings of the virtual machine, but you do not have to install the application yourself. After deployment, you can start Administration Console and connect to the Administration Server to begin working with Kaspersky Security Center.

You can also use an Azure virtual machine with Kaspersky Security Center Administration Server deployed on it to protect on-premises devices (for example, if a cloud server turns out to be easier to service and maintain than a physical one). If this is the case, you work with the Administration Server the same as you would if the Administration Server were installed on a physical device. If you do not plan to use Azure API tools, you do not need an Azure Application ID. In this case, an Azure subscription is enough.

See also:

About work in a cloud environment	820
Scenario: Deployment for cloud environment.....	821

Creating a subscription, Application ID, and password

To work with Kaspersky Security Center in the Microsoft Azure environment, you need an Azure subscription, Azure Application ID, and Azure Application password. You can use an existing subscription, if you already have one.

An Azure subscription grants its owner access to the Microsoft Azure Platform Management Portal and to Microsoft Azure services. The owner can use the Microsoft Azure Platform to manage services such as Azure SQL and Azure Storage.

► *To create a Microsoft Azure subscription,*

Go to <https://account.windowsazure.com/Subscriptions> and follow the instructions there.

More information about creating a subscription is available on the Microsoft website <https://docs.microsoft.com/en-us/partner-center/create-a-new-subscription>. You will get a subscription ID, which you will later provide to Kaspersky Security Center together with Application ID and password (see section "Step 3. Authorization in the cloud environment" on page [856](#)).

► *To create and save Azure Application ID and password:*

1. Go to <https://portal.azure.com> and make sure that you are logged in.
2. Following the instructions on the reference page <https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-create-service-principal-portal>, create your Application ID.
3. Go to the **Keys** section of the application settings.
4. In the **Keys** section, fill in the **Description** and **Expires** fields and leave the **Value** field empty.
5. Click **Save**.

When you click **Save**, the system automatically fills the **Value** field with a long sequence of characters. This sequence is your Azure Application password (for example, `yXyPOy6Tre9PYgP/j4XVyJCvepPHk2M/UYJ+QlFvdU=`). The description is displayed as you entered it.

6. Copy the password and save it, so that you can later provide the Application ID and password to Kaspersky Security Center (see section "Step 3. Authorization in the cloud environment" on page [856](#)).

You can copy the password only when it has been created. Later, the password will no longer be displayed and you cannot restore it.

The addresses of web pages cited in this document were correct as of March 2021.

See also:

Scenario: Deployment for cloud environment.....	821
---	---------------------

Assigning a role to the Azure Application ID

If you only want to detect virtual machines using device discovery, your Azure Application ID must have the Reader role. If you want not only to detect virtual machines, but also to deploy protection on the virtual machines, your Azure Application ID must have the Virtual Machine Contributor role.

Follow the instructions on the Microsoft website to assign a role to your Azure Application ID.

See also:

Scenario: Deployment for cloud environment.....[821](#)

Deploying Administration Server in Microsoft Azure and selecting database

► *To deploy Administration Server in the Microsoft Azure environment:*

1. Sign in to Microsoft Azure using your account.
2. Go to the Azure portal <https://portal.azure.com/#create/>.
3. In the left pane, click the green plus sign.
4. Type "Kaspersky Hybrid Cloud Security" in the search field in the menu.
Kaspersky Hybrid Cloud Security is a combination of Kaspersky Security Center and two security applications for protection of instances: Kaspersky Endpoint Security for Linux and Kaspersky Security for Windows Server.
5. In the list of results, select Kaspersky Hybrid Cloud Security or Kaspersky Hybrid Cloud Security (BYOL).
In the right part of the screen, an information window appears.
6. Read information and click the Create button in the end of the information window.
7. Fill all the necessary fields. Use the tooltips to get information and assistance.
8. When selecting the size, select one of the three starred options.
In most cases, 8 gigabytes (GB) of RAM is enough. However, in Azure, you can increase the size of RAM and other resources of the virtual machine at any time.
9. When selecting a database, select one of the following, according to your plan (see section "Database options for work in a cloud environment" on page [827](#)):
 - Local—If you want a database on the same virtual machine where the Administration Server will be deployed. Kaspersky Security Center comes with an SQL Server Express database. Choose this option if SQL Server Express is enough for your needs.
 - New—If you want a new RDS database in the Azure environment. Choose this option if you want a DBMS other than SQL Server Express. Your data will be transferred to the cloud environment, where it will remain, and you will not have any extra expenses.
 - Existing—If you want to use an existing database server. In this case, you will have to specify its location. If this server is outside the Azure environment, your data will be transferred over the Internet, which might result in extra expenses.
10. When entering the subscription ID, use the subscription (see section "Creating a subscription, Application ID, and password" on page [843](#)) that you created earlier.

After deployment, you can connect to the Administration Server using RDP. You can use the Administration Console to work with the Administration Server.

See also:

Scenario: Deployment for cloud environment.....	821
---	---------------------

Working with Azure SQL

This section describes which actions must be taken to prepare a Microsoft Azure database for Kaspersky Security Center, prepare an Azure storage account, and migrate an existing database to Azure SQL.

SQL Database is a general-purpose relational database managed service in Microsoft Azure.

The addresses of web pages cited in this document were correct as of March 2021.

See also:

Scenario: Deployment for cloud environment	821
Creating Azure storage account	846
Creating Azure SQL database and SQL Server	847
Migrating the database to Azure SQL	847

Creating Azure storage account

You have to create a storage account in Microsoft Azure for working with Azure SQL database and for deployment scripts.

► To create a storage account:

1. Sign in to the Azure portal.
2. In the left pane, select **Storage accounts** to proceed to the **Storage accounts** window.
3. In the **Storage accounts** window, click the **Add** button to proceed to the **Create storage account** window.
4. Fill in all the necessary fields to create a storage account:
 - Location: must be the same as the location of the Administration Server.
 - Other fields: you may leave the default values.

Use the tooltips to get information about each field.

After the storage account is created, the list of your storage accounts is displayed.

5. In the list of your storage accounts, click the name of the newly created account to see information about this account.
6. Make sure you know the account name, the resource group, and access keys for this storage account. You will need this information for working with Kaspersky Security Center.

You can refer to Azure website for help.

If you already have a storage account, you can use it for working with Kaspersky Security Center.

See also:

Scenario: Deployment for cloud environment.....[821](#)

Creating Azure SQL database and SQL Server

You need an SQL database and SQL Server in the Azure environment.

► To create an Azure SQL database and SQL Server:

1. Follow the instructions on the Azure website.

You can create a new server when Microsoft Azure prompts you to do so; if you already have an Azure SQL Server, you can use it for Kaspersky Security Center rather than creating a new one.

2. After creating the SQL database and SQL Server, make sure that you know its resource name and resource group:

- a. Go to <https://portal.azure.com> and make sure that you are logged in.
- b. In the left pane, select **SQL databases**.
- c. Click the name of a database from the list of your databases.

The properties window opens.

- d. The name of the database is the resource name. The name of the resource group is displayed in the **Overview** section of the properties window.

You need the resource name and resource group of the database for migrating the database to Azure SQL (on page [847](#)).

See also:

Scenario: Deployment for cloud environment.....[821](#)

Migrating the database to Azure SQL

After Administration Server is deployed in the Azure environment (see section "Deploying Administration Server in Microsoft Azure and selecting database" on page [845](#)), you can migrate your Kaspersky Security Center database from an on-premises device to Azure SQL. You need an Azure storage account for an Azure SQL database. You also must have Microsoft SQL Server Data-Tier Application Framework (DacFx) and SQLSysCLRTypes on your Administration Server.

► To perform the migration of the database:

1. Make sure that you have created an Azure storage account (see section "Creating Azure storage account" on page [846](#)).

2. Make sure that you have SQLSysCLRTypes and DacFx on your Administration Server.

You can download Microsoft SQL Server Data-Tier Application Framework (17.0.1 DacFx) and SQLSysCLRTypes (choose the version corresponding to the version of your SQL Server) from the official Microsoft website.

3. On your physical Administration Server (on-premises), run the Kaspersky Backup utility to back up Administration Server data with the **Migrate to Azure format** option enabled.
4. Copy the backup file to the Azure Administration Server.

Make sure that you have enough disk space on the Azure virtual machine where the Administration Server is installed. In the Azure environment, you can add disk space to your virtual machines to accommodate the process of database migration.

5. On the Administration Server located in the Microsoft Azure environment, start the Kaspersky Backup utility again in interactive mode (see section "Data backup and recovery in interactive mode" on page [619](#)).

The Backup and Restore Wizard starts.

6. At the **Select action** step, select **Restore Administration Server data** and click **Next**.
7. At the **Restore settings** step, click the **Browse** button next to the **Folder for storage of backup copies**.
8. In the **Sign In to Online Storage** window that opens, fill in the following fields and then click **OK**:

- **Azure storage account name**

You created the name of the Azure storage account (see section "Creating Azure storage account" on page [846](#)) for working with Kaspersky Security Center.

- **Backup folder**

Specify the location of the storage folder that is meant for backup.

- **Azure Subscription ID**

You created (see section "Creating a subscription, Application ID, and password" on page [843](#)) the subscription on the Azure portal.

- **Azure Application password**

You received the password of the Application ID when you created the Application ID (see section "Creating a subscription, Application ID, and password" on page [843](#)).

The characters of the password are displayed as asterisks. After you begin entering the password, the **Show** button becomes available. Click and hold this button to view the characters you entered.

- **Azure storage access key**

Available in the properties of your storage account (see section "Working with Azure SQL" on page [846](#)), in the Access Keys section. You can use any of the keys (key1 or key2).

- **Azure SQL server name**

Available in the properties of your Azure SQL Server (see section "Creating Azure SQL database and SQL Server" on page [847](#)).

- **Azure SQL server resource group**

Available in the properties of your Azure SQL Server (see section "Creating Azure SQL

database and SQL Server" on page [847](#)).

- **Azure Application ID**

You created (see section "Creating a subscription, Application ID, and password" on page [843](#)) this application ID on the Azure portal.

You can provide only one Azure Application ID for polling and other purposes. If you want to poll another Azure segment, you must first delete the existing Azure connection.

9. Select the **Migrate from local backup** option.

The **Browse** button becomes available.

10. Click the **Browse** button to choose the folder on the Azure Administration Server where you copied the backup file.

11. Click **Next** and complete the procedure.

Your data will be restored to the Azure SQL database by using your Azure storage. You can use this database for further work with Kaspersky Security Center in the Azure environment.

The addresses of web pages cited in this document were correct as of March 2021.

See also:

Scenario: Deployment for cloud environment.....[821](#)

Working in Google Cloud

This section provides information about work with Kaspersky Security Center in a cloud environment provided by Google.

In this section

Creating client email, project ID, and private key[849](#)

Working with Google Cloud SQL for MySQL instance[850](#)

Creating client email, project ID, and private key

You can use the Google API to work with Kaspersky Security Center in Google Cloud Platform. A Google account is required. Please refer to the Google documentation at <https://cloud.google.com> for more information.

You will need to create and provide Kaspersky Security Center with the following credentials:

- **Client email**
- **Project ID**
- **Private key**

See also:

Scenario: Deployment for cloud environment[821](#)

Working with Google Cloud SQL for MySQL instance

You can create a database in Google Cloud and use this database for Kaspersky Security Center.

Kaspersky Security Center works with MySQL 5.7 and 5.6. Other versions of MySQL have not been tested.

► *To create and configure a MySQL database:*

In your browser, go to <https://cloud.google.com/sql/docs/mysql/create-instance#create-2nd-gen> and follow the instructions provided.

When configuring a MySQL database, use the following flags:

- **sort_buffer_size** 10000000
- **join_buffer_size** 20000000
- **innodb_lock_wait_timeout** 300
- **max_allowed_packet** 32000000
- **innodb_thread_concurrency** 20
- **max_connections** 151
- **tmp_table_size** 67108864
- **max_heap_table_size** 67108864
- **lower_case_table_names** 1

See also:

Scenario: Deployment for cloud environment.....	821
---	---------------------

Prerequisites for client devices in a cloud environment necessary for work with Kaspersky Security Center

For the devices on which you intend to install Administration Server, Network Agent, and Kaspersky security applications, the following conditions must be met:

- The configuration of security groups make available the following ports on the Administration Server (minimum set of ports required for deployment):
 - 8060 HTTP—For transfer of Network Agent installation packages and security application installation packages from the Administration Server to protected instances
 - 8061 HTTPS—For transfer of Network Agent installation packages and security application installation packages from the Administration Server to protected instances
 - 13000 TCP—For transfers from protected instances and secondary Administration Servers to the primary Administration Server using SSL
 - 13000 UDP—For transfer of information about shutdown of instances to the Administration Server
 - 14000 TCP—For transfers from protected instances and secondary Administration Servers to the primary Administration Server without using SSL
 - 13291—For connecting Administration Console to the Administration Server
 - 40080—For the operation of deployment scripts

You can configure security groups in AWS Management Console or at the Azure portal. If you intend to use Kaspersky Security Center in a non-default configuration, please refer to the Help page at <https://support.kaspersky.com/9297#block1> <https://support.kaspersky.com/9297#block1>. Examples of non-default configurations include not installing Administration Console on the Administration Server device but installing it on your workstation instead, or using a KSN proxy server.

- Port 15000 UDP is available on the client devices (for receipt of requests for communication with the Administration Server).
- In the AWS cloud environment:
 - If you plan to use AWS API, the IAM role (see section "Creating an IAM role for installation of applications on Amazon EC2 instances" on page [834](#)) is set under which the applications will be installed on the instances.
 - On each Amazon EC2 instance, Systems Manager Agent (SSM Agent) is installed and running.
 - SSM Agent enables Kaspersky Security Center to automatically install applications on devices and groups of devices without requesting confirmation by an administrator each time.
 - On instances that are running a Windows operating system and were deployed from AMIs later than November 2016, SSM Agent is installed and running. You will have to manually install SSM Agent on all other devices. For details about installing SSM Agent on devices running Windows and Linux operating systems, please refer to the AWS Help page <http://docs.aws.amazon.com/systems-manager/latest/userguide/ssm-agent.html>.
- In the Microsoft Azure cloud environment:
 - On each Azure virtual machine, Azure VM Agent is installed and running.

By default, a new virtual machine is created with Azure VM Agent, and you do not have to install or enable it manually. Please refer to Microsoft Help pages for details about Azure VM Agent on Windows devices and on Linux devices.

- Your Azure Application ID (see section "Creating a subscription, Application ID, and password" on page [843](#)) has the following roles:
 - Reader (to discover virtual machines by using polling)
 - Virtual Machine Contributor (to deploy protection on the virtual machines)
 - SQL Server Contributor (to use an SQL database in the Microsoft Azure environment)

If you want to perform all these operations, assign (see section "Assigning a role to the Azure Application ID" on page [844](#)) all the three roles to your Azure Application ID.

Cloud Environment Configuration Wizard

To configure Kaspersky Security Center using this Wizard, you must have the following:

- Specific credentials for a cloud environment:
 - An IAM role that has been granted the right to poll the cloud segment (see section "Creating an IAM role for the Administration Server" on page [830](#)) or an IAM user account that has been granted the right to poll the cloud segment (see section "Creating an IAM user account for work with Kaspersky Security Center" on page [833](#)) (for work with Amazon Web Services)
 - Azure Application ID, password, and subscription (see section "Creating a subscription, Application ID, and password" on page [843](#)) (for work with Microsoft Azure)
 - Google client email, Project ID, and private key (see section "Working in Google Cloud" on page [849](#)) (for work with Google Cloud)

If you do not want to use cloud environment capabilities (if, for example, you want to manage protection of physical client devices only), you can close the Cloud Environment Configuration Wizard and run the standard Administration Server Quick Start Wizard (on page [265](#)) manually.

The Cloud Environment Configuration Wizard starts automatically at the first connection to Administration Server through Administration Console if you are deploying Kaspersky Security Center from a ready-to-use image. You can also start the Cloud Environment Configuration Wizard manually at any time.

► *To start the Cloud Environment Configuration Wizard manually:*

1. In the console tree, select the **Administration Server** node.
2. In the context menu of the node, select **All Tasks** → **Cloud Environment Configuration Wizard**.

The average work session with this Wizard lasts about 15 minutes.

See also:

Scenario: Deployment for cloud environment.....	821
About the Cloud Environment Configuration Wizard.....	855
Step 1. Selecting the application activation method.....	855
Step 2. Selecting the cloud environment.....	856
Step 3. Authorization in the cloud environment.....	856
Step 4. Configuring synchronization with Cloud and choosing further actions.....	858
Step 5. Configuring Kaspersky Security Network.....	860
Step 6. Configuring email notifications.....	860
Step 7. Creating an initial protection configuration.....	861
Step 8. Selecting the action when the operating system must be restarted during installation.....	862
Step 9. Receiving updates by the Administration Server.....	863

About the Cloud Environment Configuration Wizard

This Wizard allows you to configure Kaspersky Security Center while taking into account the specifics of working in a cloud environment.

The Wizard creates the following objects:

- Network Agent policy with default settings
- Policy for Kaspersky Endpoint Security for Linux
- Policy for Kaspersky Security for Windows Server
- Administration group for instances and a rule for automatically moving instances to this administration group
- Administration Server data backup task
- Tasks for installing protection on devices running Linux and Windows
- Tasks for each managed device:
 - Quick Virus Scan
 - Update download

If you selected the BYOL licensing option, the Wizard also activates Kaspersky Security Center with a key file or activation code and places the key file or activation code in the license storage.

Step 1. Selecting the application activation method

If you signed up for one of the ready-to-use AMIs (at the AWS Marketplace), or for a Usage-based monthly billed SKU (at the Azure Marketplace), this activation step will be skipped and the Wizard will immediately proceed to the next step.
You cannot purchase a ready-to-use AMI for Google Cloud.

If you selected BYOL licensing option for Kaspersky Security Center, the Wizard prompts you to select the application activation method.

Activate the application with an activation code (or a key file) for Kaspersky Security for Virtualization or for Kaspersky Hybrid Cloud Security.

You can activate the application in one of the following ways:

- By entering an activation code.
Online activation will start. This process involves verification of the specified activation code, as well as issuance and activation of a key file.
- By specifying a key file.
The application will check the key file and either activate it if it contains the correct information, or prompt you to specify another key file.

Kaspersky Security Center places the license key in the license storage and marks it as automatically distributed on managed devices (see section "Automatic distribution of a license key" on page [361](#)).

If you connect to an instance using standard Remote Desktop Connection in Microsoft Windows or a similar application, in the remote connection properties you must specify the drive of the physical device that you are using to connect. This ensures access from the instance to the files on your physical device, and lets you select and specify the key file.

When working with Kaspersky Security Center deployed from a paid AMI or for a Usage-based monthly billed SKU, you cannot add key files or activation codes to the license storage.

See also:

Licensing options in a cloud environment.....	826
Scenario: Deployment for cloud environment.....	821

Step 2. Selecting the cloud environment

Select the cloud environment in which you are deploying Kaspersky Security Center: AWS, Azure, or Google Cloud.

Step 3. Authorization in the cloud environment

AWS

If you selected AWS, either specify that you have an IAM role with the required rights (see section "Creating an IAM role for the Administration Server" on page [830](#)), or provide Kaspersky Security Center with an AWS IAM access key (see section "Creating an IAM user account for work with Kaspersky Security Center" on page [833](#)). Cloud segment polling is not possible without an IAM role or an AWS IAM access key.

Specify the following settings for the connection that will be used for further polling of the cloud segment:

- **Connection name**

Enter a name for the connection. The name cannot contain more than 256 characters. Only Unicode characters are permitted.

This name will also be used as the name for the administration group for the cloud devices.

If you plan to work with more than one cloud environment, you might want to include the name of the environment in the connection name, for example, "Azure Segment," "AWS Segment," or "Google Segment."

- **Use AWS IAM role**

Select this option if you have already created an IAM role for the Administration Server to use AWS services (see section "Creating an IAM role for the Administration Server" on page [830](#)).

- **Use AWS IAM user account**

Select this option if you have an IAM user account with the necessary permissions (see section "Creating an IAM user account for work with Kaspersky Security Center" on page [833](#)) and you can enter a key ID and secret key.

- **Access key ID**

The IAM access key ID is a sequence of alphanumeric characters. You received the key ID when you created the IAM user account (see section "Creating an IAM user account for work with Kaspersky Security Center" on page [833](#)).

The field is available if you selected an AWS IAM access key for authorization instead of an IAM role.

- **Secret key**

The secret key that you received with the access key ID when you created the IAM user account (see section "Creating an IAM user account for work with Kaspersky Security Center" on page [833](#)).

The characters of the secret key are displayed as asterisks. After you begin entering the secret key, the **Show** button is displayed. Click and hold this button for the necessary amount of time to view the characters you entered.

The field is available if you selected an AWS IAM access key for authorization instead of an IAM role.

This connection is saved in the application settings. The Cloud Environment Configuration Wizard allows you to create only a single AWS IAM access key. Subsequently, you can specify more connections to manage other cloud segments (see section "Adding connections for cloud segment polling" on page [866](#)).

If you want to install applications on instances through Kaspersky Security Center, you must make sure that your IAM role (or the IAM user whose account is associated with the key that you are entering) has all the necessary permissions (see section "Ensuring that the Kaspersky Security Center Administration Server has the permissions to work with AWS" on page [830](#)).

Azure

If you selected Azure, specify the following settings for the connection that will be used for further polling the cloud segment:

- **Connection name**

Enter a name for the connection. The name cannot contain more than 256 characters. Only Unicode characters are permitted.

This name will also be used as the name for the administration group for the cloud devices.

If you plan to work with more than one cloud environment, you might want to include the name of the environment in the connection name, for example, "Azure Segment," "AWS Segment," or "Google Segment."

- **Azure Application ID**

You created (see section "Creating a subscription, Application ID, and password" on page [843](#)) this application ID on the Azure portal.

You can provide only one Azure Application ID for polling and other purposes. If you want to poll another Azure segment, you must first delete the existing Azure connection.

- **Azure Subscription ID**

You created (see section "Creating a subscription, Application ID, and password" on page [843](#)) the subscription on the Azure portal.

- **Azure Application password**

You received the password of the Application ID when you created the Application ID (see section "Creating a subscription, Application ID, and password" on page [843](#)).

The characters of the password are displayed as asterisks. After you begin entering the password, the **Show** button becomes available. Click and hold this button to view the characters you entered.

- **Azure storage account name**

You created the name of the Azure storage account (see section "Creating Azure storage account" on page [846](#)) for working with Kaspersky Security Center.

- **Azure storage access key**

You received a password (key) when you created Azure storage account for working with Kaspersky Security Center.

The key is available in section "Overview of the Azure storage account", in subsection "Keys".

This connection is saved in the application settings.

Google Cloud

If you selected Google Cloud, specify the following settings for the connection that will be used for further polling the cloud segment:

- **Connection name**

Enter a name for the connection. The name cannot contain more than 256 characters. Only Unicode characters are permitted.

This name will also be used as the name for the administration group for the cloud devices.

If you plan to work with more than one cloud environment, you might want to include the name of the environment in the connection name, for example, "Azure Segment," "AWS Segment," or "Google Segment."

- **Client email**
- **Project ID**
- **Private key**

This connection is saved in the application settings.

See also:

| Scenario: Deployment for cloud environment.....[821](#)

Step 4. Configuring synchronization with Cloud and choosing further actions

At this step, cloud segment polling starts and a special administration group for instances is created. The instances found during polling are placed into this group. The cloud segment polling schedule is configured (every 5 minutes by default).

A **Synchronize with Cloud** (see section "**Synchronization with cloud**" on page [873](#)) automatic moving rule is also created. For each subsequent scan of the cloud network, virtual devices detected will be moved to the corresponding subgroup within the **Managed devices\Cloud** group.

On the **Synchronization with the cloud segment** page, you can configure the following settings:

- **Synchronize administration group structure with the cloud segment**

If this option is enabled, the **Cloud** group is automatically created within the **Managed devices** group and a cloud device discovery is started. The instances and virtual machines detected during each cloud network scan are placed into the Cloud group. The structure of the administration subgroups within this group matches the structure of your cloud segment (in AWS, availability zones and placement groups are not represented in the structure; in Azure, subnets are not represented in the structure). Devices that have not been identified as instances in the cloud environment are in the **Unassigned devices** group. This group structure allows you to use group installation tasks to install anti-virus applications on instances, as well as set up different policies for different groups.

If this option is disabled, the **Cloud** group is also created and the cloud device discovery is also started; however, subgroups matching the cloud segment structure are not created within the group. All detected instances are in the **Cloud** administration group so they are displayed in a single list. If your work with Kaspersky Security Center requires synchronization, you can modify the properties of the **Synchronize with Cloud** rule and enforce it (see section "**Synchronization with cloud**" on page [873](#)). Enforcing this rule alters the structure of subgroups in the Cloud group so that it matches the structure of your cloud segment.

By default, this option is disabled.

- **Deploy protection**

If this option is selected, the Wizard creates a task to install security applications on instances. After the Wizard finishes, the Protection Deployment Wizard automatically starts on the devices in your cloud segments, and you will be able to install Network Agent and security applications on those devices.

Kaspersky Security Center can perform the deployment with its native tools. If you do not have permissions to install the applications on EC2 instances or Azure virtual machines, you can configure the **Remote installation** task manually (see section "**Installing applications on devices in a cloud environment**" on page [870](#)) and specify an account with the required permissions. In this case, the Remote installation task will not work for the devices discovered using AWS API or Azure. This task will only work for the devices discovered using Active Directory polling, Windows domains polling, or IP range polling.

If this option is not selected, the Protection Deployment Wizard is not started and tasks for installing security applications on instances are not created. You can manually perform both actions later.

For Google Cloud, you can only perform the deployment with Kaspersky Security Center native tools. If you selected Google Cloud, the **Deploy protection** option is not available.

Step 5. Configuring Kaspersky Security Network

Specify the settings for relaying information about Kaspersky Security Center operations to the Kaspersky Security Network knowledge base. Select one of the following options:

- **I agree to use Kaspersky Security Network**

Kaspersky Security Center and managed applications installed on client devices will automatically transfer their operation details to Kaspersky Security Network (see section "About KSN" on page [785](#)). Participation in Kaspersky Security Network ensures faster updates of databases containing information about viruses and other threats, which ensures a faster response to emergent security threats.

- **I do not agree to use Kaspersky Security Network**

Kaspersky Security Center and managed applications will provide no information to Kaspersky Security Network.

If you select this option, the use of Kaspersky Security Network will be disabled.

Kaspersky recommends participation in Kaspersky Security Network.

Step 6. Configuring email notifications

Configure the delivery of notifications about events registered during the operation of Kaspersky applications on virtual client devices. These settings will be used as the default settings for application policies.

To configure the delivery of notifications about events occurring in Kaspersky applications, use the following settings:

- **Recipients (email addresses)**

The email addresses of users to whom the application will send notifications. You can enter one or more addresses; if you enter more than one address, separate them with a semicolon.

- **SMTP servers**

The address or addresses of your organization's mail servers.

If you enter more than one address, separate them with a semicolon. You can use the IP address or the Windows network name (NetBIOS name) of a device as the address.

- **SMTP server port**

Communication port number of the SMTP server. The default port number is 25.

- **Use ESMTP authentication**

Enables support of ESMTP authentication. When the check box is selected, in the **User name** and **Password** fields you can specify the ESMTP authentication settings. By default, this check box is cleared, and the ESMTP authentication settings are not available.

You can test the new email notification settings by clicking the **Send test message** button. If the test message was successfully received at the addresses specified in the **Recipients (email addresses)** field, the settings have been correctly configured.

Step 7. Creating an initial protection configuration

At this step, Kaspersky Security Center automatically creates policies and tasks. The **Configure initial protection** window displays a list of policies and tasks created by the application.

If you use an RDS database in the AWS cloud environment, you have to provide IAM access key pair to Kaspersky Security Center when the Administration Server backup task is being created. In this case, fill in the following fields:

- **S3 bucket name**

The name of the S3 bucket (see section "Preparing Amazon S3 bucket for database" on page [840](#)) that you created for the Backup.

- **Access key ID**

You received the key ID (sequence of alphanumeric characters) when you created the IAM user account (see section "Creating an IAM user account for work with Kaspersky Security Center" on page [833](#)) for working with S3 bucket storage instance.

The field is available if you selected RDS database on an S3 bucket.

- **Secret key**

The secret key that you received with the access key ID when you created the IAM user account (see section "Creating an IAM user account for work with Kaspersky Security Center" on page [833](#)).

The characters of the secret key are displayed as asterisks. After you begin entering the secret key, the **Show** button is displayed. Click and hold this button for the necessary amount of time to view the characters you entered.

The field is available if you selected an AWS IAM access key for authorization instead of an IAM role.

If you use an Azure SQL database in the Azure cloud environment, you have to provide information about your Azure SQL Server to Kaspersky Security Center when the Administration Server backup task is being created. In this case, fill in the following fields:

- **Azure storage account name**

You created the name of the Azure storage account (see section "Creating Azure storage account" on page [846](#)) for working with Kaspersky Security Center.

- **Azure Subscription ID**

You created (see section "Creating a subscription, Application ID, and password" on page [843](#)) the subscription on the Azure portal.

- **Azure Application password**

You received the password of the Application ID when you created the Application ID (see section "Creating a subscription, Application ID, and password" on page [843](#)).

The characters of the password are displayed as asterisks. After you begin entering the password, the **Show** button becomes available. Click and hold this button to view the characters you entered.

- **Azure Application ID**

You created (see section "Creating a subscription, Application ID, and password" on page [843](#)) this application ID on the Azure portal.

You can provide only one Azure Application ID for polling and other purposes. If you want

to poll another Azure segment, you must first delete the existing Azure connection.

- **Azure SQL server name**

The name and the resource group are available in your Azure SQL Server properties.

- **Azure SQL server resource group**

The name and the resource group are available in your Azure SQL Server properties.

- **Azure storage access key**

Available in the properties of your storage account (see section "Working with Azure SQL" on page [846](#)), in the Access Keys section. You can use any of the keys (key1 or key2).

If you are deploying the Administration Server in the Google Cloud, you have to select a folder where the backup copies will be stored. Select a folder on your local device or a folder on a virtual machine instance.

The **Next** button becomes available after the creation of all policies and tasks that are necessary for minimum configuration of protection.

If a device on which the tasks are supposed to run is not visible to the Administration Server, then the tasks start only when the device becomes visible. If you create a new EC2 instance or a new Azure virtual machine, it might take some time before it becomes visible to the Administration Server. If you want Network Agent and the security applications to be installed on all the newly created devices as soon as possible, make sure (see section "Step 5. Configuring a task schedule" on page [512](#)) that the **Run missed tasks** option is enabled for the **Install application remotely** tasks. Otherwise, a newly created instance/virtual machine will not get Network Agent and the security applications until the task starts according to its schedule.

Step 8. Selecting the action when the operating system must be restarted during installation

If you previously selected (see section "Step 4. Configuring synchronization with Cloud and choosing further actions" on page [858](#)) **Deploy protection**, you must choose what to do when the operating system of a target device has to be restarted. If you did not select the **Deploy protection** option, this step is skipped.

Select whether to restart instances if the device operating system has to be restarted during installation of applications:

- **Do not restart the device**

If this option is selected, the device will not be restarted after the security application installation.

- **Restart the device**

If this option is selected, the device will be restarted after the security application installation.

If you want to force the closing of all applications in blocked sessions on the instances before the restart, select the **Force closure of applications in blocked sessions** check box. If this check box is cleared, you will have to close manually all applications that are running on blocked instances.

Step 9. Receiving updates by the Administration Server

At this step, you can see the progress of downloading updates necessary for correct operation of the Administration Server. You can click the **Next** button, without waiting for download completion, to proceed to the final page of the Wizard.

The Wizard finishes.

Checking configuration

► *To check whether Kaspersky Security Center 13 is properly configured for working in a cloud environment:*

1. Start Kaspersky Security Center and make sure that you can connect to the Administration Server via the Administration Console.
2. In the console tree, select **Managed devices\Cloud**.
3. When viewing any of the subgroups in the **Managed devices\Cloud** group, make sure that the **Devices** tab displays all devices of that subgroup.

If the devices are not displayed, you can poll the corresponding cloud segments (see section "Network segment polling" on page [865](#)) manually to find them.

4. Make sure that the **Policies** tab has active policies for the following applications:
 - Kaspersky Security Center Network Agent
 - Kaspersky Security for Windows Server
 - Kaspersky Endpoint Security for Linux

If they are not listed, you can create them manually.

5. Make sure that the **Tasks** tab lists the following tasks:
 - **Backup of Administration Server data**
 - **Update task for Windows Server**
 - **Database maintenance**
 - **Download updates to the Administration Server repository**
 - **Find vulnerabilities and required updates**
 - **Install protection for Windows**
 - **Install protection for Linux**
 - **Quick scan task for Windows Server**
 - **Quick Scan**
 - **Install updates for Linux**

If they are not listed, you can create them manually.

Kaspersky Security Center 13 is properly configured for work in a cloud environment.

See also:

| Scenario: Deployment for cloud environment [821](#)

Cloud device group

You can manage cloud devices by combining them into groups. At the stage of initially configuring Kaspersky Security Center, the **Managed devices\Cloud** administration group is created by default, and cloud devices detected during polling are placed into this group.

If you selected the **Synchronize administration group structure with the cloud segment** option when you configured synchronization (see section "Step 4. Configuring synchronization with Cloud and choosing further actions" on page [858](#)), the structure of subgroups in this administration group is identical to the structure of your cloud segments. (However, in AWS, availability zones and placement groups are not represented in the structure; in Microsoft Azure, subnets are not represented in the structure.) Empty subgroups within the group that are detected during polling are automatically deleted.

You can also manually create administration groups (see section "Creating administration groups" on page [631](#)) by combining all or specific devices.

By default, the **Managed devices\Cloud** group inherits the policies and tasks from the **Managed devices** group. You can change the settings if the **Editing allowed** check boxes are selected in the properties of the settings of the corresponding policies and tasks.

Network segment polling

Information about the structure of the network and devices in this network is received by the Administration Server through regular polling of cloud segments by using AWS API, Azure API, or Google API tools. Kaspersky Security Center uses this information to update the contents of the **Unassigned devices** and **Managed devices** folders. If you have configured devices to be moved to administration groups automatically (see section "Synchronization with cloud" on page [873](#)), the detected devices are included in administration groups.

To allow the Administration Server to poll cloud segments, you must have the rights provided with an IAM role (see section "Creating an IAM role for the Administration Server" on page [830](#)) or IAM user account (see section "Creating an IAM user account for work with Kaspersky Security Center" on page [833](#)) (in AWS), or with Application ID and password (see section "Creating a subscription, Application ID, and password" on page [843](#)) (in Azure), or with a Google client email, Google project ID, and private key (see section "Creating client email, project ID, and private key" on page [849](#)).

You can add and delete connections, as well as set the polling schedule for each cloud segment.

See also:

Scenario: Deployment for cloud environment.....	821
Adding connections for cloud segment polling	866
Deleting connections for cloud segment polling	868
Configuring the polling schedule	869

Adding connections for cloud segment polling

► *To add a connection for cloud segment polling to the list of available connections:*

1. In the console tree, select the **Device discovery** → **Cloud** node.
2. In the workspace of the window, click **Configure polling**.
A properties window opens containing a list of connections available for cloud segment polling.
3. Click the **Add** button.
The **Connection** window opens.
4. Specify the name of the cloud environment for the connection that will be used for further polling of the cloud segment:

- **Cloud environment**

The environment in which the EC2 instances (or virtual machines) are located can be Amazon Web Services (AWS), Microsoft Azure, or Google Cloud.

If you selected AWS, specify the following settings:

- **Connection name**

Enter a name for the connection. The name cannot contain more than 256 characters. Only Unicode characters are permitted.

This name will also be used as the name for the administration group for the cloud devices.

If you plan to work with more than one cloud environment, you might want to include the name of the environment in the connection name, for example, "Azure Segment," "AWS Segment," or "Google Segment."

- **Use AWS IAM role**

Select this option if you have already created an IAM role for the Administration Server to use AWS services (see section "Creating an IAM role for the Administration Server" on page [830](#)).

- **Use AWS IAM user account**

Select this option if you have an IAM user account with the necessary permissions (see section "Creating an IAM user account for work with Kaspersky Security Center" on page [833](#)) and you can enter a key ID and secret key.

- **Access key ID**

The IAM access key ID is a sequence of alphanumeric characters. You received the key ID when you created the IAM user account (see section "Creating an IAM user account for work with Kaspersky Security Center" on page [833](#)).

The field is available if you selected an AWS IAM access key for authorization instead of an IAM role.

- **Secret key**

The secret key that you received with the access key ID when you created the IAM user account (see section "Creating an IAM user account for work with Kaspersky Security Center" on page [833](#)).

The characters of the secret key are displayed as asterisks. After you begin entering the

secret key, the **Show** button is displayed. Click and hold this button for the necessary amount of time to view the characters you entered.

The field is available if you selected an AWS IAM access key for authorization instead of an IAM role.

The Cloud Environment Configuration Wizard allows you to specify only a single AWS IAM access key. Subsequently, you can specify more connections to manage other cloud segments (see section "Adding connections for cloud segment polling" on page [866](#)).

If you selected Azure, specify the following settings:

- **Connection name**

Enter a name for the connection. The name cannot contain more than 256 characters. Only Unicode characters are permitted.

This name will also be used as the name for the administration group for the cloud devices.

If you plan to work with more than one cloud environment, you might want to include the name of the environment in the connection name, for example, "Azure Segment," "AWS Segment," or "Google Segment."

- **Azure Application ID**

You created (see section "Creating a subscription, Application ID, and password" on page [843](#)) this application ID on the Azure portal.

You can provide only one Azure Application ID for polling and other purposes. If you want to poll another Azure segment, you must first delete the existing Azure connection.

- **Azure Subscription ID**

You created (see section "Creating a subscription, Application ID, and password" on page [843](#)) the subscription on the Azure portal.

- **Azure Application password**

You received the password of the Application ID when you created the Application ID (see section "Creating a subscription, Application ID, and password" on page [843](#)).

The characters of the password are displayed as asterisks. After you begin entering the password, the **Show** button becomes available. Click and hold this button to view the characters you entered.

- **Azure storage account name**

You created the name of the Azure storage account (see section "Creating Azure storage account" on page [846](#)) for working with Kaspersky Security Center.

- **Azure storage access key**

You received a password (key) when you created Azure storage account for working with Kaspersky Security Center.

The key is available in section "Overview of the Azure storage account", in subsection "Keys".

If you selected Google Cloud, specify the following settings:

- **Connection name**

Enter a name for the connection. The name cannot contain more than 256 characters. Only Unicode characters are permitted.

This name will also be used as the name for the administration group for the cloud devices.

If you plan to work with more than one cloud environment, you might want to include the name of the environment in the connection name, for example, "Azure Segment," "AWS Segment," or "Google Segment."

- **Client email**
- **Project ID**
- **Private key**

1. If you want, select **Set polling schedule** and change the default settings (see section "Configuring the polling schedule" on page [869](#)).

The connection is saved in the application settings.

After the new cloud segment is polled for the first time, the subgroup corresponding to that segment appears in the **Managed devices\Cloud** administration group.

If you specify incorrect credentials, no instances will be found during cloud segment polling and a new subgroup will not appear in the **Managed devices\Cloud** administration group.

See also:

Scenario: Deployment for cloud environment.....[821](#)

Deleting connections for cloud segment polling

If you no longer have to poll a specific cloud segment, you can delete the connection corresponding to that segment from the list of available connections. You can also delete a connection if, for example, permissions to poll a cloud segment have been transferred to another AWS IAM user with a different key.

► *To delete a connection:*

1. In the console tree, select the **Device discovery** → **Cloud** node.
2. In the workspace of the window, select **Configure polling**.
A window opens containing a list of connections available for cloud segment polling.
3. Select the connection that you want to delete and click the **Delete** button in the right part of the window.
4. In the window that opens, click the **OK** button to confirm your selection.

If you are deleting connections from the list of available connections, the devices that are in the corresponding segments are automatically deleted from the corresponding administration groups.

See also:

Scenario: Deployment for cloud environment.....[821](#)

Configuring the polling schedule

Cloud segment polling is performed according to schedule. You can set the polling frequency.

The polling frequency is automatically set at 5 minutes by the Cloud Environment Configuration Wizard. You can change this value at any time and set a different schedule. However, it is not recommended to configure polling to run more frequently than every 5 minutes, because this could lead to errors in the API operation.

► *To configure a cloud segment polling schedule:*

1. In the console tree, select the **Device discovery** → **Cloud** node.
2. In the workspace, click **Configure polling**.

The cloud properties window opens.

3. In the list, select the connection you want and click the **Properties** button.

The connection properties window opens.

4. In the properties window, click the **Set polling schedule** link.

The **Schedule** window opens.

5. Define the following settings:

- **Scheduled start**

Polling schedule options:

- **Every N days**

The polling runs regularly, with the specified interval in days, starting from the specified date and time.

By default, the polling runs every day, starting from the current system date and time.

- **Every N minutes**

The polling runs regularly, with the specified interval in minutes, starting from the specified time.

By default, the polling runs every five minutes, starting from the current system time.

- **By days of week**

The polling runs regularly, on the specified days of week, and at the specified time.

By default, the polling runs every Friday at 6:00:00 P.M.

- **Every month on specified days of selected weeks**

The polling runs regularly, on the specified days of each month, and at the specified time.

By default, no days of month are selected; the default start time is 6:00:00 P.M.

- **Run missed tasks**

If the Administration Server is switched off or unavailable during the time for which the poll is scheduled, the Administration Server can either start the poll immediately after it is switched on, or wait for the next time for which the poll scheduled.

If this option is enabled, the Administration Server starts polling immediately after it is switched on.

If this option is disabled, the Administration Server waits for the next time for which the

polling is scheduled.

By default, this option is enabled.

6. Click **OK** to save the changes.

The polling schedule is configured and saved.

See also:

Scenario: Deployment for cloud environment [821](#)

Installing applications on devices in a cloud environment

You can install the following Kaspersky applications on the devices in a cloud environment: Kaspersky Security for Windows Server (for Windows devices) and Kaspersky Endpoint Security for Linux (for Linux devices).

Client devices on which you intend to install protection must meet the requirements for Kaspersky Security Center operation in a cloud environment (see section "Prerequisites for client devices in a cloud environment necessary for work with Kaspersky Security Center" on page [852](#)). You must have a valid license to install applications on AWS instances, Microsoft Azure virtual machines or Google virtual machine instances.

Kaspersky Security Center 13 supports the following scenarios:

- A client device is discovered by means of an API; the installation is also performed by means of an API. For AWS and Azure cloud environments, this scenario is supported.
- A client device is discovered by means of Active Directory polling, Windows domains polling, or IP range polling; the installation is performed by means of Kaspersky Security Center.
- A client device is discovered by means of Google API; the installation is performed by means of Kaspersky Security Center. For Google Cloud, only this scenario is supported.

Other ways of installation of the applications are not supported.

To install applications on virtual devices, use installation packages (see section "Creating installation packages of applications" on page [717](#)).

► *To create a task for remote installation of the application on instances by using AWS API or Azure API:*

1. In the console tree, select the **Tasks** folder.
2. Click the **New task** button.

The New Task Wizard starts. Follow the instructions of the Wizard.

3. On the **Select the task type** page, select **Install application remotely** as the task type.
4. On the **Select devices** page, select the relevant devices from the **Managed devices\Cloud** group.
5. If Network Agent has not yet been installed on the devices on which you are intending to install the application, on the **Selecting an account to run the task** page select **Account required (Network Agent is not used)** and click the **Add** button in the right part of the window. In the menu that appears, select one of the following:
 - **Cloud account**

Select this option if you want to install applications on instances in AWS and you have an AWS IAM access key with the required permissions but do not have an IAM role. Also select this option if you want to install applications on devices in the Azure environment.

In the window that opens, provide Kaspersky Security Center with credentials that grant you rights to install applications on the relevant devices (see section "Step 3. Authorization in the cloud environment" on page [856](#)).

Select the cloud environment: AWS or Azure.

In the **Account name** field, enter a name for these credentials. You will see this name in the list of the accounts to run the task.

If you selected AWS, in the **Access key ID** and **Secret key** fields, enter the credentials for the IAM user account that has the rights to install applications on the specified devices.

If you selected Azure, in the **Azure subscription ID** and **Azure Application password** fields enter the credentials for the Azure account that has the rights to install applications on the specified devices.

If you specify incorrect credentials, the remote installation task will end with an error on the devices for which it is scheduled.

- **Account**

For instances running Windows, select this option in case you do not intend to install the application using AWS or Azure API tools. In this case, make sure that the devices in your cloud segment meet the necessary conditions (see section "Forced deployment through the remote installation task of Kaspersky Security Center" on page [158](#)). Kaspersky Security Center installs applications on its own, without using AWS API or Azure API.

If you specify incorrect data, the remote installation task will end with an error on the devices for which it is scheduled.

- **IAM role**

Select this option if you want to install applications on the instances in the AWS environment and have an IAM role with the required rights (see section "Creating an IAM role for installation of applications on Amazon EC2 instances" on page [834](#)).

If you select this option, but do not have an IAM role with the required rights, the remote installation task will end with an error on the devices for which it is scheduled.

- **SSH certificate**

For instances running Linux, select this option in case you do not intend to install the application using AWS API or Azure API tools. In this case, make sure that the devices in your cloud segment meet the necessary conditions (see section "Forced deployment through the remote installation task of Kaspersky Security Center" on page [158](#)). Kaspersky Security Center installs applications on its own, without using AWS API or Azure API.

You can provide multiple credentials by clicking the **Add** button for each new one. If different cloud segments require different credentials, provide the credentials for all the segments.

After the Wizard finishes, the task for remote installation of the application appears in the list of tasks in the workspace of the **Tasks** folder.

In Microsoft Azure, remote installation of security applications on a virtual machine may result in deleting Custom Script Extension installed on this virtual machine.

See also:

Scenario: Deployment for cloud environment.....[821](#)

Viewing the properties of cloud devices

► *To view the properties of a cloud device:*

1. In the console tree, in the **Device discovery** → **Cloud** node, select the subnode that corresponds to the group where the relevant instance is located.

If you are unaware of the group where the relevant virtual device is located, use the search function:

- a. Right-click the name of the **Managed devices** → **Cloud** node, and then select **Search** in the context menu.
- b. In the window that opens, perform a search (see section "Device search settings" on page [916](#)).

If a device exists that meets the criteria that you set, its name and details will be displayed in the lower part of the window.

2. Right-click the name of the relevant node. In the context menu, select **Properties**.

In the window that opens, the object properties are displayed.

The **System Info** → **General system info** section contains the properties that are specific for devices in cloud environment:

- **Device discovered using API (AWS, Azure, or Google Cloud;** if the device cannot be detected by using API tools, the **No** value is displayed).
- **Cloud Region.**
- **Cloud VPC** (for AWS and Google Cloud devices only).
- **Cloud availability zone** (for AWS and Google Cloud devices only).
- **Cloud subnet.**
- **Cloud placement group** (this unit is only displayed if the instance belongs to a placement group; otherwise, it is not displayed).

You can click the **Export to file** button to export this information to a .csv or .txt file.

See also:

Scenario: Deployment for cloud environment.....[821](#)

Synchronization with cloud

During the Cloud Environment Configuration Wizard operation, the Synchronize with Cloud rule is created automatically. This rule allows you to automatically move instances detected in each poll, from the **Unassigned devices** group to the **Managed devices\Cloud** group, to make these instances available for centralized management. By default, the rule is active after it is created. You can disable, modify, or enforce the rule at any time.

► *To edit the properties of the Synchronize with Cloud rule and/or enforce the rule:*

1. In the console tree, right-click the name of the **Device discovery** node.
2. In the context menu, select **Properties**.
3. In the properties window that opens, in the **Sections** pane, select **Move devices**.
4. In the list of device moving rules in the workspace, select **Synchronize with Cloud** and then click the **Properties** button in the lower part of the window.

The rule properties window opens.

5. If necessary, specify the following settings in the **Cloud segments** settings group:

- **Device is in cloud segment**

The rule only applies to devices that are in the selected cloud segment. Otherwise, the rule applies to all devices that have been discovered.

By default, this property is selected.

- **Include child objects**

The rule applies to all devices in the selected segment and in all nested cloud subsections. Otherwise, the rule only applies to devices that are in the root segment.

By default, this option is selected.

- **Move devices from nested objects to corresponding subgroups**

If this option is enabled, devices from nested objects are automatically moved to the subgroups that correspond to their structure.

If this option is disabled, devices from nested objects are automatically moved to the root of the Cloud subgroup without any further branching.

By default, this option is enabled.

- **Create subgroups corresponding to containers of newly detected devices**

If this option is enabled, when the structure of the **Managed devices\Cloud** group has no subgroups that will match the section containing the device, Kaspersky Security Center creates such subgroups. For example, if a new subnet is discovered during device discovery, a new group with the same name will be created under the **Managed devices\Cloud** group.

If this option is disabled, Kaspersky Security Center does not create any new subgroups. For example, if a new subnet is discovered during network poll, a new group with the same name will not be created under the **Managed devices\Cloud** group, and the devices that are in that subnet will be moved into the **Managed devices\Cloud** group.

By default, this option is enabled.

- **Delete subgroups for which no match is found in the cloud segments**

If this option is enabled, the application deletes from the Cloud group all the subgroups that do not match any existing cloud objects.

If this option is disabled, subgroups that do not match any of the existing cloud objects are retained.

By default, this option is enabled.

If you enabled the **Synchronize with Cloud** option when running the Cloud Environment Configuration Wizard, the Synchronize with Cloud rule is created with the **Create subgroups corresponding to containers of newly detected devices** and **Delete subgroups for which no match is found in the cloud segments** check boxes selected.

If you did not enable **Synchronize with Cloud** option, the Synchronize with Cloud rule is created with these options disabled (cleared). If your work with Kaspersky Security Center requires that the structure of subgroups in the **Managed devices\Cloud** subgroup matches the structure of cloud segments, enable the **Create subgroups corresponding to containers of newly detected devices** and **Delete subgroups for which no match is found in the cloud segments** options in the rule properties, and then enforce the rule.

6. In the **Device discovered using API** drop-down list, select one of the following values:
 - **AWS**. The device is discovered by using AWS API, that is, the device definitely is in the AWS cloud environment.
 - **Azure**. The device is discovered by using Azure API, that is, the device definitely is in the Azure cloud environment.
 - **Google Cloud**. The device is discovered by using Google API, that is, the device definitely is in the Google cloud environment.
 - **No**. The device cannot be detected by using AWS, Azure or Google API, that is, it is either outside the cloud environment, or it is in the cloud environment but it cannot be detected by using an API for some reason.
 - **No value**. This criterion cannot be applied.
7. If necessary, set up other rule properties in other sections (see section "Device search settings" on page [916](#)).
8. If necessary, enforce the rule by clicking the **Force** button in the lower part of the window.

The Rule Execution Wizard starts. Follow the instructions of the Wizard. When the Wizard finishes, the rule will be run and the structure of subgroups in the **Managed devices\Cloud** subgroup will match the structure of your cloud segments.

9. Click the **OK** button.

The properties are set up and saved.

► *To disable the Synchronize with Cloud rule:*

1. In the console tree, right-click the name of the **Device discovery** node.
2. In the context menu, select **Properties**.
3. In the properties window that opens, in the **Sections** pane, select **Move devices**.
4. In the list of device moving rules in the workspace, disable (clear) the **Synchronize with Cloud** option and click **OK**.

The rule is disabled and will no longer be applied.

See also:

Scenario: Deployment for cloud environment	821
--	---------------------

Using deployment scripts for deploying security applications

When Kaspersky Security Center is deployed in a cloud environment, you can use deployment scripts for automating the deployment of security applications. The deployment scripts for the Amazon Web Services, Microsoft Azure, and Google Cloud are available as ZIP files at the Kaspersky Support page.

You can deploy the latest versions of Kaspersky Endpoint Security for Linux and Kaspersky Security for Windows Server by using deployment scripts only if you already have created installation packages and management plugins for these programs. To deploy the latest versions of the security applications by using deployment scripts, perform the following on the Administration Server in the cloud environment:

1. Run the Cloud Environment Configuration Wizard (on page [853](#)).
2. Follow the instructions provided at <https://support.kaspersky.com/14713>
<https://support.kaspersky.com/14713>.

See also:

Scenario: Deployment for cloud environment.....[821](#)

Deployment of Kaspersky Security Center in Yandex.Cloud

Information given in this section is only applicable for users in Russia and other countries where Yandex services are in use. This section describes a feature only available in Kaspersky Security Center 12.2 or later versions.

You can deploy Kaspersky Security Center in Yandex.Cloud. Only the pay-per-use mode is available; cloud databases are not supported.

In Yandex.Cloud, the following deployment methods for the security applications are available:

- By native means of Kaspersky Security Center, that is, via the *Remote installation* task (the deployment of the security programs is only possible if Administration Server and the virtual machines to be protected are on the same network segment)
- Via deployments scripts (see section "Using deployment scripts for deploying security applications" on page [876](#))

For deployment of Kaspersky Security Center in Yandex.Cloud, you must have a service account in Yandex.Cloud. You must give this account the marketplace.meteringAgent permission and associate this account with the virtual machine (please refer to <https://cloud.yandex.ru> <https://cloud.yandex.ru> for details).

Troubleshooting

This section provides information about the most frequent errors and problems encountered when deploying and using Kaspersky Security Center, as well as recommendations on how to solve those issues.

In this chapter

Problems with remote installation of applications.....	878
Incorrect copying of a hard drive image	881
Problems with Exchange Mobile Device Server.....	882
Problems with iOS MDM Server	883
Problems with KES devices.....	885
Problems with tasks when using Administration Server as WSUS server	886

Problems with remote installation of applications

The table below lists problems that may be encountered when installing applications remotely, as well as common causes of those issues.

Table 71. Problems with remote installation of applications

Issue	Common causes and solutions
Installation rights are inadequate	The account under which installation is running has insufficient rights to execute the operations required to install the application.
Low disk space	Not enough free disk space for installation completion. Free up more disk space and retry the operation.
Unplanned OS restart	An unplanned restart of the OS has occurred during installation, the exact result of installation may be unavailable. Check the installer's settings for correctness or contact Technical Support.
Required file not found	A required file has not been found in the installation package. Check your installation package for integrity.
Incompatible platform	The installation package is not intended for this platform. Use a dedicated installation package.
Incompatible application	An application, which is incompatible with the application being installed, is already installed on the device. Before starting the installation, remove all applications that are listed as incompatible.
Poor system requirements	The installation package requires some additional software in the system. Check whether the system configuration meets the system requirements of the application being installed.
Incomplete installation	The previous installation or removal of the application has not completed normally. To complete the previous installation or removal of the application on this device, you need to restart the OS and retry the installation process.
Wrong version of installer	Installation of this installation package is not supported by the current version of the installer on this device.
Installation already running	Installation of another application has already been started on this device.
Could not open installation package	Possible cause: the package is missing, the package is corrupted, or not enough rights to access the package.
Incompatible localization	The installation package is not intended for installation on this localization of the OS.
Installation blocked by policy	Installation of applications on this device is prohibited by a policy.
Error writing file	A writing error has occurred during the application installation. Check the account under which installation has been run for required rights, and evaluate the free disk space.
Invalid uninstall password	The password for application removal has been incorrect.
Poor hardware requirements	The system hardware does not meet the application requirements (RAM, free space on the hard drive, etc.)
Invalid installation folder	The application cannot be installed in the specified folder as it is prohibited by the installer's policy.
New installation attempt required after restart	You need to run the application installer again after restarting the device.

Issue	Common causes and solutions
Restart required to continue installation	To proceed with the installer, you have to restart the device.

Incorrect copying of a hard drive image

If a hard drive image with Network Agent installed has been copied without following the rules of deployment (see section "Deployment by capturing and copying the hard drive image of a device" on page [154](#)), some devices may be displayed together in Administration Console under a single icon with a name that changes constantly.

You can resolve this issue using one of the following methods:

- Removing Network Agent

This method is the most reliable. You must remove Network Agent on devices that have been incorrectly copied from the image, using third-party tools, and then install it again. Network Agent cannot be removed through Kaspersky Security Center tools, because Administration Server cannot distinguish between faulty devices (they all share the same icon in Administration Console).

- Running the klmover utility with the "-dupfix" key

Use third-party tools to run the klmover utility, located in the Network Agent installation folder, with the "-dupfix" key (klmover -dupfix) once on faulty devices (those incorrectly copied from the image). You cannot run the utility with Kaspersky Security Center tools, because Administration Server cannot distinguish between faulty devices (they all share the same icon in Administration Console).

Then delete the icon on which the faulty devices had been displayed before you run the utility.

- Toughening up the rule for detection of incorrectly copied devices.

This method is only applicable if Administration Server and Network Agents version 10 Service Pack 1 or later are installed.

The rule for detection of incorrectly copied Network Agents must be toughened so that changing the NetBIOS name of a device results in an automatic "fix" of those Network Agents (with the assumption that all of the copied devices have unique NetBIOS names).

On the device with Administration Server, you must import the reg file shown below to the Registry and then restart the Administration Server service.

- If a 32-bit operating system is installed on the device with Administration Server:

```
REGEDIT4
[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags]
"KLSRV_CheckClones"=dword:00000003
```

- If a 64-bit operating system is installed on the device with Administration Server:

```
REGEDIT4
[HKEY_LOCAL_MACHINE\SOFTWAREWow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags]
"KLSRV_CheckClones"=dword:00000003
```

Problems with Exchange Mobile Device Server

This section provides information about errors and problems that may be encountered when using Exchange Mobile Device Server.

Error during installation of Exchange Mobile Device Server

If an error occurred during a local or remote installation, you can find out the cause of the error by viewing the error.log file located on the device where the application installation has been run, at C:\Windows\Temp\klmdm4exch-2014-11-28-15-56-37\ (numbers stand for the application installation date and time). As a rule, information from the file error.log is enough for solving the problem.

The table below lists examples of the most common errors logged in the error.log file.

Table 72. Common errors

Error	Description	Cause
Error occurred on installation step: 'Test connection to PowerShell'	Error: Processing data from remote server failed with the following error message: The user "oreh-security.ru/Users/TestInstall" isn't assigned to any management roles.	The account under which the application installation has been run, does not have the Organization Management role.
Error occurred on installation step: 'Test connection to PowerShell'	Connecting to remote server failed with the following error message: The WinRM client cannot process the request. The authentication mechanism requested by the client is not supported by the server or unencrypted traffic is disabled in the service configuration. Verify the unencrypted traffic setting in the service configuration or specify one of the authentication mechanisms supported by the server. To use Kerberos, specify the computer name as the remote destination. Also verify that the client computer and the destination computer are joined to a domain. To use Basic, specify the computer name as the remote destination, specify Basic authentication and provide user name and password. Possible authentication mechanisms reported by server: Digest For more information, see the about_Remote_Troubleshooting Help topic.	Windows authentication mechanism is not enabled in the settings of IIS web server for PowerShell virtual directory.

List of devices and mail accounts is empty

To find out the cause, which makes it impossible to retrieve the list of devices and mail accounts, you can view the events saved in Administration Console, in the Administration Server node, on the **Events** tab in the **Functional failures** event selection. If the events contain no information, check the connection between the Administration Server and Network Agent on the device with Exchange Mobile Device Server deployed.

Problems with iOS MDM Server

This section provides information about errors and problems that may be encountered when using iOS MDM Server, as well as ways of solving those issues.

In this section

Portal support.kaspersky.com	883
Checking APNs service for accessibility.....	883
Recommended procedure for solving problems with iOS MDM web service	883

Portal support.kaspersky.com

Information about some of the problems that occur when using iOS MDM Server is given in the Knowledge Base on Technical Support website <http://support.kaspersky.com/ks10mob>.

Checking APNs service for accessibility

To check APNs service for accessibility, you can use the following commands from the utility Telnet:

- From the iOS MDM web service side:

```
$ telnet gateway.push.apple.com 2195
```

- From the iOS MDM device side (the check must be performed from the network on which the device is located):

```
$ telnet 1-courier.push.apple.com 5223
```

Recommended procedure for solving problems with iOS MDM web service

- ▶ *If you encounter some problems when using iOS MDM web service, perform the following actions:*
 1. Check the certificates for accuracy.
 2. Check the events of Administration Console for errors and incomplete commands from iOS MDM Server.
 3. Check the mobile device through the iPhone Configuration Utility console.
 4. Check the trace files of the iOS MDM web service: Internal services, such as the RPC service and web service (100 streams), must be running successfully.

Checking the certificate of iOS MDM web service for accuracy using an OpenSSL-based cross-platform utility

Example of a command:

```
$ openssl s_client -connect mymdm.mycompany.com:443
```

Execution result

```
CONNECTED(00000003)
```

```
...
```

```
---
```

Certificate chain

```
0 s:/C=RU/ST=Msk/L=Msk/O=My Company/OU=AdminKit/CN=mymdm.mycompany.com  
i:/CN=Kaspersky iOS MDM Server CA
```

```
...
```

```
.
```

Checking trace files of the iOS MDM web service

To find out how to receive trace files of the iOS MDM web service, please refer to the relevant article in the Knowledge Base on Technical Support website <http://support.kaspersky.com/9792>.

Example of successful tracing:

```
I1117 20:58:39.050226 7984] [MAIN]: Starting service...  
I1117 20:58:39.050226 7984] [RPC]: Starting rpc service...  
...  
I1117 20:58:39.081428 7984] [RPC]: Rpc service started  
I1117 20:58:39.081428 3724] [WEB]: Starting web service...  
I1117 20:58:39.455832 3724] [WEB]: Starting thread [T000]  
I1117 20:58:39.455832 3724] [WEB]: Starting thread [T001]  
...  
I1117 20:58:39.455832 3724] [WEB]: Starting thread [T099]
```

Example of tracing with an occupied socket:

```
[WEB]: Starting web service...  
Error 28 fault: SOAP-ENV:Server [no subcode] "Only one usage of each socket  
address (protocol/network address/port) is normally permitted."  
Detail: [no detail]  
[WEB]: Web service terminated
```

Checking trace files using the console of iPhone Configuration Utility

Example of successful tracing:

```
Services covering MDM - profiled, mdmd  
mdmd[174] <Notice>: (Note) MDM: mdmd starting...  
mdmd[174] <Notice>: (Note) MDM: Looking for managed app states to clean up  
profiled[175] <Notice>: (Note) profiled: Service starting...  
mdmd[174] <Notice>: (Note) MDM: Network reachability has changed.  
mdmd[174] <Notice>: (Note) MDM: Network reachability has changed.  
mdmd[174] <Notice>: (Note) MDM: Polling MDM server https://10.255.136.71 for  
commands  
mdmd[174] <Notice>: (Note) MDM: Transaction completed. Status: 200  
mdmd[174] <Notice>: (Note) MDM: Attempting to perform MDM request:  
DeviceLock  
mdmd[174] <Notice>: (Note) MDM: Handling request type: DeviceLock  
mdmd[174] <Notice>: (Note) MDM: Command Status: Acknowledged  
profiled[175] <Notice>: (Note) profiled: Recomputing passcode requirement  
message  
profiled[175] <Notice>: (Note) profiled: Locking device  
mdmd[174] <Notice>: (Note) MDM: Transaction completed. Status: 200  
mdmd[174] <Notice>: (Note) MDM: Server has no commands for this device.  
mdmd[174] <Notice>: (Note) MDM: mdmd stopping...
```

Problems with KES devices

This section provides information about errors and problems that may be encountered when using KES devices, as well as ways of solving those issues.

In this section

Portal support.kaspersky.com	886
Checking the settings of Google Firebase Cloud Messaging service	886
Checking Google Firebase Cloud Messaging for accessibility.....	886

Portal support.kaspersky.com

Information about problems that may arise when using KES devices is given in the Knowledge Base on Technical Support website <http://support.kaspersky.com/ks10mob>.

Checking the settings of Google Firebase Cloud Messaging service

You can check the Google Firebase Cloud Messaging settings on the Google portal <https://console.developers.google.com/>.

Checking Google Firebase Cloud Messaging for accessibility

To check Google Firebase Cloud Messaging for accessibility from the Kaspersky Security Center side (see section "Using Google Firebase Cloud Messaging" on page [211](#)), you can use the following Telnet command:

```
telnet android.googleapis.com 443
```

Problems with tasks when using Administration Server as WSUS server

If the Administration Server acts as a WSUS server, the results of the *Find vulnerabilities and required updates* task or the *Install required updates and fix vulnerabilities* task may contain a warning of the 0x80240033 "Windows Update Agent error 80240033 ("License terms could not be downloaded.")" error. In this case, you have to ensure the correct completion of the task (or tasks).

► *To ensure correct completion of tasks:*

1. Open the Windows Registry of the device that has Administration Server installed and add a new DWORD (32-bit) value flag (KLWUS_TREAT_EULA_TEXT_ERROR_AS_EULA_EXIST=1) to the corresponding directory:
 - HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags for 32-bit systems
 - HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags for 64-bit systems
2. Use the klscflag utility to set up the flag. To do this, enter the following command at the Windows command prompt: `klscflag.exe -fset -pv klserver -n KLWUS_TREAT_EULA_TEXT_ERROR_AS_EULA_EXIST -t d -v 1.`

3. Restart the Administration Server device and run the *Find vulnerabilities and required updates* task or the *Install required updates and fix vulnerabilities* task again. The error will still persist after the task finishes, but the updates will be installed successfully.

Appendices

This section provides reference information and additional facts regarding the use of Kaspersky Security Center.

In this chapter

Advanced features	888
Features of using the management interface	895
Reference information	901
Searching and exporting data	914
Settings of tasks	928
Global list of subnets	941
Usage of Network Agent for Windows, for macOS and for Linux: comparison	942

Advanced features

This section describes a range of additional options of Kaspersky Security Center designed for expanding the functionality of centralized management of applications on devices.

In this section

Kaspersky Security Center operation automation. klakaut utility	889
Custom tools	889
Network Agent disk cloning mode	889
Preparing a reference device with Network Agent installed for creating an image of operating system ...	890
Configuring receipt of messages from File Integrity Monitor	891
Administration Server maintenance	892
User notification method window	893
General section	894
Device selection window	894
Define the name of the new object window	894
Application categories section	894
About multi-tenant applications	895

Kaspersky Security Center operation automation. klakaut utility

You can automate the Kaspersky Security Center operation using the klakaut utility. The klakaut utility and a Help system for it are located in the Kaspersky Security Center installation folder.

Custom tools

Kaspersky Security Center allows you to create a list of *custom tools* (hereinafter also referred to simply as *tools*), that is, applications activated for a client device in Administration Console, through the **Custom tools** group of the context menu. Each tool in the list will be associated with a separate menu command, which Administration Console uses to start the application corresponding to that tool.

The applications starts on the administrator's workstation. The application can accept the attributes of a remote client device as command-line arguments (NetBIOS name, DNS name, or IP address). Connection to the remote device can be established through tunneling.

By default, the list of custom tools contains the following service programs for each client device:

- **Remote diagnostics** is a utility for remote diagnostics of Kaspersky Security Center.
- **Remote Desktop** is a standard Microsoft Windows component named Remote Desktop Connection.
- **Computer Management** is a standard Microsoft Windows component.

► *To add or remove custom tools, or to edit their settings,*

In the context menu of the client device, select **Custom tools** → **Configure custom tools**.

The **Custom tools** window opens. In this window you can add or remove custom tools, and edit their settings using the **Add**, **Modify**, and **Remove** (✗) buttons.

Network Agent disk cloning mode

Cloning the hard drive of a reference device is a popular method of software installation on new devices. If Network Agent is running in standard mode on the hard drive of the reference device, the following problem arises:

After the reference disk image with Network Agent is deployed on new devices, they are displayed in Administration Console under a single icon. This problem arises because the cloning procedure causes new devices to keep identical internal data, which allows the Administration Server to associate a device with an icon in Administration Console.

The special *Network Agent disk cloning mode* allows you to avoid problems with an incorrect display of new devices in Administration Console after cloning. Use this mode when you deploy software (with Network Agent) on new devices by cloning the disk.

In disk cloning mode, Network Agent keeps running but does not connect to the Administration Server. When exiting the cloning mode, Network Agent deletes the internal data, which causes Administration Server to associate multiple devices with a single icon in Administration Console. Upon completing the cloning of the reference device image, new devices are displayed in Administration Console properly (under individual icons).

Network Agent disk cloning mode use scenario

1. The administrator installs Network Agent on the reference device.

2. The administrator checks the Network Agent connection to the Administration Server using the `klmagchk` utility (see section "Manually checking the connection between a client device and the Administration Server. `klmagchk` utility" on page [643](#)).
3. The administrator enables the Network Agent disk cloning mode.
4. The administrator installs software and patches on the device, and restarts it as many times as needed.
5. The administrator clones the hard drive of the reference device on any number of devices.
6. Each cloned copy must meet the following conditions:
 - a. The device name must be changed.
 - b. The device must be restarted.
 - c. The disk cloning mode must be disabled.

Enabling and disabling the disk cloning mode using the `klmover` utility

► *To enable or disable the Network Agent disk cloning mode:*

1. Run the `klmover` utility on the device with Network Agent installed that you have to clone.
The `klmover` utility is located in the Network Agent installation folder.
2. To enable the disk cloning mode, enter the following command at the Windows command prompt:
`klmover -cloningmode 1`.
Network Agent switches to disk cloning mode.
3. To request the current status of the disk cloning mode, enter the following command at the command prompt: `klmover -cloningmode`.
The utility window shows whether the disk cloning mode is enabled or disabled.
4. To disable the disk cloning mode, enter the following command in the utility command line: `klmover -cloningmode 0`.

See also:

- Deployment by capturing and copying the hard drive image of a device [154](#)
- Preparing a reference device with Network Agent installed for creating an image of operating system ... [890](#)

Preparing a reference device with Network Agent installed for creating an image of operating system

You may want to create an operating system image of a reference device with Network Agent installed and then to deploy the image on the networked devices. In this case, you create an operating system image of a reference device on which the Network Agent has not yet been started. If you start the Network Agent on a reference device before creating an operating system image, Administration Server's identification of devices deployed from an operating system image of the reference device will be problematic.

► *To prepare the reference device for creating an image of the operating system:*

1. Make sure that the Windows operating system is installed on the reference device and install the other software that you need on that device.

2. On the reference device, in the Windows Network Connections settings, disconnect the reference device from the network where Kaspersky Security Center is installed.
3. On the reference device, start the local installation of Network Agent by using the setup.exe file.
The Kaspersky Security Center Network Agent Setup Wizard starts. Follow the instructions of the Wizard.
4. On the **Administration Server** page of the Wizard, specify the Administration Server IP address.
If you do not know the exact address of the Administration Server, enter localhost. You can change the IP address later by using the klmover utility (see section "Manually connecting a client device to the Administration Server. Klmover utility" on page [638](#)) with the `-address` key.
5. On the **Start application** page of the Wizard, disable the **Start application during installation** option.
6. When the Network Agent installation is complete, do not restart the device before creating an operating system image.
If you restart the device, you will have to repeat the whole process of preparing a reference device for creation of an operating system image.
7. On the reference device, in the command line, start the sysprep utility (see section "Configuring sysprep.exe utility" on page [716](#)) and execute the following command: `sysprep.exe /generalize /oobe /shutdown`.

The reference device is ready for creating an operating system image (see section "Creating installation packages of applications" on page [717](#)).

See also:

Network Agent disk cloning mode.....	889
Deployment by capturing and copying the hard drive image of a device	154

Configuring receipt of messages from File Integrity Monitor

Managed applications such as Kaspersky Security for Windows Server or Kaspersky Security for Virtualization Light Agent send messages from File Integrity Monitor to Kaspersky Security Center. Kaspersky Security Center also allows you to monitor any changes to critically important components of systems (such as web servers and ATMs) and promptly respond to breaches of the integrity of such systems. For these purposes, you can receive messages from the File Integrity Monitor component. The File Integrity Monitor component lets you monitor not only the file system of a device, but also its registry hives, firewall status, and the status of connected hardware.

You must configure Kaspersky Security Center to receive messages from the File Integrity Monitor component without using Kaspersky Security for Windows Server or Kaspersky Security for Virtualization Light Agent.

► To configure receipt of messages from File Integrity Monitor:

1. Open the system registry of the device on which Administration Server is installed (for example, locally, using the regedit command in the **Start** → **Run** menu).
2. Go to the following hive:
 - For a 64-bit system:

HKEY_LOCAL_MACHINE\SOFTWAREWow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags

- For a 32-bit system:

HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags

3. Create keys:

- Create the key KLSRV_EVP_FIM_PERIOD_SEC to specify the time period for counting the number of processed events. Specify the following settings:
 - a. Specify KLSRV_EVP_FIM_PERIOD_SEC as the key name.
 - b. Specify DWORD as the key type.
 - c. Specify a range of values for the time interval from 43 200 to 172 800 seconds. By default, the time interval is 86 400 seconds.
- Create the key KLSRV_EVP_FIM_LIMIT to limit the number of received events for the specified time interval. Specify the following settings:
 - a. Specify KLSRV_EVP_FIM_LIMIT as the key name.
 - b. Specify DWORD as the key type.
 - c. Specify a range of values for received events from 2 000 to 50 000. The default number of events is 20 000.
- Create the key KLSRV_EVP_FIM_PERIOD_ACCURACY_SEC to count events with accuracy up to a specific time interval. Specify the following settings:
 - a. Specify KLSRV_EVP_FIM_PERIOD_ACCURACY_SEC as the key name.
 - b. Specify DWORD as the key type.
 - c. Specify a range of values from 120 to 600 seconds. The default time interval is 300 seconds.
- Create the key KLSRV_EVP_FIM_OVERFLOW_LATENCY_SEC so that, after the specified amount of time, the application can check whether the number of events processed over the time interval is turning out to be less than the specified limit. This check is performed upon reaching the limit for receiving events. If this condition is met, the application resumes saving events to the database. Specify the following settings:
 - a. Specify KLSRV_EVP_FIM_OVERFLOW_LATENCY_SEC as the key name.
 - b. Specify DWORD as the key type.
 - c. Specify a range of values from 600 to 3 600 seconds. The default time interval is 1 800 seconds.

If the keys are not created, the default values are used.

4. Restart the Administration Server service.

The limits on receiving events from the File Integrity Monitor component will be configured. You can view the results of the File Integrity Monitor component in the reports named **Top 10 rules of File Integrity Monitor / System Integrity Monitoring that were triggered on devices most frequently** and **Top 10 devices with File Integrity Monitor / System Integrity Monitoring rules most frequently triggered**.

Administration Server maintenance

The Administration Server maintenance allows you to reduce the database volume, and improve the performance and operation reliability of the application. We recommend that you maintain the Administration Server at least every week.

The Administration Server maintenance is performed using the dedicated task. The application performs the following actions when maintaining the Administration Server:

- Checks the database for errors.
- Re-organizes database indexes.
- Updates the database statistics.
- Shrinks the database (if necessary).

The *Administration Server maintenance* task does not support MySQL and MariaDB. If MySQL or MariaDB is used as the DBMS, administrators will have to maintain the database on their own.

► *To create an Administration Server maintenance task:*

1. In the console tree, select the node of the Administration Server for which you want to create an *Administration Server maintenance* task.
2. Select the **Tasks** folder.
3. By clicking the **New task** button in the workspace of the **Tasks** folder.
The New Task Wizard starts.
4. In the **Select the task type** window of the Wizard, select **Administration Server maintenance** as the task type and click **Next**.
5. If you have to shrink the Administration Server database during maintenance, in the **Settings** window of the Wizard, select the **Shrink database** check box.
6. Follow the rest of the Wizard instructions.

The newly created task is displayed in the list of tasks in the workspace of the **Tasks** folder. Only one *Administration Server maintenance* task can be running for a single Administration Server. If an *Administration Server maintenance* task has already been created for an Administration Server, no new *Administration Server maintenance* task can be created.

User notification method window

In the **User notification method** window, you can configure the user notification about certificate installation on the mobile device:

- **Show link in Wizard.** If you select this option, a link to the installation package will be shown at the final step of the New Device Connection Wizard.
- **Send link to user.** If you select this option, you can specify the settings for notifying the user about connection of a device.

In the **By email** group of settings, you can configure user notification about installation of a new certificate on his or her mobile device using email messages. This notification method is only available if the SMTP Server (see section "Step 8. Configuring email notifications" on page [271](#)) is enabled.

In the **By SMS** group of settings, you can configure the user notification about installation of a certificate on his or her mobile device by using SMS. This notification method is only available if SMS notification is enabled.

Click the **Edit message** link in the **By email** and **By SMS** groups of settings to view and edit the notification message, if necessary.

See also:

Installing a certificate for a user711

General section

In this section, you can adjust the general profile settings for Exchange ActiveSync mobile devices:

- **Name**

Profile name.

- **Allow non-provisionable devices**

If this check box is selected, devices that cannot access all of the settings of the Exchange ActiveSync policy, are also allowed to connect to the Mobile devices server.

If the check box is cleared, such devices are not allowed to connect to the Mobile device server.

By default, this check box is selected.

- **Updating frequency (hours)**

If this check box is selected, the application refreshes information about the Exchange ActiveSync policy with the frequency specified in the entry field.

If the check box is cleared, information about the Exchange ActiveSync policy is not refreshed.

The check box is selected by default, and the refreshing interval is one hour.

Device selection window

Choose a selection from the **Device selection** list. The list contains the default selections and the selections created by the user.

You can view the details of device selections in the workspace of the **Device selections** section.

Define the name of the new object window

In the window, specify the name of the newly created object. A name cannot be more than 100 characters long and cannot include any special characters (*<>?\\:|).

Application categories section

In this section, you can configure the distribution of information about application categories on client devices.

Full data transmission (for Network Agents Service Pack 2 and earlier)

If this option is selected, all data from an application category will be transmitted to client devices after that category is modified. This data transmission option is used with Network Agent Service Pack 2 and earlier versions.

Transmission of modified data only (for Network Agents Service Pack 2 and later)

If this option is selected, when an application category is modified, only modified data will be transmitted to client devices, not all data from that category. This data transmission option is used with Network Agent Service Pack 2 and later versions.

See also:

Creating application categories for Kaspersky Endpoint Security for Windows policies.....[487](#)

About multi-tenant applications

Kaspersky Security Center enables administrators of service providers and tenant administrators to use Kaspersky applications with multitenancy support. After a multi-tenant Kaspersky application is installed in the infrastructure of a service provider, tenants can start using the application.

To separate tasks and policies related to different tenants, you must create a dedicated virtual Administration Server in Kaspersky Security Center for each tenant. All tasks and policies for multi-tenant applications running for a tenant must be created for the Managed devices administration group of the virtual Administration Server corresponding to that tenant. The tasks created for the administration groups related to the primary Administration Server do not affect the devices of tenants.

Unlike service provider administrators, a tenant administrator can create and view tasks and application policies only for the devices of the corresponding tenant. The sets of tasks and policy settings available to service provider administrators and tenant administrators are different. Some of the tasks and policy settings are not available to tenant administrators.

Within a hierarchical structure of a tenant, the policies created for multi-tenant applications are inherited to lower-level administration groups as well as to upper-level administration groups: the policy is propagated to all client devices that belong to the tenant.

Features of using the management interface

This section describes actions that you can perform in the main window of Kaspersky Security Center.

In this section

Console tree	896
How to return to a properties window that disappeared	900
How to update data in the workspace	900
How to navigate the console tree	900
How to open the object properties window in the workspace.....	901
How to select a group of objects in the workspace	901
How to change the set of columns in the workspace	901

Console tree

The console tree (see the figure below) is designed to display the hierarchy of Administration Servers on the corporate network, the structure of their administration groups, and other objects of the application, such as the **Repositories** or **Application management** folders. The name space of Kaspersky Security Center can contain

several nodes including the names of servers corresponding to the installed Administration Servers included in the hierarchy.

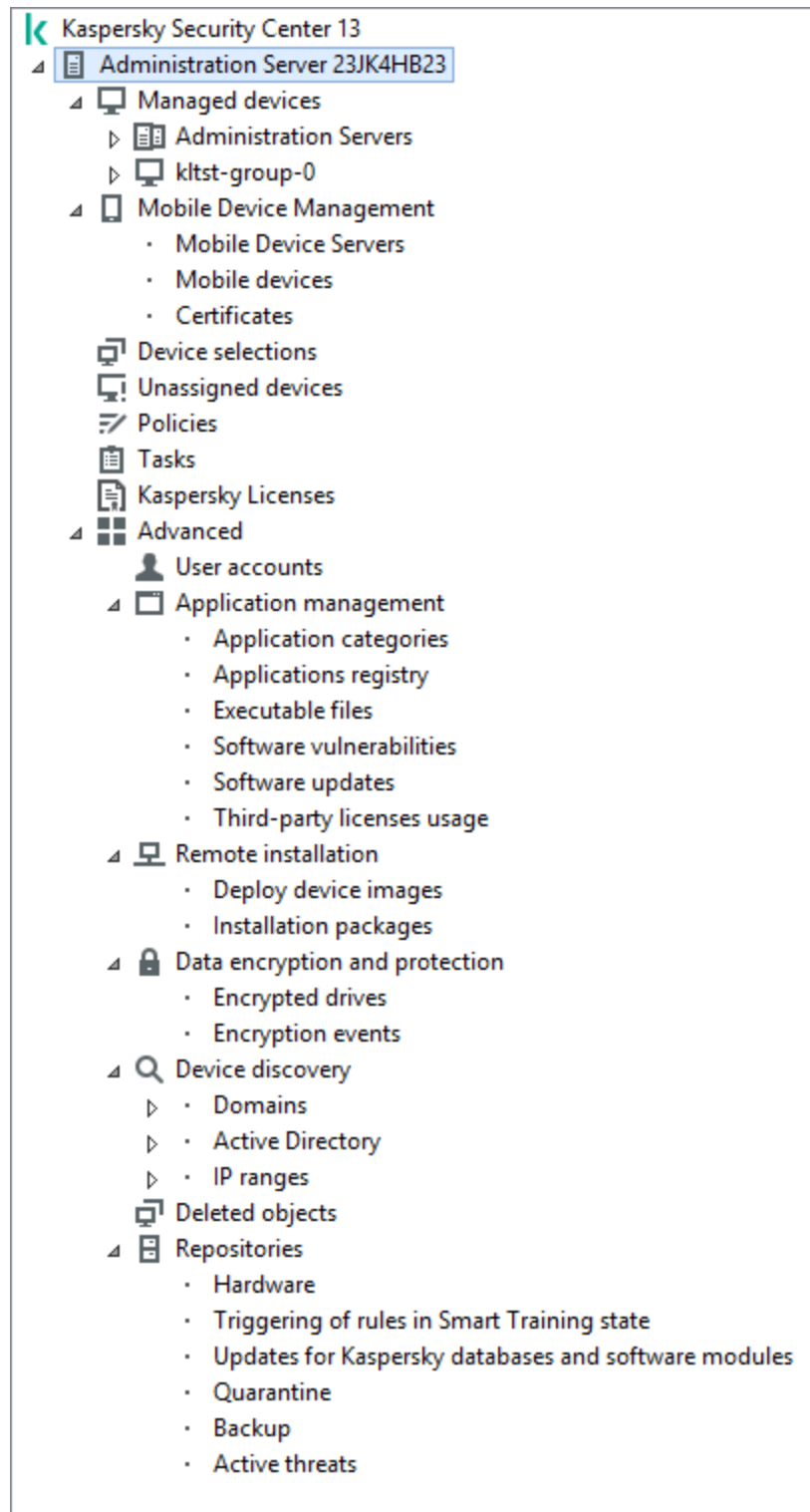


Figure 11. Console tree

Administration Server node

The **Administration Server – <Device name>** node is a container that shows the structural organization of the selected Administration Server.

The workspace of the **Administration Server** node contains summary information about the current status of the application and devices managed through the Administration Server. Information in the workspace is distributed between various tabs:

- **Monitoring.** Displays information about the application operation and the current status of client devices in real-time mode. Important messages for the administrator (such as messages on vulnerabilities, errors, or viruses detected) are highlighted in a specific color. You can use links on the **Monitoring** tab to perform the standard administrator tasks (for example, install and configure the security application on client devices), as well as to go to other folders in the console tree.
- **Statistics.** Contains a set of charts grouped by topics (protection status, Anti-Virus statistics, updates, etc.). These charts visualize current information about the application operation and the status of client devices.
- **Reports.** Contains templates for reports generated by the application. On this tab, you can create reports using preset templates, as well as create custom report templates.
- **Events** window. Contains records on events that have been registered during the application operation. Those records are distributed between topics for ease of reading and filtering. On this tab, you can view selections of events that have been generated automatically, as well as create custom selections.

Folders in the Administration Server node

The **Administration Server – <Device name>** node includes the following folders:

- **Managed devices.** This folder is intended for storage, display, configuration, and modification of the structure of administration groups, group policies, and group tasks.
- **Mobile Device Management.** This folder is intended for managing mobile devices. The **Mobile Device Management** folder contains the following subfolders:
 - **Mobile Device Servers.** Intended for managing iOS MDM Servers and Microsoft Exchange Mobile Devices Servers.
 - **Mobile Devices.** It is intended for managing mobile devices, KES, Exchange ActiveSync, and iOS MDM.
 - **Certificates.** It is intended for managing certificates of mobile devices.
- **Device selections.** This folder is intended for quick selection of devices that meet specified criteria (a device selection) among all managed devices. For example, you can quickly select devices on which no security application is installed, and proceed to these devices (view the list). You can perform specific actions on these selected devices, for example, assign them some tasks. You can use preset selections or create your own custom selections.
- **Unassigned devices.** This folder contains a list of devices that have not been included in any of the administration groups. You can perform some actions on unassigned devices, for example, move them into administration groups or install applications on them.
- **Policies.** This folder is intended for viewing and creating policies.
- **Tasks.** This folder is intended for viewing and creating tasks.
- **Kaspersky Licenses.** Contains a list of license keys available for Kaspersky applications. In the workspace of this folder, you can add new license keys to the license key repository, deploy license keys to managed devices, and view the license key usage report.

- **Advanced.** This folder contains a set of subfolders that correspond to various groups of application features.

Advanced folder. Moving folders in the console tree

The **Advanced** folder includes the following subfolders:

- **User accounts.** Contains a list of network user accounts.
- **Application management.** Intended for managing applications installed on devices on the network. The **Application management** folder contains the following subfolders:
 - **Application categories.** Intended for managing custom application categories.
 - **Applications registry.** Contains a list of applications on devices with Network Agent installed.
 - **Executable files.** Contains the list of executable files stored on client devices with Network Agent installed.
 - **Software vulnerabilities.** Contains a list of vulnerabilities in applications on devices with Network Agent installed.
 - **Software updates.** Contains a list of application updates received by Administration Server that can be distributed on devices.
 - **Third-party licenses usage.** Contains a list of licensed applications groups. You can use licensed applications groups to monitor the usage of licenses for third-party software (non-Kaspersky applications) and possible violations of licensing restrictions.
- **Remote installation.** This folder is intended for managing remote installation of operating systems and applications. The **Remote installation** folder contains the following subfolders:
 - **Deploy device images.** Intended for deploying images of operating systems on devices.
 - **Installation packages.** Contains a list of installation packages that can be used for remote installation of applications on devices.
- **Data encryption and protection.** This folder is intended for managing the process of data encryption on hard drives and removable drives.
- **Network poll.** This folder displays the network in which Administration Server is installed. Administration Server receives information about the structure of the network and its devices, through regular polls of the Windows network, IP subnets, and Active Directory® on the corporate network. Poll results are displayed in the workspaces of the corresponding folders: **Domains**, **IP ranges**, and **Active Directory**.
- **Repositories.** This folder is intended for operations with objects used to monitor the status of devices and perform maintenance. The **Repositories** folder contains the following subfolders:
 - **Adaptive anomaly detection.** Contains a list of detects performed by the Kaspersky Endpoint Security rules working in the SMART Training mode on client devices.
 - **Kaspersky software updates and patches.** Contains a list of updates received by Administration Server that can be distributed to devices.
 - **Hardware.** Contains a list of hardware connected to the organization's network.
 - **Quarantine.** Contains a list of objects moved to Quarantine by anti-virus applications on devices.
 - **Backup.** Contains a list of backup copies of files that were deleted or modified during disinfection on devices.
 - **Unprocessed files.** Contains a list of files assigned for later scanning by anti-virus applications.

You can change the set of subfolders included in the **Advanced** folder. Frequently used subfolders can be moved up one level from the **Advanced** folder. Subfolders that are used rarely can be moved to the **Advanced** folder.

► *To move a subfolder out of the **Advanced** folder:*

1. In the console tree, select the subfolder that you want to move out of the **Advanced** folder.
2. In the context menu of the subfolder, select **View** → **Move from Advanced folder**.

You can also move a subfolder out of the **Advanced** folder in the workspace of the **Advanced** folder by clicking the **Move from Advanced folder** link in the section with the name of that subfolder.

► *To move a subfolder to the **Advanced** folder:*

1. In the console tree, select the subfolder that you need to move to the **Advanced** folder.
2. In the context menu of the subfolder, select **View** → **Move to Advanced folder**.

How to return to a properties window that disappeared

Sometimes an open object properties window disappears from the screen. This happens because the properties window is covered by the main application window (this situation is characteristic of the Microsoft Management Console).


► *To go to the properties window that disappeared,*

Press **ALT+TAB**.

How to update data in the workspace



In Kaspersky Security Center, the workspace data (such as device statuses, statistics, and reports) are never updated automatically.


► *To update data in the workspace:*

- Press the **F5** key.
- In the context menu of the object in the console tree, select **Refresh**.
- Click the  button in the workspace.

How to navigate the console tree

To navigate the console tree, you can use the following toolbar buttons:

- —One step back.
- —One step forward.

- —One level up.

You can also use a navigation chain located in the upper-right corner of the workspace. The navigation chain contains the full path to the folder of the console tree in which you are currently located. All elements of the chain, except for the last one, are links to the objects in the console tree.

How to open the object properties window in the workspace

You can change the properties of the most Administration Console objects in the object properties window.

► *To open the properties window of an object located in the workspace:*

- From the context menu of the object, select **Properties**.
- Select an object and press **ALT+ENTER**.

How to select a group of objects in the workspace

You can select a group of objects in the workspace. You can select a group of objects, for example, to create a set of devices for which you may create tasks later.

► *To select an objects range:*

1. Select the first object in the range and press **SHIFT**.
2. Hold down the **SHIFT** key and select the last object in the range.

The range will be selected.

► *To group separate objects:*

1. Select the first object in the group and press **CTRL**.
2. Hold down the **CTRL** key and select other objects that you want to include in the group.

The objects will be grouped.

How to change the set of columns in the workspace

Administration Console allows you to change a set of columns displayed in the workspace.

► *To change a set of columns displayed in the workspace:*

1. In the console tree, click the object for which you wish to change the set of columns.
2. In the workspace of the folder, open the window intended for configuration of the set of columns by clicking the **Add/Remove columns** link.
3. In the **Add/Remove columns** window, specify the set of columns to be displayed.

Reference information

Tables of this section provide summary information about the context menu of Administration Console objects, as well as about the statuses of console tree objects and workspace objects.

In this section

Context menu commands.....	902
List of managed devices. Description of columns	905
Statuses of devices, tasks, and policies	910
File status icons in Administration Console	913

Context menu commands

This section lists Administration Console objects and corresponding context menu items (see table below).

Table 73. Items of the context menu of Administration Console objects

Object	Menu item	Menu item purpose
General items of context menu	Search	Opens the devices search window.
	Refresh	Refreshes the display of the selected object.
	Export list	Exports the current list to a file.
	Properties	Opens the properties window of the selected object.
	View → Add/Remove columns	Adds or removes columns to/from the table of objects in the workspace.
	View → Large icons	Shows objects in the workspace as large icons.
	View → Small icons	Shows objects in the workspace as small icons.
	View → List	Shows objects in the workspace as a list.
	View → Table	Shows objects in the workspace as a table.
	View → Configure	Configures the display of Administration Console elements.
Kaspersky Security Center	New → Administration Server	Adds an Administration Server to the console tree.
<Administration Server name>	Connect to Administration Server	Connects to the Administration Server.
	Disconnect from Administration Server	Disconnects from the Administration Server.

Object	Menu item	Menu item purpose
Managed devices	Install application	Starts the Application Remote Installation Wizard.
	View → Configure interface	Configures the display of interface elements.
	Remove	Removes the Administration Server from the console tree.
	Install application	Starts the Remote Installation Wizard for the administration group.
	Reset Virus Counter	Resets the virus counters for devices included in the administration group.
	View report on threats	Creates a report on threats and virus activity on devices included in the administration group.
	New → Group	Creates an administration group.
	All Tasks → New group structure	Creates a structure of administration groups based on the structure of domains or Active Directory.
	All Tasks → Show Message	Starts the New Message for User Wizard intended for the users of devices included in the administration group.
Managed devices → Administration Servers	New → Secondary Administration Server	Starts the Add Secondary Administration Server Wizard.
	New → Virtual Administration Server	Starts the New Virtual Administration Server Wizard.
Mobile Device Management → Mobile devices	New → Mobile device	Connects a new mobile device of the user.
Mobile Device Management → Certificates	New → Certificate	Creates a certificate.
	Create → Mobile device	Connects a new mobile device of the user.
Device selections	New → New selection	Creates a device selection.
	All Tasks → Import	Imports a selection from a file.

Object	Menu item	Menu item purpose
Kaspersky Licenses	Add activation code or key file	Adds a license key to the Administration Server repository.
	Activate Application	Starts the Application Activation Task Creation Wizard.
	Report on usage of license keys	Creates and shows a report on license keys on client devices.
Application management → Application categories	New → Category	Creates an application category.
Application management → Applications registry	Filter	Sets up a filter for the list of applications.
	Monitored Applications	Configures the publishing of events related to installation of applications.
	Remove applications that are not installed	Clears the list of all details of applications that are no longer installed on networked devices.
Application management → Software updates	Accept License Agreements for updates	Accepts the License Agreements of software updates.
Application management → Third-party licenses usage	New → Licensed applications group	Creates a licensed applications group.
Remote installation → Installation packages	Show current application versions	Shows the list of up-to-date versions of Kaspersky applications available on web servers.
	New → Installation package	Creates an installation package.
	All Tasks → Update databases	Updates application databases in installation packages.
	All Tasks → Show the general list of stand-alone packages	Shows the list of stand-alone packages created for installation packages.

Object	Menu item	Menu item purpose
Device discovery → Domains	All Tasks → Device Activity	Sets up the Administration Server's response to inactivity of networked devices.
Device discovery → IP ranges	New → IP range	Creates an IP range.
Repositories → Updates for Kaspersky databases and software modules	Download updates	Opens the properties window of the Download updates to the repository task of the Administration Server.
	Updates Download Settings	Configures the Download updates to the repository task of the Administration Server.
	Report on usage of anti-virus databases	Creates and shows a report on versions of databases.
	All Tasks → Clear updates repository	Clears the repository of updates on the Administration Server.
Repositories → Hardware	New → Device	Creates a new device.

List of managed devices. Description of columns

The following table displays the names and respective descriptions of columns in the list of managed devices.

Table 74. Descriptions of columns in the list of managed devices

Column name	Value
Name	NetBIOS name of the client device. The descriptions of the icons of device names are given in the appendix (see section "Statuses of devices, tasks, and policies" on page 910).
Operating system type	Type of operating system installed on the client device.
Windows domain	Name of the Windows domain in which the client device is located.
Network Agent is installed	Result of Network Agent installation on the client device (<i>Yes, No, Unknown</i>).
Network Agent is running	The result of Network Agent operation (<i>Yes, No, Unknown</i>).
Real-time protection	Security application is installed (<i>Yes, No, Unknown</i>).
Last connected to Administration Server	Time period that has elapsed since the client device was connected to the Administration Server.
Protection last updated	The time period that has elapsed since the last update of managed devices.
Status	Current status of the client device (<i>OK, Critical, or Warning</i>).

Column name	Value
Status description	<p>Reasons for change of the client device status to <i>Critical</i> or <i>Warning</i>. The device status changes to <i>Warning</i> or <i>Critical</i> for the following reasons:</p> <ul style="list-style-type: none"> • Security application is not installed. • Too many viruses detected. • Real-time protection level differs from the level set by the Administrator. • Virus scan has not been performed in a long time. • Databases are outdated. • Not connected in a long time. • Active threats are detected. • Restart is required. • Incompatible applications are installed. • Software vulnerabilities have been detected. • Check for Windows Update updates has not been performed in a long time. • Invalid encryption status. • Mobile device settings do not comply with the policy. • Unprocessed incidents detected. • Device status defined by application. • Device is out of disk space. • License expires soon. <p>The device status only changes to <i>Critical</i> by the following reasons:</p> <ul style="list-style-type: none"> • License expired. • Device has become unmanaged. • Protection is disabled. • Security application is not running. <p>Managed Kaspersky applications on client devices can add status descriptions to the list. Kaspersky Security Center can receive the description of a client device status from managed Kaspersky applications installed on that device. If the status that has been assigned to the device by a managed application is other than that assigned by Kaspersky Security Center, Administration Console displays the status that is the most critical to the device security. For example, if a managed application has assigned the <i>Critical</i> status to the device while Kaspersky Security Center has assigned it the <i>Warning</i> status, Administration Console displays the <i>Critical</i> status for that device with the corresponding description provided by the managed application.</p>
Information last updated	Time period that has elapsed since the client device was last synchronized successfully with the Administration Server (that is, since the last network scan).
DNS name	DNS domain name of the client device.
DNS domain	The main DNS suffix.
IP address	IP address of the client device. It is recommended to use the IPv4 address.




















Column name	Value
Last visible	Time period during which the client device has remained visible on the network.
Last full scan	Date and time of the last scan of the client device performed by the security application upon the user's request.
Total number of threats detected	Number of threats found.
Real-time protection status	Real-time protection status (<i>Starting, Running, Running (maximum protection), Running (maximum speed), Running (recommended settings), Running (custom settings), Stopped, Paused, Failed</i>).
Connection IP address	The IP address that is used for connection to Kaspersky Security Center Administration Server.
Network Agent version	Version of Network Agent.
Application version	Version of the security application installed on the client device.
Anti-virus databases last updated	The version of the anti-virus databases.
System last started	Date and time when the client device was last turned on.
Restart is required	Restart of the client device is required.
Distribution point	Name of the device that acts as distribution point for this client device.
Description	Description of the client device received after a network scan.
Encryption status	Data encryption status of the client device.
WUA status	Status of Windows Update Agent on the client device. Yes corresponds to client devices that receive updates through Windows Update from the Administration Server. No corresponds to client devices that receive updates through Windows Update from other sources.
Operating system bit size	Bit size of the operating system installed on the client device.
Spam protection status	Status of Spam protection component (<i>Running, Starting, Stopped, Paused, Failed, No data from device</i>)
Data Leakage Prevention status	Status of Data Leakage Prevention component (<i>Running, Starting, Stopped, Paused, Failed, No data from device</i>)














Column name	Value
Collaboration servers protection status	Status of Content Filtering component (<i>Running, Starting, Stopped, Paused, Failed, No data from device</i>)
Anti-virus protection status of mail servers	Status of Mail Server anti-virus protection component (<i>Running, Starting, Stopped, Paused, Failed, No data from device</i>)
Endpoint Sensor status	Status of Endpoint Sensor component (<i>Running, Starting, Stopped, Paused, Failed, No data from device</i>)
Created	Time when the <Device Name> icon was created. This attribute is used to compare various events with each other.
Name of virtual or secondary Administration Server	Name of virtual or secondary Administration Server. This column is only available in lists that contain devices from different Administration Servers.
Parent group	Name of the administration group (see section "Administration groups" on page 49) where the < Device Name> icon is located. This column is only available in lists that contain devices from different Administration Servers.
Managed by a different Administration Server	The parameter can take one of these values: <ul style="list-style-type: none"> • True, if during remote installation of security applications on the device, it turns out that the device is managed by different Administration Server. • False, otherwise.
Operating system build	The build number of the operating system. You can specify whether the selected operating system must have an equal, earlier, or later build number. You can also configure searching for all build numbers (see section "Configuring a device selection" on page 522), except the specified one.
Operating system release ID	The release identifier (ID) of the operating system. You can specify whether the selected operating system must have an equal, earlier, or later release ID. You can also configure searching for all release ID numbers (see section "Configuring a device selection" on page 522), except the specified one.

Statuses of devices, tasks, and policies

The table below contains a list of icons displayed in the console tree and in the Administration Console workspace, next to the names of devices, tasks, and policies. Those icons define the statuses of objects.

Table 75. Statuses of devices, tasks, and policies

Icon	Status
	Device with an operating system for workstations detected in the system but not yet included in any of the administration groups.
	Device with an operating system for workstations included in an administration group, with the <i>OK</i> status.
	Device with an operating system for workstations included in an administration group, with the <i>Warning</i> status.
	Device with an operating system for workstations included in an administration group, with the <i>Critical</i> status.
	Device with an operating system for workstations included in an administration group, which has lost connection with the Administration Server.
	Device with an operating system for servers detected in the system but not yet included in any of the administration groups.
	Device with an operating system for servers included in an administration group, with the <i>OK</i> status.
	Device with an operating system for servers included in an administration group, with the <i>Warning</i> status.
	Device with an operating system for servers included in an administration group, with the <i>Critical</i> status.
	Device with an operating system for servers included in an administration group, which has lost connection with the Administration Server.
	Mobile device detected on the network and included in none of the administration groups.
	Mobile device included in an administration group, with the <i>OK</i> status.
	Mobile device included in an administration group, with the <i>Warning</i> status.
	Mobile device included in an administration group, with the <i>Critical</i> status.
	Mobile device included in an administration group, having lost its connection with the Administration Server.
	UEFI protection device detected on the network but not included in any administration group. UEFI protection device is on the network.
	UEFI protection device detected on the network but not included in any administration group. UEFI protection device is not on the network.
	UEFI protection device included in an administration group, with <i>OK</i> status. UEFI protection device is on the network.
	UEFI protection device included in an administration group, with <i>OK</i> status. UEFI protection device is not in the network.










	UEFI protection device included in an administration group, with <i>Warning</i> status. UEFI protection device is in the network.
	UEFI protection device included in an administration group, with <i>Warning</i> status. UEFI protection device is not on the network.
	UEFI protection device included in an administration group, with <i>Critical</i> status. UEFI protection device is on the network. UEFI protection device is on the network.
	UEFI protection device included in an administration group, with <i>Critical</i> status. UEFI protection device is not on the network.
	Active policy.
	Inactive policy.
	Active policy inherited from a group that was created on the primary Administration Server.
	Active policy inherited from a top-level group.
	Task (group task, Administration Server task, or task for specific devices) with the <i>Scheduled</i> or <i>Completed successfully</i> status.
	Task (group task, Administration Server task, or task for specific devices) with the <i>Running</i> status.
	Task (group task, Administration Server task, or task for specific devices) with the <i>Failed</i> status.
	Task inherited from a group that was created on the primary Administration Server.
	Task inherited from a top-level group.

File status icons in Administration Console

For ease of file management in Kaspersky Security Center Administration Console, icons are displayed next to the names of files (see table below). Icons indicate statuses assigned to files by managed Kaspersky applications on client devices. Icons are shown in the workspaces of the **Quarantine**, **Backup**, and **Active threats** folders.

Statuses are assigned to objects by Kaspersky Endpoint Security installed on the client device on which the object is located.

Table 76. Correspondence between icons and file statuses

Icon	Status
	File with the <i>Infected</i> status.
	File with the <i>Warning</i> or <i>Probably infected</i> status.
	File with the <i>Added by user</i> status.
	File with the <i>False positive</i> status.
	File with the <i>Disinfected</i> status.
	File with the <i>Deleted</i> status.
	File in the Quarantine folder with the <i>Not infected</i> , <i>Password-protected</i> or <i>Must be sent to Kaspersky</i> status. If there is no status description next to an icon, this means that the managed Kaspersky application on the client device has reported an unknown status to Kaspersky Security Center.
	File in the Backup folder with the <i>Not infected</i> , <i>Password-protected</i> or <i>Must be sent to Kaspersky</i> status. If there is no status description next to an icon, this means that the managed Kaspersky application on the client device has reported an unknown status to Kaspersky Security Center.
	File in the Active threats folder with <i>Not infected</i> , <i>Password-protected</i> or <i>Must be sent to Kaspersky</i> status. If there is no status description next to an icon, this means that the managed Kaspersky application on the client device has reported an unknown status to Kaspersky Security Center.

Searching and exporting data

This section contains information about data search methods and about exporting data.

In this section

Finding devices	914
Device search settings	916
Using masks in string variables	927
Using regular expressions in the search field	927
Exporting lists from dialog boxes	928

Finding devices

Kaspersky Security Center allows you to find devices on the basis of specified criteria. Search results can be saved to a text file.

The search feature allows you to find the following devices:

- Client devices in administration groups of an Administration Server and its secondary Servers.
- Unassigned devices managed by an Administration Server and its secondary Servers.

► *To find client devices included in an administration group:*

1. In the console tree, select an administration group folder.
2. Select **Search** from the context menu of the administration group folder.
3. On the tabs of the **Search** window, specify the criteria for the search of devices, and click the **Find now** button.

Devices that meet the specified search criteria are now displayed in a table in the lower part of the **Search** window.

► *To find unassigned devices:*

1. In the console tree, select the **Unassigned devices** folder.
2. Select **Search** from the context menu of the **Unassigned devices** folder.
3. On the tabs of the **Search** window, specify the criteria for the search of devices, and click the **Find now** button.

Devices that meet the specified search criteria are now displayed in a table in the lower part of the **Search** window.

► *To find devices regardless of whether they are included in an administration group:*

1. In the console tree, select the **Administration Server** node.
2. In the context menu of the node, select **Search**.
3. On the tabs of the **Search** window, specify the criteria for the search of devices, and click the **Find now** button.

Devices that meet the specified search criteria are now displayed in a table in the lower part of the **Search** window.

In the **Search** window you can also search for administration groups and secondary Administration Servers using a drop-down list in the top right corner of the window. Search functionality for administration groups and secondary Administration Servers is not available if you opened the **Search** window from the **Unassigned devices** folder.

To find devices, you can use regular expressions (see section "Using regular expressions in the search field" on page [927](#)) in the fields of the **Search** window.

Full text search in the **Search** window is available:

- On the **Network** tab, in the **Description** field
- On the **Hardware** tab, in the **Device**, **Vendor**, and **Description** fields

See also:

Device search settings.....	916
-----------------------------	-----

Device search settings

Below are descriptions of the settings used for searching managed devices (see section "Finding devices" on page [914](#)). Search results are displayed in the lower part of the window.

Network

On the **Network** tab, you can specify the criteria that will be used to search for devices according to their network data:

- **Device name or IP address**
Name of the device in the Windows network (NetBIOS name).
- **Windows domain**
Displays all devices included in the specified Windows domain.
- **Administration group**
Displays devices included in the specified administration group.
- **Description**
Text in the device properties window: In the **Description** field of the **General** section.
To describe text in the **Description** field, you can use the following characters:
 - Within a word:
 - *. Replaces any string with any number of characters.
Example:
To describe words such as **Server** or **Server's**, you can enter **Server***.
 - ?. Replaces any single character.
Example:
To describe words such as **Window** or **Windows**, you can enter **Windo?**.
Asterisk (*) or question mark (?) cannot be used as the first character in the query.
 - To find several words:
 - Space. You will see all devices whose descriptions contain any of the listed words.
Example:
To find a phrase that contains **Secondary** or **Virtual** words, you can include **Secondary Virtual** line in your query.
 - +. When a plus sign precedes a word, all search results will contain this word.
Example:
To find a phrase that contains both **Secondary** and **Virtual**, enter the

+Secondary+Virtual query.

- -. When a minus sign precedes a word, no search results will contain this word.

Example:

To find a phrase that contains **Secondary** and does not contain **Virtual**, enter the **+Secondary-Virtual** query.

- "<some text>". Text enclosed in quotation marks must be present in the text.

Example:

To find a phrase that contains **Secondary Server** word combination, you can enter "**Secondary Server**" in the query.

- **IP range**

If this check box is selected, you can enter the initial and final IP addresses of the IP range in which the relevant devices must be included.

By default, this check box is cleared.

- **Managed by a different Administration Server**

Select one of the following values:

- **Yes.** Only the client devices managed by other Administration Servers are considered.
- **No.** Only the client devices managed by the same Administration Server are considered.
- **No value is selected.** The criterion will not be applied.

Tags

On the **Tags** tab, you can configure a device search based on key words (tags) that were previously added to the descriptions of managed devices:

- **Apply if at least one specified tag matches**

If this check box is selected, the search results will show devices with descriptions that contain at least one of the selected tags.

If this check box is cleared, the search results will only show devices with descriptions that contain all the selected tags.

By default, this check box is cleared.

- **Tag must be included**

If this option is selected, the search results will display the devices whose descriptions contain the selected tag. To find devices, you can use the asterisk, which stands for any string with any number of characters.

By default, this option is selected.

- **Tag must be excluded**

If this option is selected, the search results will display the devices whose descriptions do not contain the selected tag. To find devices, you can use the asterisk, which stands for any string with any number of characters.

Active Directory

On the **Active Directory** tab, you can specify the criteria that will be used to search for devices according to their Active Directory data:

- **Device is in an Active Directory organizational unit**

If this check box is selected, the selection includes devices from the Active Directory unit specified in the entry field.

By default, this check box is cleared.

- **Include child organizational units**

If this check box is selected, the selection includes devices from all child OUs of the specified Active Directory OU.

By default, this check box is cleared.

- **This device is a member of an Active Directory group**

If this check box is selected, the selection includes devices from the Active Directory group specified in the entry field.

By default, this check box is cleared.

Network activity

On the **Network activity** tab, you can specify the criteria that will be used to search for devices according to their network activity:

- **This device is a distribution point**

In the drop-down list, you can set up the criterion for including devices in the selection when performing search:

- **Yes.** The selection includes devices that act as distribution points.
- **No.** Devices that act as distribution points are not included in the selection.
- **No value is selected.** The criterion will not be applied.

- **Do not disconnect from the Administration Server**

In the drop-down list, you can set up the criterion for including devices in the selection when performing search:

- **Enabled.** The selection will include devices on which the **Do not disconnect from the Administration Server** check box is selected.
- **Disabled.** The selection will include devices on which the **Do not disconnect from the Administration Server** check box is cleared.
- **No value is selected.** The criterion will not be applied.

- **Connection profile switched**

In the drop-down list, you can set up the criterion for including devices in the selection when performing search:

- **Yes.** The selection will include devices that connected to the Administration Server after the connection profile was switched.
- **No.** The selection will not include devices that connected to the Administration Server after the connection profile was switched.
- **No value is selected.** The criterion will not be applied.

- **Last connected to Administration Server**

You can use this check box to set a search criterion for devices according to the time they last connected to the Administration Server.

If this check box is selected, in the entry fields you can specify the time interval (date and time) during which the last connection was established between Network Agent installed on the client device and the Administration Server. The selection will include devices that fall within the specified interval.

If this check box is cleared, the criterion will not be applied.

By default, this check box is cleared.

- **New devices detected by network poll**

Searches for new devices that have been detected by network polling over the last few days.

If this check box is selected, the selection only includes new devices that have been detected by device discovery over the number of days specified in the **Detection period (days)** field.

If this check box is cleared, the selection includes all devices that have been detected by device discovery.

By default, this check box is cleared.

- **Device is visible**

In the drop-down list, you can set up the criterion for including devices in the selection when performing search:

- **Yes.** The application includes in the selection devices that are currently visible in the network.
- **No.** The application includes in the selection devices that are currently invisible in the network.
- **No value is selected.** The criterion will not be applied.

Application

On the **Application** tab, you can specify the criteria that will be used to search for devices according to the selected managed application:

- **Application name**

In the drop-down list, you can set a criterion for including devices in a selection when search is performed by the name of a Kaspersky application.

The list provides only the names of applications with management plug-ins installed on the administrator's workstation.

If no application is selected, the criterion will not be applied.

- **Application version**

In the entry field, you can set a criterion for including devices in a selection when search is performed by the version number of a Kaspersky application.

If no version number is specified, the criterion will not be applied.

- **Critical update name**

In the entry field, you can set a criterion for including devices in a selection when search is performed by application name or by update package number.

If the field is left blank, the criterion will not be applied.

- **Modules last updated**

You can use this setting to set a criterion for searching devices by time of the last update of modules of applications installed on those devices.

If this check box is selected, in the entry fields you can specify the time interval (date and time) during which the last update of modules of applications installed on those devices was performed.

If this check box is cleared, the criterion will not be applied.

By default, this check box is cleared.

- **Device is managed through Kaspersky Security Center 13**

In the drop-down list, you can include in the selection the devices managed through Kaspersky Security Center:

- **Yes.** The application includes in the selection devices managed through Kaspersky Security Center.
- **No.** The application includes devices in the selection if they are not managed through Kaspersky Security Center.
- **No value is selected.** The criterion will not be applied.

- **Security application is installed**

In the drop-down list, you can include in the selection all devices with the security application installed:

- **Yes.** The application includes in the selection all devices with the security application installed.
- **No.** The application includes in the selection all devices with no security application installed.
- **No value is selected.** The criterion will not be applied.

Operating system

On the **Operating system** tab, you can set up the following criteria to find devices by their operating system (OS) type:

- **Operating system version**

If the check box is selected, you can select an operating system from the list. Devices with the specified operating systems installed are included in the search results.

- **Operating system bit size**

In the drop-down list, you can select the architecture for the operating system, which will determine how the moving rule is applied to the device (**Unknown**, **x86**, **AMD64**, or **IA64**). By default, no option is selected in the list so that the operating system's architecture is not defined.

- **Operating system service pack version**

In this field, you can specify the package version of the operating system (in *X.Y* format), which will determine how the moving rule is applied to the device. By default, no version value is specified.

- **Operating system build**

This setting is applicable to Windows operating systems only.

The build number of the operating system. You can specify whether the selected operating system must have an equal, earlier, or later build number. You can also configure searching for all build numbers except the specified one.

- **Operating system release ID**

This setting is applicable to Windows operating systems only.

The release identifier (ID) of the operating system. You can specify whether the selected operating system must have an equal, earlier, or later release ID. You can also configure searching for all release ID numbers except the specified one.

Device status

On the **Device status** tab, you can specify criteria for searching devices based on the device status from the managed application:

- **Device status**

Drop-down list in which you can select one of the device statuses: *OK*, *Critical*, or *Warning*.
- **Real-time protection status**

Drop-down list, in which you can select the real-time protection status. Devices with the specified real-time protection status are included in the selection.
- **Device status description**

In this field, you can select the check boxes next to conditions that, if met, assign one of the following statuses to the device: *OK*, *Critical*, or *Warning*.
- **Device status defined by application**

Drop-down list, in which you can select the real-time protection status. Devices with the specified real-time protection status are included in the selection.

Protection components

On the **Protection components** tab, you can set up the criteria to search for client devices by their protection status.

- **Databases released**

If this check box is selected, you can search for client devices by anti-virus database release date. In the entry fields you can set the time interval, on the basis of which the search is performed.

By default, this check box is cleared.
- **Last scanned**

If this check box is selected, you can search for client devices by time of the last virus scan. In the entry fields you can specify the time period within which the last virus scan was performed.

By default, this check box is cleared.

- **Total number of threats detected**

If this check box is selected, you can search for client devices by number of viruses detected. In the entry fields you can set the lower and upper threshold values for the number of viruses found.

By default, this check box is cleared.

Applications registry

On the **Applications registry** tab, you can configure the search for devices according to applications installed on them:

- **Application name**

Drop-down list in which you can select an application. Devices on which the specified application is installed, are included in the selection.

- **Application version**

Entry field in which you can specify the version of selected application.

- **Vendor**

Drop-down list in which you can select the manufacturer of an application installed on the device.

- **Application status**

A drop-down list in which you can select the status of an application (*Installed, Not installed*). Devices on which the specified application is installed or not installed, depending on the selected status, will be included in the selection.

- **Find by update**

If this check box is selected, search will be performed using the details of updates for applications installed on the relevant devices. After you select the check box, the **Application name**, **Application version**, and **Application status** fields change to **Update name**, **Update version**, and **Status** respectively.

By default, this check box is cleared.

- **Incompatible security application name**

Drop-down list in which you can select third-party security applications. During the search, devices on which the specified application is installed, are included in the selection.

- **Application tag**

In the drop-down list, you can select the application tag. All devices that have installed applications with the selected tag in the description are included in the device selection.

Hierarchy of Administration Servers

On the **Hierarchy of Administration Servers** tab, check the **Include data from secondary Administration Servers (down to level)** box if you want the information stored on secondary Administration Servers to be considered while searching for devices, and in the entry field, you can specify the nesting level of secondary Administration Server from which information is considered while searching for devices. By default, this check box is cleared.

Virtual machines

On the **Virtual machines** tab, you can configure the search for devices according to whether these are virtual machines or part of virtual desktop infrastructure (VDI):

- **This is a virtual machine**

In the drop-down list you can select the following options:

- **Not important.**

- **No.** Find devices that are not virtual machines.
- **Yes.** Find devices that are virtual machines.

- **Virtual machine type**

In the drop-down list, you can select the virtual machine manufacturer.

This drop-down list is available if the **Yes** or **Not important** value is selected in the **This is a virtual machine** drop-down list.

- **Part of Virtual Desktop Infrastructure**

In the drop-down list you can select the following options:

- **Not important.**

- **No.** Find devices that are not part of Virtual Desktop Infrastructure.
- **Yes.** Find devices that are part of the Virtual Desktop Infrastructure (VDI).

Hardware

On the **Hardware** tab, you can configure search for client devices according to their hardware:

- **Device**

In the drop-down list, you can select a unit type. All devices with this unit are included in the search results.

The field supports the full-text search.

- **Vendor**

In the drop-down list, you can select the name of a unit manufacturer. All devices with this unit are included in the search results.

The field supports the full-text search.

- **Description**

Description of the device or hardware unit. Devices with the description specified in this field are included in the selection.

A device's description in any format can be entered in the properties window of that device. The field supports the full-text search.

- **Inventory number**

Equipment with the inventory number specified in this field will be included in the selection.

- **CPU frequency, in MHz**

The frequency range of a CPU. Devices with CPUs that match the frequency range in these fields (inclusive) will be included in the selection.

- **Virtual CPU cores**

Range of the number of virtual cores in a CPU. Devices with CPUs that match the range in these fields (inclusive) will be included in the selection.

- **Hard drive volume, in GB**

Range of values for the size of the hard drive on the device. Devices with hard drives that match the range in these entry fields (inclusive) will be included in the selection.

- **RAM size, in MB**

Range of values for the size of the device RAM. Devices with RAMs that match the range in these entry fields (inclusive) will be included in the selection.

Vulnerabilities and updates

On the **Vulnerabilities and updates** tab, you can set up the criterion to search for devices according to their Windows Update source:

- **WUA is switched to Administration Server**

You can select one of the following search options from the drop-down list:

- **Yes.** If this option is selected, the search results will include devices that receive updates through Windows Update from the Administration Server.
- **No.** If this option is selected, the results will include devices that receive updates through Windows Update from another sources.

Users

On the **Users** tab, you can set up the criteria to search for devices according to the accounts of users who have logged in to the operating system.

- **Last user who logged in to the system**

If this check box is selected, click the **Browse** button to specify a user account. The search results include devices on which the specified user performed the last login to the system.

- **User who logged in to the system at least once**

If this check box is selected, click the **Browse** button to specify a user account. The search results include devices on which the specified user logged in to the system at least once.

Status-affecting problems in managed applications

On the **Status-affecting problems in managed applications** tab, you can set up search for devices according to descriptions of their statuses provided by the managed application:

- **Device status description**

You can select check boxes for descriptions of statuses from the managed application; upon receipt of these statuses, the devices will be included in the selection. When you select a status listed for several applications, you have the option to select this status in all of the lists automatically.

Statuses of components in managed applications

On the **Statuses of components in managed applications** tab, you can set up the criteria to search for devices according to the statuses of components in managed applications:

- **Data Leakage Prevention status**

Search for devices by the status of Data Leakage Prevention (*No data from device, Stopped, Starting, Paused, Running, Failed*).

- **Collaboration servers protection status**

Search for devices by the status of server collaboration protection (*No data from device, Stopped, Starting, Paused, Running, Failed*).

- **Anti-virus protection status of mail servers**

Search for devices by the status of Mail Server protection (*No data from device, Stopped, Starting, Paused, Running, Failed*).

- **Endpoint Sensor status**

Search for devices by the status of the Endpoint Sensor component (*No data from device, Stopped, Starting, Paused, Running, Failed*).

Encryption

- **Encryption**

Advanced Encryption Standard (AES) symmetrical block cipher algorithm. In the drop-down list, you can select the encryption key size (56-bit, 128-bit, 192-bit, or 256-bit).

Available values: *AES56, AES128, AES192, and AES256*.

Cloud segments

On the **Cloud segments** tab, you can configure a search based on whether a device belongs to specific cloud segments:

- **Device is in a cloud segment**

If this check box is selected, you can click the **Browse** button to specify the segment to search.

If the **Include child objects** check box is also selected, the search is run on all child objects of the specified segment.

Search results include only devices from the selected segment.

- **Device discovered by using the API**

In the drop-down list, you can select whether a device is detected by API tools.

- **AWS.** The device is discovered by using AWS API, that is, the device definitely is in the AWS cloud environment.
- **Azure.** The device is discovered by using Azure API, that is, the device definitely is in the Azure cloud environment.
- **Google Cloud.** The device is discovered by using Google API, that is, the device definitely is in the Google cloud environment.

- **No.** The device cannot be detected by using AWS, Azure or Google API, that is, it is either outside the cloud environment, or it is in the cloud environment but it cannot be detected by using an API for some reason.
- No value. This criterion cannot be applied.

Application components

This section contains the list of components of those applications that have corresponding management plugins installed in Administration Console.

In the **Application components** section, you can specify criteria for including devices in a selection according to the statuses and version numbers of the components that refer to the application that you select:

- **Status**

Search for devices according to the component status sent by an application to the Administration Server. You can select one of the following statuses: *No data from device*, *Stopped*, *Starting*, *Paused*, *Running*, *Malfunction*, or *Not installed*. If the selected component of the application installed on a managed device has the specified status, the device is included in the device selection.

Statuses sent by applications:

- *Starting*—The component is currently in the process of initialization.
- *Running*—The component is enabled and working properly.
- *Paused*—The component is suspended, for example, after the user has paused protection in the managed application.
- *Malfunction*—An error has occurred during the component operation.
- *Stopped*—The component is disabled and not working at the moment.
- *Not installed*—The user did not select the component for installation when configuring custom installation of the application.

Unlike other statuses, the *No data from device* status is not sent by applications. This option shows that the applications have no information about the selected component status. For example, this can happen when the selected component does not belong to any of the applications installed on the device, or when the device is turned off.

- **Version**

Search for devices according to the version number of the component that you select in the list. You can type a version number, for example *3.4.1.0*, and then specify whether the selected component must have an equal, earlier, or later version. You can also configure searching for all versions except the specified one.

See also:

Using regular expressions in the search field.....	927
Finding devices.....	914

Using masks in string variables

Using masks for string variables is allowed. When creating masks, you can use the following regular expressions:

- Wildcard character (*)—Any string of 0 or more characters.
- Question mark (?)—Any single character.
- [`<range>`]—Any single character from a specified range or set.
For example: `[0-9]`—Any digit. `[abcdef]`—Any of the characters a, b, c, d, e, or f.

Using regular expressions in the search field

You can use the following regular expressions in the search field to search for specific words and characters:

- *. Replaces any sequence of characters. To search for such words as `Server`, `Servers`, or `Server room`, enter the `Server*` expression in the search field.
- ?. Replaces any single character. To search for such words as `Word` or `Ward`, enter the `W?rd` expression in the search field.

Text in the search field cannot begin with a question mark (?).

- [`<range>`]. Replaces any single character from a specified range or set. To search for any numeral, enter the `[0-9]` expression in the search field. To search for one of the characters—`a`, `b`, `c`, `d`, `e`, or `f`—enter the `[abcdef]` expression in the search field.

Use the following regular expressions in the search field to run a full-text search:

- Space. You will see all devices whose descriptions contain any of the listed words. For example, to search for a phrase that contains the word "Secondary" or "Virtual" (or both these words), enter the `Secondary Virtual` expression in the search field.
- Plus sign (+), AND, or &&. When a plus sign precedes a word, all search results will contain this word. For example, to search for a phrase that contains both the word "Secondary" and the word "Virtual", you can enter any of the following expressions in the search field: `+Secondary+Virtual`, `Secondary AND Virtual`, `Secondary && Virtual`.
- OR or ||. When placed between two words, it indicates that one word or the other can be found in the text. To search for a phrase that contains either the word "Secondary" or the word "Virtual", you can enter any of the following expressions in the search field: `Secondary OR Virtual`, `Secondary || Virtual`.
- Minus sign (-). When a minus sign precedes a word, no search results will contain this word. To search for a phrase that must contain such word as `Secondary` and must not contain such word as `Virtual`, you must enter the `+Secondary-Virtual` expression in the search field.
- "`<some text>`". Text enclosed in quotation marks must be present in the text. To search for a phrase that contains such word combination as `Secondary Server`, you must enter the `"Secondary Server"` expression in the search field.

Full-text search is available in the following filtering blocks:

- In the event list filtering block, by the **Event** and **Description** columns.
- In the user account filtering block, by the **Name** column.

- In the applications registry filtering block, by the **Name** column, if the **Show in list** section has **no grouping** selected as the filtering criterion.

Exporting lists from dialog boxes

In dialog boxes of the application you can export lists of objects to text files.

Export of a list of objects is possible for dialog box sections that contain the **Export to file** button.

Settings of tasks

This section lists all settings of tasks in Kaspersky Security Center.

In this section

General task settings	928
Download updates to the repository of the Administration Server task settings	934
Download updates to the repositories of distribution points task settings	936
Find vulnerabilities and required updates task settings.....	937
Install required updates and fix vulnerabilities task settings.....	939

General task settings

Settings specified during task creation

You can specify the following settings when creating a task. Some of these settings can also be modified in the properties of the created task.

- Operating system restart settings:
 - **Do not restart the device**

Client devices are not restarted automatically after the operation. To complete the operation, you must restart a device (for example, manually or through a device management task). Information about the required restart is saved in the task results and in the device status. This option is suitable for tasks on servers and other devices where continuous operation is critical.
 - **Restart the device**

Client devices are always restarted automatically if a restart is required for completion of the operation. This option is useful for tasks on devices that provide for regular pauses in their operation (shutdown or restart).
 - **Prompt user for action**

The restart reminder is displayed on the screen of the client device, prompting the user to restart it manually. Some advanced settings can be defined for this option: text of the message for the user, the message display frequency, and the time interval after which a restart will be forced (without the user's confirmation). This option is most suitable for

workstations where users must be able to select the most convenient time for a restart.

By default, this option is selected.

- **Repeat prompt every (min)**

If this option is enabled, the application prompts the user to restart the operating system with the specified frequency.

By default, this option is enabled. The default interval is 5 minutes. Available values are between 1 and 1 440 minutes.

If this option is disabled, the prompt is displayed only once.

- **Restart after (min)**

After prompting the user, the application forces restart of the operating system upon expiration of the specified time interval.

By default, this option is enabled. The default delay is 30 minutes. Available values are between 1 and 1 440 minutes.

- **Force closure of applications in blocked sessions**

Running applications may prevent a restart of the client device. For example, if a document is being edited in a word processing application and is not saved, the application does not allow the device to restart.

If this option is enabled, such applications on a locked device are forced to close before the device restart. As a result, users may lose their unsaved changes.

If this option is disabled, a locked device is not restarted. The task status on this device states that a device restart is required. Users have to manually close all applications running on locked devices and restart these devices.

By default, this option is disabled.

- Task scheduling settings:
 - **Scheduled start:**

Select the schedule according to which the task runs, and configure the selected schedule.

- **Every N hours**

The task runs regularly, with the specified interval in hours, starting from the specified date and time.

By default, the task runs every six hours, starting from the current system date and time.

- **Every N days**

The task runs regularly, with the specified interval in days. Additionally, you can specify a date and time of the first task run. These additional options become available, if they are supported by the application for which you create the task.

By default, the task runs every day, starting from the current system date and time.

- **Every N weeks**

The task runs regularly, with the specified interval in weeks, on the specified day of week and at the specified time.

By default, the task runs every Monday at the current system time.

- **Every N minutes**

The task runs regularly, with the specified interval in minutes, starting from the specified time on the day that the task is created.

By default, the task runs every 30 minutes, starting from the current system time.

- **Daily (daylight saving time is not supported)**

The task runs regularly, with the specified interval in days. This schedule does not support observance of daylight saving time (DST). It means that when clocks jump one hour forward or backward at the beginning or ending of DST, the actual task start time does not change.

We do not recommend that you use this schedule. It is needed for backward compatibility of Kaspersky Security Center.

By default, the task starts every day at the current system time.

- **Weekly**

The task runs every week on the specified day and at the specified time.

- **By days of week**

The task runs regularly, on the specified days of week, at the specified time.

By default, the task runs every Friday at 6:00:00 P.M.

- **Monthly**

The task runs regularly, on the specified day of the month, at the specified time.

In months that lack the specified day, the task runs on the last day.

By default, the task runs on the first day of each month, at the current system time.

- **Manually**

The task does not run automatically. You can only start it manually.

- **Every month on specified days of selected weeks**

The task runs regularly, on the specified days of each month, at the specified time.

By default, no days of month are selected; the default start time is 6:00:00 P.M.

- **When new updates are downloaded to the repository**

The task runs after updates are downloaded to the repository. For example, you may want to use this schedule for the find vulnerabilities and required updates task.

- **On virus outbreak**

The task runs after a *Virus outbreak* event occurs. Select application types that will monitor virus outbreaks. The following application types are available:

- Anti-virus for workstations and file servers
- Anti-virus for perimeter defense
- Anti-virus for mail systems

By default, all application types are selected.

You may want to run different tasks depending on the anti-virus application type that reports a virus outbreak. In this case, remove the selection of the application types that you do not need.

- **On completing another task**

The current task starts after another task completes. You can select how the previous task must complete (successfully or with error) to trigger the start of the current task. For example, you may want to run the Manage devices task with the **Turn on the device** option and, after it completes, run the Virus scan task.

- **Run missed tasks**

This option determines the behavior of a task if a client device is not visible on the network when the task is about to start.

If this option is enabled, the system attempts to start the task the next time the Kaspersky application is run on the client device. If the task schedule is **Manually, Once** or **Immediately**, the task is started immediately after the device becomes visible on the network or immediately after the device is included in the task scope.

If this option is disabled, only scheduled tasks run on client devices; for **Manually, Once** and **Immediately**, tasks run only on those client devices that are visible on the network. For example, you may want to disable this option for a resource-consuming task that you want to run only outside of business hours.

By default, this option is enabled.

- **Use automatically randomized delay for task starts**

If this option is enabled, the task is started on client devices randomly within a specified time interval, that is, *distributed task start*. A distributed task start helps to avoid a large number of simultaneous requests by client devices to the Administration Server when a scheduled task is running.

The distributed start time is calculated automatically when a task is created, depending on the number of client devices to which the task is assigned. Later, the task is always started on the calculated start time. However when task settings are edited or the task is started manually, the calculated value of the task start time changes.

If this option is disabled, the task starts on client devices according to the schedule.

- **Use randomized delay for task starts within an interval of (min)**

If this option is enabled, the task is started on client devices randomly within the specified time interval. A distributed task start helps to avoid a large number of simultaneous requests by client devices to the Administration Server when a scheduled task is running.

If this option is disabled, the task starts on client devices according to the schedule.

By default, this option is disabled. The default time interval is one minute.

- Devices to which the task will be assigned:

- **Select networked devices detected by Administration Server**

The task is assigned to specific devices. The specific devices can include devices in administration groups as well as unassigned devices.

For example, you may want to use this option in a task of installing Network Agent on unassigned devices.

- **Specify device addresses manually or import addresses from a list**

You can specify NetBIOS names, DNS names, IP addresses, and IP subnets of devices to which you want to assign the task.

You may want to use this option to execute a task for a specific subnet. For example, you may want to install a certain application on devices of accountants or to scan devices in a

subnet that is probably infected.

- **Assign task to a device selection**

The task is assigned to devices included in a device selection. You can specify one of the existing selections.

For example, you may want to use this option to run a task on devices with a specific operating system version.

- **Assign task to an administration group**

The task is assigned to devices included in an administration group. You can specify one of the existing groups or create a new one.

For example, you may want to use this option to run a task of sending a message to users if the message is specific for devices included in a specific administration group.

- Account settings

- **Default account**

The task will be run under the same account as the application that performs this task.

By default, this option is selected.

- **Specify account**

Fill in the **Account** and **Password** fields to specify the details of an account under which the task is run. The account must have sufficient rights for this task.

- **Account**

Account under which the task is run.

- **Password**

Password of the account under which the task will be run.

Settings specified after task creation

You can specify the following settings only after a task is created.

- Advanced scheduling settings:

- **Activate the device before the task is started through Wake-on-LAN (min)**

The operating system on the device starts at the specified time before the task is started. The default time period is five minutes.

Enable this option if you want the task to run on all of the client devices from the task scope, including those devices that are turned off when the task is about to start.

If you want the device to be automatically turned off after the task is complete, enable the **Shut down device when task is complete** option. This option can be found in the same window.

By default, this option is disabled.

- **Shut down device when task is complete**

For example, you may want to enable this option for an install update task that installs updates to client devices each Friday after business hours, and then turns off these devices for the weekend.

By default, this option is disabled.

- **Stop if the task is taking longer than (min)**

After the specified time period expires, the task is stopped automatically, whether it is completed or not.

Enable this option if you want to interrupt (or stop) tasks that take too long to execute.

By default, this option is disabled. The default task execution time is 120 minutes.

- Notification settings:
 - **Store task history** block
 - **On Administration Server for (days)**

Application events related to execution of the task on all client devices from the task scope are stored on the Administration Server during the specified number of days. When this period elapses, the information is deleted from the Administration Server.

By default, this option is enabled.

- **Store in the OS event log on device**

Application events related to execution of the task are stored locally in Windows Event Log of each client device.

By default, this option is disabled.

- **Store in the OS event log on Administration Server**

Application events related to execution of the task on all client devices from the task scope are stored centrally in Windows Event Log of the Administration Server operating system (OS).

By default, this option is disabled.

- **Save all events**

If this option is selected, all events related to the task are saved to the event logs.

- **Save events related to task progress**

If this option is selected, only events related to the task execution are saved to the event logs.

- **Save only task execution results**

If this option is selected, only events related to the task results are saved to the event logs.

- **Notify administrator of task execution results**

You can select the methods by which administrators receive notifications about task execution results: by email, by SMS, and by running an executable file. To configure notification, click the **Settings** link.

By default, all notification methods are disabled.

- **Notify of errors only**

If this option is enabled, administrators are only notified when a task execution completes with an error.

If this option is disabled, administrators are notified after every task execution completion.

By default, this option is enabled.

- Security settings
- Task scope settings

Depending on how the task scope is determined, the following settings are present:

- **Devices**

If the scope of a task is determined by an administration group, you can view this group. No changes are available here. However, you can set **Exclusions from task scope**.

If the scope of a task is determined by a list of devices, you can modify this list by adding and removing devices.

- **Device selection**

You can change the device selection to which the task is applied.

- **Exclusions from task scope**

You can specify groups of devices to which the task is not applied. Groups to be excluded can only be subgroups of the administration group to which the task is applied.

- **Revision history**

Download updates to the repository of the Administration Server task settings

Settings specified during task creation

You can specify the following settings when creating a task. Some of these settings can also be modified in the properties of the created task.

- **Sources of updates**

The following resources can be used as a source of updates for the Administration Server:

- Kaspersky update servers.

HTTP(S) servers at Kaspersky from which Kaspersky applications download database and application module updates. By default, the Administration Server communicates with Kaspersky update servers and downloads updates by using the HTTPS protocol. You can configure the Administration Server to use the HTTP protocol instead of HTTPS.

Selected by default.

- Primary Administration Server. (This option might not work in Kaspersky Security Center 13 Web Console.)

This resource applies to tasks created for a secondary or virtual Administration Server.

- Local or network folder.

A local or network folder that contains the latest updates. A network folder can be an FTP or HTTP server, or an SMB share. When selecting a local folder, you must specify a folder on the device that has Administration Server installed.

An FTP or HTTP server or a network folder used by an update source must contain a folders structure (with updates) that matches the structure created when using Kaspersky update servers.

- **Other settings**

- **Force update of secondary Administration Servers**

If this option is enabled, the Administration Server starts the update tasks on the secondary Administration Servers as soon as new updates are downloaded. Otherwise, the update tasks on the secondary Administration Servers start according to their schedules.

By default, this option is disabled.

- **Copy downloaded updates to additional folders**

After the Administration Server receives updates, it copies them to the specified folders. Use this option if you want to manually manage the distribution of updates on your network.

For example, you may want to use this option in the following situation: the network of your organization consists of several independent subnets, and devices from each of the subnets do not have access to other subnets. However devices in all of the subnets have access to a common network share. In this case, you set Administration Server in one of the subnets to download updates from Kaspersky update servers, enable this option, and then specify this network share. In downloaded updates to the repository tasks for other Administration Servers, specify the same network share as the update source.

By default, this option is disabled.

- **Do not force updating of devices and secondary Administration Servers unless copying is complete**

The tasks of downloading updates to client devices and secondary Administration Servers start only after those updates are copied from the main update folder to additional update folders.

This option must be enabled if client devices and secondary Administration Servers download updates from additional network folders.

By default, this option is disabled.

- **Update Network Agent modules (for Network Agent versions earlier than 10 Service Pack 2)**

If this option is enabled, updates for software modules of Network Agent are installed automatically after the Administration Server completes the download updates to the repository task. Otherwise, updates received for Network Agent modules can be installed manually.

By default, this option is enabled.

Settings specified after task creation

You can specify the following settings only after a task is created.

- **Settings** section, **Content of updates** block
 - **Download diff files**

This option enables the downloading diff files feature (see section "Using diff files for updating Kaspersky databases and software modules" on page [412](#)).

By default, this option is disabled.

- **Update verification** section
 - **Verify updates before distributing**

Administration Server downloads updates from the source, saves them to a temporary repository, and runs the task defined in the **Update verification task** field. If the task completes successfully, the updates are copied from the temporary repository to a shared folder on the Administration Server and then distributed to all devices for which the Administration Server acts as the source of updates (tasks with the **When new updates are downloaded to the repository** schedule type are started). The task of downloading updates to the repository is finished only after completion of the update verification task.

By default, this option is disabled.

- **Update verification task**

This task verifies downloaded updates before they are distributed to all devices for which the Administration Server acts as the source of updates.

See also:

General task settings	928
Creating the task for downloading updates to the repository of the Administration Server	413
Verifying downloaded updates	422

Download updates to the repositories of distribution points task settings

Settings specified during task creation

You can specify the following settings when creating a task. Some of these settings can also be modified in the properties of the created task.

- **Sources of updates**

The following resources can be used as a source of updates for the Administration Server:

- Kaspersky update servers.
HTTP(S) servers at Kaspersky from which Kaspersky applications download database and application module updates. By default, the Administration Server communicates with Kaspersky update servers and downloads updates by using the HTTPS protocol. You can configure the Administration Server to use the HTTP protocol instead of HTTPS.
Selected by default.
- Primary Administration Server. (This option might not work in Kaspersky Security Center 13 Web Console.)
This resource applies to tasks created for a secondary or virtual Administration Server.
- Local or network folder.
A local or network folder that contains the latest updates. A network folder can be an FTP or HTTP server, or an SMB share. When selecting a local folder, you must specify a folder on the device that has Administration Server installed.

An FTP or HTTP server or a network folder used by an update source must contain a folders structure (with updates) that matches the structure created when using Kaspersky update servers.

- **Other settings**
 - **Folder for storing updates**

The folder is used to download updates. Specify a local folder on the devices that are assigned to act as distribution point. You can use system variables.

Settings specified after task creation

You can specify the following settings only after a task is created.

- **Settings** section, **Content of updates** block.

- **Download diff files**

This option enables the downloading diff files feature (see section "Using diff files for updating Kaspersky databases and software modules" on page [412](#)).

By default, this option is disabled.

See also:

General task settings	928
Creating the Downloading updates to the repositories of distribution points task	417

Find vulnerabilities and required updates task settings

Settings specified during task creation

You can specify the following settings when creating a task. Some of these settings can also be modified in the properties of the created task.

- **Search for vulnerabilities and updates listed by Microsoft**

When searching for vulnerabilities and updates, Kaspersky Security Center uses the information about applicable Microsoft updates from the source of Microsoft updates, which are available at the present moment.

For example, you may want to disable this option if you have different tasks with different settings for Microsoft updates and updates of third-party applications.

By default, this option is enabled.

- **Connect to the update server to update data**

Windows Update Agent on a managed device connects to the source of Microsoft updates. The following servers can act as a source of Microsoft updates:

- Kaspersky Security Center Administration Server (see the settings of Network Agent policy (see section "Network Agent policy settings" on page [665](#)))
- Windows Server with Microsoft Windows Server Update Services (WSUS) deployed in your organization's network
- Microsoft Updates servers

If this option is enabled, Windows Update Agent on a managed device connects to the source of Microsoft updates to refresh the information about applicable Microsoft Windows updates.

If this option is disabled, Windows Update Agent on a managed device uses the information about applicable Microsoft Windows updates that was received from the source of Microsoft updates earlier and that is stored in the device's cache.

Connecting to the source of Microsoft updates can be resource-consuming. You might want to disable this option if you set regular connection to this source of updates in another task or in the properties of Network Agent policy, in the section **Software updates and vulnerabilities**. If you do not want to disable this option, then, to reduce the Server overload, you can configure the task schedule to randomize delay for task starts within 360 minutes.

By default, this option is enabled.

Combination of the following options of the settings of Network Agent policy defines the mode of getting updates:

- Windows Update Agent on a managed device connects to the Update Server to get updates only if the **Connect to the update server to update data** option is enabled and the **Active** option, in the **Windows Update search mode** settings group, is selected.
- Windows Update Agent on a managed device uses the information about applicable Microsoft Windows updates that was received from the source of Microsoft updates earlier and that is stored in the device's cache, if the **Connect to the update server to update data** option is enabled and the **Passive** option, in the **Windows Update search mode** settings group, is selected, or if the **Connect to the update server to update data** option is disabled and the **Active** option, in the **Windows Update search mode** settings group, is selected.
- Irrespective of the **Connect to the update server to update data** option's status (enabled or disabled), if **Disabled** option, in the **Windows Update search mode** settings group is selected, Kaspersky Security Center does not request any information about updates.

- **Search for third-party vulnerabilities and updates listed by Kaspersky**

If this option is enabled, Kaspersky Security Center searches for vulnerabilities and required updates for third-party applications (applications made by software vendors other than Kaspersky and Microsoft) in Windows Registry and in the folders specified under **Specify paths for advanced search of applications in file system**. The full list of supported third-party applications is managed by Kaspersky.

If this option is disabled, Kaspersky Security Center does not search for vulnerabilities and required updates for third-party applications. For example, you may want to disable this option if you have different tasks with different settings for Microsoft Windows updates and updates of third-party applications.

By default, this option is enabled.

- **Specify paths for advanced search of applications in file system**

The folders in which Kaspersky Security Center searches for third-party applications that require vulnerability fix and update installation. You can use system variables.

Specify the folders to which applications are installed. By default, the list contains system folders to which most of the applications are installed.

- **Enable advanced diagnostics**

If this feature is enabled, Network Agent writes traces even if tracing is disabled for Network Agent in Kaspersky Security Center Remote Diagnostics Utility. Traces are written to two files in turn; the total size of both files is determined by the **Maximum size, in MB, of advanced diagnostics files** value. When both files are full, Network Agent starts writing to them again. The files with traces are stored in the %WINDIR%\Temp folder. These files are accessible in the remote diagnostics utility (see section "Remote diagnostics of client devices. Kaspersky Security Center remote diagnostics utility" on page [651](#)), you can download or delete them there.

If this feature is disabled, Network Agent writes traces according to the settings in Kaspersky Security Center Remote Diagnostics Utility. No additional traces are written.

When creating a task, you do not have to enable advanced diagnostics. You may want to use this feature later if, for example, a task run fails on some of the devices and you want to collect additional information during another task run.

By default, the feature is disabled.

- **Maximum size, in MB, of advanced diagnostics files**

The default value is 100 MB, and available values are between 1 MB and 2 048 MB. You may be asked to change the default value by Kaspersky Technical Support specialists when information in the advanced diagnostics files sent by you is not enough to troubleshoot the problem.

See also:

General task settings	928
Scanning applications for vulnerabilities.....	464

Install required updates and fix vulnerabilities task settings

Settings specified during task creation

You can specify the following settings when creating a task. Some of these settings can also be modified in the properties of the created task.

- **Specify rules for installing updates**

These rules are applied to installation of updates on client devices. If rules are not specified, the task has nothing to perform. For information about operations with rules, refer to Rules for update installation (on page [482](#)).

- **Start installation at device restart or shutdown**

If this option is enabled, updates are installed when the device is restarted or shut down. Otherwise, updates are installed according to a schedule.

Use this option if installing the updates might affect the device performance.

By default, this option is disabled.

- **Install required general system components**

If this option is enabled, before installing an update the application automatically installs all general system components (prerequisites) that are required to install the update. For example, these prerequisites can be operating system updates

If this option is disabled, you may have to install the prerequisites manually.

By default, this option is disabled.

- **Allow installation of new application versions during updates**

If this option is enabled, updates are allowed when they result in installation of a new version of a software application.

If this option is disabled, the software is not upgraded. You can then install new versions of the software manually or through another task. For example, you may use this option if your company infrastructure is not supported by a new software version or if you want to check an upgrade in a test infrastructure.

By default, this option is enabled.

Upgrading an application may cause malfunction of dependent applications installed on client devices.

- **Download updates to the device without installing them**

If this option is enabled, the application downloads updates to the device but does not install them automatically. You can then Install downloaded updates manually.

Microsoft updates are downloaded to the system Windows storage. Updates of third-party applications (applications made by software vendors other than Kaspersky and Microsoft) are downloaded to the folder specified in the **Folder for downloading updates** field.

If this option is disabled, the updates are installed to the device automatically.

By default, this option is disabled.

- **Folder for downloading updates**

This folder is used to download updates of third-party applications (applications made by software vendors other than Kaspersky and Microsoft).

- **Enable advanced diagnostics**

If this feature is enabled, Network Agent writes traces even if tracing is disabled for Network Agent in Kaspersky Security Center Remote Diagnostics Utility. Traces are written to two files in turn; the total size of both files is determined by the **Maximum size, in MB, of advanced diagnostics files** value. When both files are full, Network Agent starts writing to them again. The files with traces are stored in the %WINDIR%\Temp folder. These files are accessible in the remote diagnostics utility (see section "Remote diagnostics of client devices. Kaspersky Security Center remote diagnostics utility" on page [651](#)), you can download or delete them there.

If this feature is disabled, Network Agent writes traces according to the settings in Kaspersky Security Center Remote Diagnostics Utility. No additional traces are written.

When creating a task, you do not have to enable advanced diagnostics. You may want to use this feature later if, for example, a task run fails on some of the devices and you want to collect additional information during another task run.

By default, the feature is disabled.

- **Maximum size, in MB, of advanced diagnostics files**

The default value is 100 MB, and available values are between 1 MB and 2 048 MB. You may be asked to change the default value by Kaspersky Technical Support specialists when information in the advanced diagnostics files sent by you is not enough to troubleshoot the problem.

Settings specified after task creation

You can specify the following settings only after a task is created.

- Updates to install

In the **Updates to install** section, you can view the list of updates that the task installs. Only updates that match the applied task settings are shown.

- Test installation of updates:

- **Do not scan.** Select this option if you do not want to perform a test installation of updates.

- **Run scan on selected devices.** Select this option if you want to test updates installation on selected devices. Click the **Add** button and select devices on which you need to perform test installation of updates.
- **Run scan on devices in the specified group.** Select this option if you want to test updates installation on a group of devices. In the **Specify a test group** field, specify a group of devices on which you want to perform a test installation.
- **Run scan on specified percentage of devices.** Select this option if you want to test updates installation on some portion of devices. In the **Percentage of test devices out of all target devices** field, specify the percentage of devices on which you want to perform a test installation of updates.

See also:

General task settings	928
Installing updates on devices manually	444
Fixing vulnerabilities in applications	469

Global list of subnets

This section provides information about the global list of subnets that you can use in the rules.

To store the information about subnets of your network, you can set up a global list of subnets for each Administration Server you use. This list helps you match pairs {IP address, mask} and physical units such as branch offices. You can use subnets from this list in the networking rules and settings.

In this section

Adding subnets to the global list of subnets	941
Viewing and modifying subnet properties in the global list of subnets	942

Adding subnets to the global list of subnets

You can add subnets with their descriptions to the global list of subnets.

► *To add a subnet to the global list of subnets:*

1. In the console tree, select the node of the Administration Server that you require.
2. In the context menu of the Administration Server, select **Properties**.
3. In the **Properties** window that opens, in the **Sections** pane select **List of global subnets**.
4. Click the **Add** button.

The **New subnet** window opens.

5. Fill in the following fields:

- **General settings**

The subnet address for the subnet you are adding.

- **Subnet mask**

The subnet mask for the subnet you are adding.

- **Name**

The name of the subnet. It must be unique within the global list of subnets. If you enter the name that already exists in the list, an index will be added, for example: ~-1, ~-2.

- **Description**

Description may contain some additional information about the branch office which has this subnet. This text will appear in all lists where this subnet is present, for example, in the list of traffic limitation rules.

This field is not obligatory and may be left empty.

1. Click **OK**.

The subnet appears in the list of subnets.

Viewing and modifying subnet properties in the global list of subnets

You can view and modify the properties of subnets in the global list of subnets.

► *To view or modify properties of a subnet in the global list of subnets:*

1. In the console tree, select the node of the Administration Server that you require.
2. In the context menu of the Administration Server, select **Properties**.
3. In the **Properties** window that opens, in the left **Sections** pane, select **List of global subnets**.
4. In the list, select the subnet that you want.
5. Click the **Properties** button.

The **New subnet** window opens.

6. If necessary, change the settings (see section "Adding subnets to the global list of subnets" on page [941](#)) of the subnet.
7. Click **OK**.

If you have made changes, they will be stored.

Usage of Network Agent for Windows, for macOS and for Linux: comparison

The Network Agent usage varies depending on the operating system of the device. The Network Agent policy (see section "Network Agent policy settings" on page [665](#)) and installation package (see section "Network Agent installation package settings" on page [183](#)) settings also differ depending on the operating system. The table below compares Network Agent features and usage scenarios available for Windows, macOS, and Linux operating systems.

Table 77. Network Agent feature comparison

Network Agent feature	Windows	macOS	Linux
Installation	Installation	Installation	Installation
Automatic generating of the Network Agent installation package after the installation of Kaspersky Security Center (see section "Installation packages" on page 152)	✓	No	No
Installing in forced mode, using special options in the remote installation task of Kaspersky Security Center (see section "Forced deployment through the remote installation task of Kaspersky Security Center" on page 158)	✓	✓	✓
Installing by sending device users links to stand-alone packages generated by Kaspersky Security Center (see section "Running stand-alone packages created by Kaspersky Security Center" on page 159)	✓	✓	✓
Installing by cloning an image of the administrator's hard drive with the operating system and Network Agent: using tools provided by Kaspersky Security Center for handling disk images, or using third-party tools (see section "Deployment by capturing and copying the hard drive image of a device" on page 154)	✓	No	No
Installing with third-party tools for remote installation of applications (see section "Deployment with third-party tools for remote installation of applications" on page 153)	✓	✓	✓
Installing manually, by running application installers on devices (see section "Options for manual installation of applications" on page 159)	✓	✓	✓
Installing Network Agent in silent mode (see section "Installation in silent mode (with a response file)" on page 164)	✓	✓	✓

Network Agent feature	Windows	macOS	Linux
Installing Network Agent in non-interactive mode (see section "Installing Network Agent in non-interactive (silent) mode" on page 179)	✓	No	No
Manually connecting a client device to the Administration Server. klmove utility (on page 638)	✓	✓	✓
Automatic installing of updates and patches for Kaspersky Security Center components (see section "Automatic updating and patching for Kaspersky Security Center components" on page 457)	✓	No	No
Automatic distributing of a key (see section "Automatic distribution of a license key" on page 361)	✓	✓	✓
Forced synchronization (on page 646)	✓	✓	✓
Distribution point	Distribution point	Distribution point	Distribution point
Using as distribution point (see section "About distribution points" on page 133)	✓	✓	✓
Automatic assignment of distribution points (see section "Calculating the number and configuration of distribution points" on page 134)	✓	✓	✓
All types of network polling (see section "Device discovery" on page 304)	✓	No	No
Running KSN Proxy service on a distribution point side (see section "Assigning a device a distribution point manually" on page 427)	✓	No	No

Network Agent feature	Windows	macOS	Linux
Push installation of applications on Windows devices	✓	Restricted: after the operating system type is defined on the networked devices through polling, Administration Server does not attempt to perform push installation on Windows devices by using non-Windows distribution points	Restricted: after the operating system type is defined on the networked devices through polling, Administration Server does not attempt to perform push installation on Windows devices by using non-Windows distribution points
Downloading updates to the repositories of distribution points directly from Kaspersky update servers (see section "Creating the Downloading updates to the repositories of distribution points task" on page 417)	✓	No (if one or more devices running Linux or macOS are within the scope of the Download updates to the repositories of distribution points task, the task completes with the Failed status, even if it has successfully completed on all Windows devices)	No (if one or more devices running Linux or macOS are within the scope of the Download updates to the repositories of distribution points task, the task completes with the Failed status, even if it has successfully completed on all Windows devices)
Offline model of update download (on page 442)	✓	✓	✓
Handling other applications	Handling other applications	Handling other applications	Handling other applications
Remote installing of applications on devices (see section "Remote installation of applications on devices with Network Agent installed" on page 160)	✓	No	No
Software updates (see section "Installation of third-party software updates" on page 432)	✓	No	No
Configuring operating system updates in a Network Agent policy (see section "Configuring Windows updates in a Network Agent policy" on page 455)	✓	No	No
Viewing information about software vulnerabilities (on page 463)	✓	No	No

Network Agent feature	Windows	macOS	Linux
Scanning applications for vulnerabilities (on page 464)	✓	No	No
Inventory of software installed on devices (see section "Changing the software inventory start time" on page 497)	✓	No	No
Viewing the applications registry (on page 496)	✓	No	No
Installation of applications via stand-alone packages created by Kaspersky Security Center (see section "Running stand-alone packages created by Kaspersky Security Center" on page 159)	✓	No	No
Virtual machines	Virtual machines	Virtual machines	Virtual machines
Installing Network Agent on a virtual machine (see section "Virtual infrastructure" on page 175)	✓	No	✓
Optimization settings for virtual desktop infrastructure (VDI) (see section "Tips on reducing the load on virtual machines" on page 175)	✓	✓	✓
Support of dynamic virtual machines (on page 175)	✓	✓	✓
Other	Other	Other	Other
Auditing actions on a remote client device by using Windows Desktop Sharing (see section "Auditing actions on a remote client device" on page 641)	✓	No	No
Monitoring the anti-virus protection status (see section "Monitoring the anti-virus protection status using information from the system registry" on page 584)	✓	No	No
Managing device restarts (see section "Configuring the restart of a client device" on page 641)	✓	No	No
Support of file system rollback (see section "Support of file system rollback for devices with Network Agent" on page 176)	✓	✓	✓

Network Agent feature	Windows	macOS	Linux
Using a Network Agent as connection gateway (see section "Using a distribution point as connection gateway" on page 594)	✓	✓	✓
Connections manager (see section "About connection schedule" on page 647)	✓	✓	✓
Network Agent switching from one Administration Server to another (automatically by network location) (see section "About switching Network Agent to other Administration Servers" on page 291)	✓	✓	✓
Checking the connection between a client device and the Administration Server. klnagchk utility (see section "Manually checking the connection between a client device and the Administration Server. Klnagchk utility" on page 643)	✓	✓	✓
Remotely connecting to the desktop of a client device (on page 639)	✓	✓	✓
Downloading a stand-alone installation package through the Migration Wizard	✓	No	No

See also:

Deploying Network Agent and the security application[150](#)



Dear User,

Thank you for choosing Kaspersky as your security software provider. We hope that this document will help you to use our product.

Attention! This document is the property of AO Kaspersky Lab (herein also referred to as Kaspersky): all rights to this document are reserved by the copyright laws of the Russian Federation and by international treaties. Illegal reproduction and distribution of this document or parts hereof incur civil, administrative, or criminal liability under applicable law.

Any type of reproduction or distribution of any materials, including translations, is allowed only with the written permission of Kaspersky.

This document, and graphic images related to it, may be used for informational, non-commercial, and personal purposes only.

Kaspersky reserves the right to amend this document without additional notification.

Kaspersky assumes no liability for the content, quality, relevance, or accuracy of any materials used in this document to which rights are held by third parties, or for any potential harms associated with use of the document.

Document revision date: 3/22/2021

© 2021 AO Kaspersky Lab

<https://www.kaspersky.com>

<https://help.kaspersky.com>

<https://support.kaspersky.com>

About Kaspersky: (<https://www.kaspersky.com/about/company>)

Frequently Asked Questions



Deployment

What operating systems and platforms are supported? (see section "Hardware and software requirements" on page [31](#))

What processes does Kaspersky Security Center start? (see section "Ports used by Kaspersky Security Center" on page [65](#))

How to select a structure for protection of an organization (see section "Selecting a structure for protection of an enterprise" on page [125](#)): single office (see section "Standard configuration: Single office" on page [126](#)), few large-scale offices (see section "Standard configuration: A few large-scale offices run by their own administrators" on page [127](#)), or multiple small remote offices (see section "Standard configuration: Multiple small remote offices" on page [127](#))?

How many client devices can be connected to the Kaspersky Security Center? (see section "Results of Administration Server performance testing" on page [148](#))

What rights are required for work with the DBMS? (see section "Accounts for work with the DBMS" on page [215](#))

How to install the Administration Server (see section "Administration Server installation parameters" on page [166](#)) and the Network Agent (see section "Network Agent installation parameters" on page [171](#)) from the command line (installation settings)?

What will change with the system after installing the Administration Server? (see section "Changes in the system after Administration Server installation on the device" on page [259](#))

How to connect the Administration Console to the Administration Server? (see section "Configuring the connection of Administration Console to Administration Server" on page [278](#))

How to configure a proxy server for the Kaspersky Security Center? (see section "Step 2. Configuring a proxy server" on page [271](#))

How to configure a SMTP server for the Kaspersky Security Center? (see section "Step 8. Configuring email notifications" on page [271](#))

What are the most common problems with installing Kaspersky Security Center? (see section "Problems with remote installation of applications" on page [878](#))

How to move the Administration Server to another server? (see section "Moving Administration Server to another device" on page [622](#))



Upgrading

How to build an update structure: (see section "Adjustment of distribution points and connection gateways" on page [587](#)) single office (see section "Standard configuration of distribution points: Single office" on page [588](#)), multiple small remote offices? (see section "Standard configuration of distribution points: Multiple small remote offices" on page [588](#))

How to connect WSUS server? (see section "Synchronizing updates from Windows Update with Administration Server" on page [436](#))

How to update Kaspersky Endpoint Security manually? (see section "Manual setup of the group update task for Kaspersky Endpoint Security" on page [371](#))

How to update third-party applications? (see section "Installation of third-party software updates" on page [432](#))

Is it possible to install update offline? (see section "Offline model of update download" on page [442](#))

How to configure automatic updates distribution? (see section "Automatic distribution of updates" on page [424](#))



Control and reports

Where to view the deployment report for protection applications? (see section "Viewing a protection deployment report" on page [342](#))

How is the protection application and the Network Agent monitored on new devices? (see section "Monitoring the deployment of applications" on page [163](#))

What is the average traffic consumption per day? (see section "Traffic per 24 hours" on page [141](#))

How to enable audit on a remote computer turn on? (see section "Auditing actions on a remote client device" on page [641](#))

How to monitor the status of anti-virus protection in the system registry? (see section "Monitoring the anti-virus protection status using information from the system registry" on page [584](#))

How to get the trace file? (see section "Enabling and disabling tracing, downloading the trace file" on page [654](#))

How to perform software inventory on a remote computer? (see section "Changing the software inventory start time" on page [654](#))

How to create event selections for reporting? (see section "Event selections" on page [518](#))

How to download the event log? (see section "Downloading event logs" on page [656](#))

Kaspersky Security Center 13 Web Console

This section describes operations that you can perform by using Kaspersky Security Center 13 Web Console.

In this chapter

About Kaspersky Security Center 13 Web Console	954
Hardware and software requirements for Kaspersky Security Center 13 Web Console	955
List of Kaspersky applications supported by Kaspersky Security Center 13 Web Console.....	957
Deployment diagram of Kaspersky Security Center Administration Server and Kaspersky Security Center 13 Web Console	959
Ports used by Kaspersky Security Center 13 Web Console	960
Scenario: Installation and initial setup of Kaspersky Security Center 13 Web Console	962
Installation.....	964
Migration to Kaspersky Security Center Cloud Console	980
Logging in to Kaspersky Security Center 13 Web Console and logging out.....	991
Configuring domain authentication by using the NTLM and Kerberos protocols	992
Quick Start Wizard (Kaspersky Security Center 13 Web Console).....	993
Protection Deployment Wizard	1001
Configuring Administration Server.....	1007
Kaspersky applications deployment through Kaspersky Security Center 13 Web Console	1023
Discovering networked devices	1037
Kaspersky applications: licensing and activation	1054
Configuring network protection.....	1061
Scenario: Upgrading Kaspersky Security Center and managed security applications	1173
Updating Kaspersky databases and applications.....	1174
Managing third-party applications on client devices.....	1207
Monitoring and reporting.....	1277
Kaspersky Security Center 13 Web Console activity logging.....	1368
Integration between Kaspersky Security Center Web Console and other Kaspersky solutions ...	1369
Working with Kaspersky Security Center 13 Web Console in a cloud environment	1370
Remote diagnostics of client devices	1387

About Kaspersky Security Center 13 Web Console

Kaspersky Security Center 13 Web Console is a web application designed to manage the status of the security system of a network protected by Kaspersky applications.

Using the application, you can do the following:

- Manage the status of the organization's security system.
- Install Kaspersky applications on devices on your network and manage installed applications.
- Manage policies created for devices on your network.
- Manage user accounts.
- Manage tasks for applications installed on your network devices.
- View reports on the security system status.
- Manage the delivery of reports to system administrators and other IT experts.

Kaspersky Security Center 13 Web Console provides a web interface that ensures interaction between your device and Administration Server over a browser. Administration Server is an application designed for managing Kaspersky applications installed on your network devices. Administration Server connects to devices on your network over channels protected with Secure Socket Layer (SSL). When you connect to Kaspersky Security Center 13 Web Console by using your browser, the browser establishes a connection with Kaspersky Security Center 13 Web Console Server.

You operate Kaspersky Security Center 13 Web Console as follows:

1. Use a browser to connect to Kaspersky Security Center 13 Web Console, where the web portal interface is displayed.
2. Use web portal controls to choose a command that you want to run. Kaspersky Security Center 13 Web Console performs the following operations:
 - If you select a command used for receiving information (for example, to view a list of devices), Kaspersky Security Center 13 Web Console generates a request for information to Administration Server, receives the necessary data, and sends it to the browser in an easy-to-view format.
 - If you have chosen a command used for management (for example, remote installation of an application), Kaspersky Security Center 13 Web Console receives the command from the browser and sends it to Administration Server. Then the application receives the result from Administration Server and sends it to the browser in an easy-to-view format.

Kaspersky Security Center 13 Web Console is a multi-language application. You can change the interface language at any time, without reopening the application. When you install Kaspersky Security Center 13 Web Console together with Kaspersky Security Center, Kaspersky Security Center 13 Web Console has the same interface language as the installation file. When you install only Kaspersky Security Center 13 Web Console, the application has the same interface language as your operating system. If Kaspersky Security Center 13 Web Console does not support the language of the installation file or operating system, English is set by default.

Mobile Device Management is not supported in Kaspersky Security Center 13 Web Console. However, if you added mobile devices to an administration group by using Microsoft Management Console, these devices are also displayed in Kaspersky Security Center 13 Web Console.

Work in cloud environments (see section "Working with Kaspersky Security Center 13 Web Console in a cloud environment" on page [1370](#)) is supported in Kaspersky Security Center 12.1 Web Console or a later version.

Hardware and software requirements for Kaspersky Security Center 13 Web Console

Kaspersky Security Center 13 Web Console Server

Minimum hardware requirements:

- CPU: 4 cores, operating frequency of 2.5 GHz
- RAM: 8 GB
- Available disk space: 40 GB

One of the following operating systems:

- Microsoft Windows (64-bit versions only):
 - Microsoft Windows 10 20H2
 - Microsoft Windows 10 20H1
 - Microsoft Windows 10 Enterprise 2019 LTSC
 - Microsoft Windows 10 Enterprise 2016 LTSC
 - Microsoft Windows 10 Enterprise 2015 LTSC
 - Microsoft Windows 10 Pro RS5 (October 2018 Update, 1809)
 - Microsoft Windows 10 Pro for Workstations RS5 (October 2018 Update, 1809)
 - Microsoft Windows 10 Enterprise RS5 (October 2018 Update, 1809)
 - Microsoft Windows 10 Education RS5 (October 2018 Update, 1809)
 - Microsoft Windows 10 Pro 19H1
 - Microsoft Windows 10 Pro for Workstations 19H1
 - Microsoft Windows 10 Enterprise 19H1
 - Microsoft Windows 10 Education 19H1
 - Microsoft Windows 10 Home 19H2
 - Microsoft Windows 10 Pro 19H2
 - Microsoft Windows 10 Pro for Workstations 19H2
 - Microsoft Windows 10 Enterprise 19H2
 - Microsoft Windows 10 Education 19H2
 - Microsoft Windows 8.1 Pro
 - Microsoft Windows 8.1 Enterprise
 - Windows Server® 2019 Standard
 - Windows Server 2019 Core
 - Windows Server 2019 Datacenter
 - Windows Server 2016 Server Standard RS3 (v1709) (LTSC/CBB)
 - Windows Server 2016 Server Datacenter RS3 (v1709) (LTSC/CBB)

- Windows Server 2016 Server Core RS3 (v1709) (Installation Option) (LTSB/CBB)
- Windows Server 2016 Standard (LTSB)
- Windows Server 2016 Server Core (Installation Option) (LTSB)
- Windows Server 2016 Datacenter (LTSB)
- Windows Server 2012 R2 Standard
- Windows Server 2012 R2 Server Core
- Windows Server 2012 R2 Foundation
- Windows Server 2012 R2 Essentials
- Windows Server 2012 R2 Datacenter
- Windows Server 2012 Standard
- Windows Server 2012 Server Core
- Windows Server 2012 Foundation
- Windows Server 2012 Essentials
- Windows Server 2012 Datacenter
- Windows Storage Server 2016
- Windows Storage Server 2012 R2
- Windows Storage Server 2012
- Linux (64-bit versions only):
 - Debian GNU/Linux® 10.x (Buster)
 - Debian GNU/Linux 9.x (Stretch)
 - Ubuntu Server 20.04 LTS (Focal Fossa)
 - Ubuntu Server 18.04 LTS (Bionic Beaver)
 - CentOS 8.x
 - CentOS 7.x
 - Red Hat Enterprise Linux Server 8.x
 - Red Hat Enterprise Linux Server 7.x
 - SUSE Linux Enterprise Server 15 (all Service Packs)
 - SUSE Linux Enterprise Server 12 (all Service Packs)
 - Astra Linux Special, version 1.6
 - Astra Linux Special, version 1.5
 - Astra Linux Common Edition, version 2.12
 - ALT 9.1
 - ALT 8.3
 - ALT SE 8

Client devices

For a client device, use of Kaspersky Security Center 13 Web Console requires only a browser.

The hardware and software requirements for the device are identical to the requirements of the browser that is used with Kaspersky Security Center 13 Web Console.

Browser:

- Mozilla Firefox™ 78 Extended Support Release
- Mozilla Firefox 78 or later
- Google Chrome™ 88 or later
- Safari 14 on macOS

See also:

List of Kaspersky applications supported by Kaspersky Security Center 13 Web Console.....[957](#)

List of Kaspersky applications supported by Kaspersky Security Center 13 Web Console

Kaspersky Security Center 13 Web Console supports centralized deployment and management of the following Kaspersky applications:

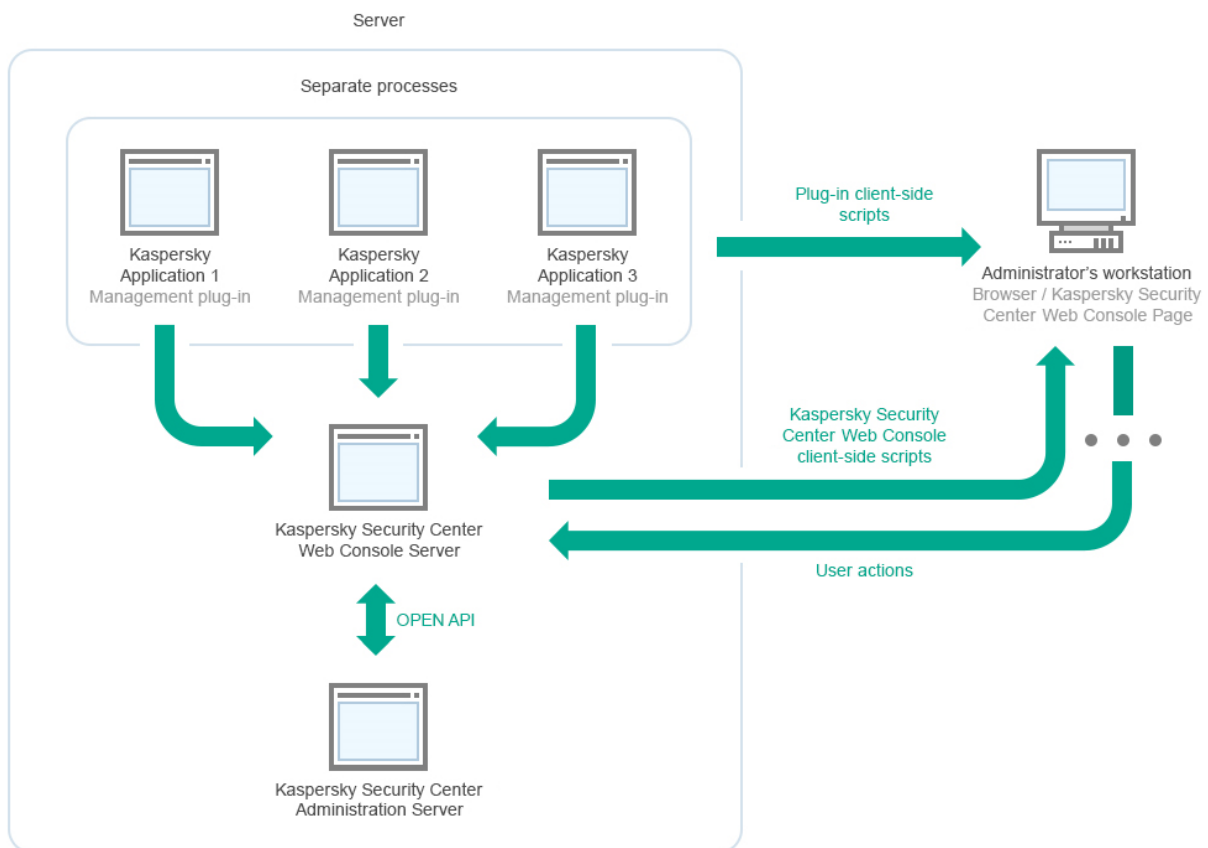
- **For workstations:**
 - Kaspersky Endpoint Security 11 for Windows (workstation mode): 11.5, 11.6
 - Kaspersky Endpoint Security 11 for Linux (Desktop Protection): 11.1, 11.2
 - Kaspersky Endpoint Security 10.1 for Linux ARM Edition
 - Kaspersky Endpoint Security 11 for Mac: 11.0, 11.1
 - Kaspersky Embedded Systems Security 3.0 for Windows
 - Kaspersky Endpoint Agent: 3.9, 3.10
 - Kaspersky Managed Detection and Response 2.0
- **For file servers:**
 - Kaspersky Security 11 for Windows Server
 - Kaspersky Endpoint Security 11 for Windows (file server mode): 11.5, 11.6
 - Kaspersky Endpoint Security 11 for Linux (Server Protection): 11.1, 11.2
- **For virtual machines:** Kaspersky Security for Virtualization 5.1 Light Agent

Kaspersky Security Center 13 Web Console supports centralized management of the following Kaspersky applications:

- Kaspersky IoT Secure Gateway 2.0
- KasperskyOS for Thin Client

Deployment diagram of Kaspersky Security Center Administration Server and Kaspersky Security Center 13 Web Console

The figure below shows the deployment diagram of Kaspersky Security Center Administration Server and Kaspersky Security Center 13 Web Console.



Management plug-ins for Kaspersky applications installed on protected devices (one plug-in for each application) are deployed together with Kaspersky Security Center 13 Web Console Server.

As an administrator, you access Kaspersky Security Center 13 Web Console by using a browser on your workstation.

When you perform specific actions in Kaspersky Security Center 13 Web Console, Kaspersky Security Center 13 Web Console Server communicates with Kaspersky Security Center Administration Server through OpenAPI. Kaspersky Security Center 13 Web Console Server requests the required information from Kaspersky Security Center Administration Server and displays the results of your operations in Kaspersky Security Center 13 Web Console.

Ports used by Kaspersky Security Center 13 Web Console

The table below lists the ports that must be open on the device where Kaspersky Security Center 13 Web Console Server (also referred to as Kaspersky Security Center 13 Web Console) is installed.

Table 78. Ports used by Kaspersky Security Center 13 Web Console

Service name	Port number	Protocol	Port purpose	Scope
KSCWebConsole	2000 (not used in Kaspersky Security Center 12.1 Web Console or later versions)	HTTP S	Port for web interface	Running node.exe processes of both Kaspersky Security Center 13 Web Console and management plugins
	2001	HTTP S	API port that is used to receive requests from the KSCWebConsoleManagementService service running on the same device	
KSCWebConsoleManagementService	2002 (not used in Kaspersky Security Center 12.1 Web Console or later versions)	HTTP S	Port for web interface	Updating Kaspersky Security Center 13 Web Console components
	2003	HTTP S	API port that is used to receive requests from the KSCWebConsole service running on the same device	
KSCWebConsoleMessageQueue	8200	HTTP	API port that is used to generate certificates by means of HashiCorp Vault (for more details, see the HashiCorp Vault website https://www.vaultproject.io/)	Installing Kaspersky Security Center 13 Web Console and updating Kaspersky Security Center 13 Web Console components
	4152	HTTP S	API port of the Message Broker that is used for communication between processes of both Kaspersky Security Center 13 Web Console and management plugins	Interaction between Kaspersky Security Center 13 Web Console and management plugins

See also:

Ports used by Kaspersky Security Center	65
---	--------------------

Scenario: Installation and initial setup of Kaspersky Security Center 13 Web Console

This scenario describes how to install Kaspersky Security Center 13 Administration Server and Kaspersky Security Center 13 Web Console, perform initial setup of the Administration Server by using the Quick Start Wizard, and install Kaspersky applications on managed devices by using the Protection Deployment Wizard.

Installation and initial setup of Kaspersky Security Center 13 Web Console proceeds in stages:

a. Installing a database management system (DBMS)

Install the DBMS (see section "Installing a database management system" on page [964](#)) that will be used by Kaspersky Security Center or use an existing one.

b. Installing Administration Server, Administration Console, Network Agent

Administration Console and the server version of Network Agent are installed together with Administration Server.

During the installation of Kaspersky Security Center 13 Administration Server (see section "Installing Kaspersky Security Center (Standard installation)" on page [966](#)), specify whether you want to install Kaspersky Security Center 13 Web Console on the same device. If you choose to install both components on the same device, you do not have to install Kaspersky Security Center 13 Web Console separately, because it is installed automatically. If you want to install Kaspersky Security Center 13 Web Console on a different device, then, after installing Kaspersky Security Center 13 Administration Server, proceed to installing Kaspersky Security Center 13 Web Console.

c. Installing Kaspersky Security Center 13 Web Console

If you did not choose to install Kaspersky Security Center 13 Web Console together with the Kaspersky Security Center Administration Server, install Kaspersky Security Center 13 Web Console (see section "Installing Kaspersky Security Center 13 Web Console" on page [967](#)) on a different device.

d. Performing initial setup

When Administration Server installation is complete, the first connection to the Administration Server the Quick Start Wizard (see section "Quick Start Wizard (Kaspersky Security Center 13 Web Console)" on page [993](#)) starts automatically. Perform initial configuration of Administration Server according to the existing requirements. During the initial configuration stage, the Wizard uses the default settings to create the policies (see section "About policies and policy profiles" on page [1110](#)) and tasks (see section "About tasks" on page [1078](#)) that are required for protection deployment. However, the default settings may be less than optimal for the needs of your organization. If necessary, you can edit the settings of policies and tasks (see section "Scenario: Configuring network protection" on page [364](#)).

e. Licensing of Kaspersky Security Center (optional)

Kaspersky Security Center with support of Administration Console basic functionality (see section "Kaspersky Security Center licensing options" on page [320](#)) does not require a license. You need a commercial license if you want to use one or several of the additional features, including Vulnerability and Patch Management, Mobile Device Management, and Integration with the SIEM systems. You can add a key file or activation code for these features at the corresponding step (see section "Step 9. Selecting the application activation method" on page [998](#)) of the Quick Start Wizard or manually (see section "Adding a license key to the Administration Server repository" on page [1056](#)).

Kaspersky Security Center 13 Web Console does not support Mobile Device Management (on page [727](#)), Integration with the SIEM systems (see section "Exporting events to SIEM systems" on page [791](#)), and work in a cloud environment (see section "Working in a cloud environment" on page [820](#)). You can use Kaspersky Security Center 13 Web Console to add a key file or activation code for these features, but

subsequently the corresponding functionality will only be available in Microsoft Management Console-based Administration Console.

f. Discovery of networked devices

This stage is handled by the Quick Start Wizard (see section "Quick Start Wizard (Kaspersky Security Center 13 Web Console)" on page [993](#)). You can also discover the devices (see section "Scenario: Discovering networked devices" on page [303](#)) manually. Kaspersky Security Center receives the addresses and names of all devices detected on the network. You can then use Kaspersky Security Center to install Kaspersky applications and software from other vendors on the detected devices. Kaspersky Security Center regularly starts device discovery, which means that if any new instances appear on the network, they will be detected automatically.

g. Arranging devices into administration groups

This stage is handled by the Quick Start Wizard (see section "Quick Start Wizard (Kaspersky Security Center 13 Web Console)" on page [993](#)), but you can also move the detected devices into groups manually.

h. Installing Network Agent and security applications on networked devices

Deployment of protection on an enterprise network entails installation of Network Agent and security applications (for example, Kaspersky Endpoint Security for Windows (see section "Scenario: Kaspersky applications deployment through Kaspersky Security Center 13 Web Console" on page [1023](#))) on devices that have been detected by Administration Server during the device discovery.

To install the applications remotely, run the Protection Deployment Wizard.

Security applications protect devices against viruses and other programs that pose a threat. Network Agent ensures communication between the device and Administration Server. Network Agent settings are configured automatically by default.

Before you start installing Network Agent and the security applications on networked devices, make sure that these devices are accessible (turned on).

i. Deploying license keys to client devices

Deploy license keys (see section "Kaspersky applications: licensing and activation" on page [357](#)) to client devices to activate managed security applications on those devices.

j. Configuring Kaspersky application policies

To apply different application settings to different devices you can use device-centric security management and/or user-centric security management (see section "About device-centric and user-centric security management approaches" on page [367](#)). Device-centric security management can be implemented by using policies (see section "About policies and policy profiles" on page [1110](#)) and tasks (see section "About tasks" on page [1078](#)). You can apply tasks only to those devices that meet specific conditions. To set the conditions for filtering devices, use device selections (on page [1037](#)) and tags (see section "About device tags" on page [1046](#)).

k. Monitoring the network protection status

You can monitor your network by using widgets on the dashboard (see section "Using the dashboard" on page [1281](#)), generate reports (see section "Using reports" on page [1283](#)) from Kaspersky applications, configure and view selections of events (see section "Using event selections" on page [1289](#)) received from the applications on the managed devices, and view notification lists.

Installation

This section describes installation of Kaspersky Security Center and Kaspersky Security Center 13 Web Console.

In this chapter

Installing a database management system	964
Configuring the MariaDB x64 server for working with Kaspersky Security Center 13	964
Installing Kaspersky Security Center (Standard installation).....	966
Installing Kaspersky Security Center 13 Web Console	967
Installation of Kaspersky Security Center 13 Web Console on Linux platforms	969
Upgrading Kaspersky Security Center Web Console.....	974
Specifying certificates for trusted Administration Servers	975
Replacing certificate for Kaspersky Security Center 13 Web Console	976
Converting a PFX certificate to the PEM format.....	977
Reissuing the certificate for Kaspersky Security Center Web Console.....	978

Installing a database management system

Install the database management system (DBMS) that will be used by Kaspersky Security Center. You can choose from one of the supported (see section "Hardware and software requirements" on page [31](#)) versions of Microsoft SQL Server, MySQL, or MariaDB.

For information about how to install the selected DBMS, refer to its documentation.

For optimal use of MariaDB, you need to configure the recommended settings (see section "Configuring the MariaDB x64 server for working with Kaspersky Security Center 13" on page [964](#)).

See also:

Scenario: Installation and initial setup of Kaspersky Security Center 13 Web Console	962
--	---------------------

Configuring the MariaDB x64 server for working with Kaspersky Security Center 13

Kaspersky Security Center 13 supports MariaDB version 10.3.22 and later.

If you use the MariaDB server for Kaspersky Security Center, enable support of InnoDB and MEMORY storage, and of UTF-8 and UCS-2 encodings.

Recommended settings for the my.ini file

► *To configure the my.ini file:*

1. Open the my.ini file <https://mariadb.com/kb/en/configuring-mariadb-with-option-files/> in a text editor.
2. Enter the following lines into the my.ini file:

```
sort_buffer_size=10M
join_buffer_size=100M
join_buffer_space_limit=300M
join_cache_level=8
tmp_table_size=512M
max_heap_table_size=512M
key_buffer_size=200M
innodb_buffer_pool_size=<value>
innodb_thread_concurrency=20
innodb_flush_log_at_trx_commit=0
innodb_lock_wait_timeout=300
max_allowed_packet=32M
max_connections=151
```

The value of the `innodb_buffer_pool_size` must be no less than 80 percent of the expected KAV database size.

It is recommended to use the parameter value `innodb_flush_log_at_trx_commit=0`, because the values "1" or "2" negatively affect the operating speed of MariaDB.

By default, the optimizer add-ons `join_cache_incremental`, `join_cache_hashed`, and `join_cache_bka` are enabled. If these add-ons are not enabled, you must enable them.

► *To check whether optimizer add-ons are enabled:*

1. In the MariaDB client console, execute the command:

```
SELECT @@ optimizer_switch
```

2. Check that its output contains the following lines:

```
join_cache_incremental=on
join_cache_hashed=on
join_cache_bka=on
```

If these lines are present and have the value `on`, then the optimizer add-ons are enabled.

If these lines are missing or have the value `off`, you need to do the following:

1. Open the my.ini file in a text editor.
2. Add the following lines into the my.ini file:

```
optimizer_switch='join_cache_incremental=on'
optimizer_switch='join_cache_hashed=on'
optimizer_switch='join_cache_bka=on'
```

The add-ons `join_cache_incremental`, `join_cache_hash`, and `join_cache_bka` are enabled.

Installing Kaspersky Security Center (Standard installation)

This procedure describes how to install Kaspersky Security Center. Before installation, you must install a database management system (see section "Installing a database management system" on page [964](#)).

► *To install Kaspersky Security Center:*

1. Under an account with administrative privileges, run the `ksc_<build number>_full_<localization language>.exe` executable file.
2. In the application selection window that opens, click **Install Kaspersky Security Center**.
The Kaspersky Security Center Administration Server Setup Wizard starts.
3. Beginning with the Welcome page, proceed through the Wizard by using the **Next** button.
4. If Microsoft .NET Framework is not installed, install it.
5. Accept the terms of the License Agreement and the Privacy Policy.
6. Select the installation type. For evaluation purposes, we recommend that you keep the default **Standard** value.
7. If you want to install Kaspersky Security Center 13 Web Console on the same device, select the **Install Kaspersky Security Center 13 Web Console** check box.
If you clear the check box, you can later install Kaspersky Security Center 13 Web Console (see section "Installing Kaspersky Security Center 13 Web Console" on page [967](#)) separately on the same or another device.
8. Select the size of your network. For evaluation purposes, we recommend that you keep the default **Fewer than 100 networked devices** value.
9. Select the type of database server that you installed earlier (see section "Installing a database management system" on page [964](#)).
10. Specify the connection parameters for the database server that you installed earlier.
11. Specify the authentication parameters for the database server that you installed earlier.
12. Click the **Install** button to start the installation.
13. After the installation successfully completes, choose whether or not you want to start Administration Console right after you close the Wizard.

If you choose to open Kaspersky Security Center 13 Web Console, the login screen (see section "Installing Kaspersky Security Center 13 Web Console" on page [967](#)) will open. Then you will be able to perform the initial configuration of the Administration Server by using the Quick Start Wizard (see section "Quick Start Wizard (Kaspersky Security Center 13 Web Console)" on page [993](#)).

You can open Kaspersky Security Center 13 Web Console only if it is already installed. You cannot open Kaspersky Security Center 13 Web Console if you did not install it during the installation of Kaspersky Security Center or separately.

14. In the Administration Console window that opens, click the installed Administration Server.
15. In the Administration Server certificate window that opens, click the **Yes** button to continue.

The Administration Server Quick Start Wizard (on page [265](#)) starts if you did not run it in the web-based Administration Console.

Troubleshooting

If the Administration Server certificate window does not open and connection errors are displayed, try the following:

1. In Windows, open **Services (Control Panel → Administrative Tools → Services)**. Check that Kaspersky Security Center Network Agent and Kaspersky Security Center Administration Server services are running.
2. In Windows, open **Event Viewer (Control Panel → Administrative Tools → Event Viewer)**, and then select **Applications and Services Logs → Kaspersky Event Log**. Make sure that the log does not contain errors and contains events like **Administration Server <version number> is running**.

See also:

Scenario: Installation and initial setup of Kaspersky Security Center 13 Web Console[962](#)

Installing Kaspersky Security Center 13 Web Console

This section describes how to install Kaspersky Security Center 13 Web Console Server (also referred to as Kaspersky Security Center 13 Web Console) separately. Before installation, you must install a database management system (see section "Installing a database management system" on page [964](#)) and the Kaspersky Security Center (see section "Installing Kaspersky Security Center (Standard installation)" on page [966](#)) Administration Server. You can install Kaspersky Security Center 13 Web Console either on the same device where Kaspersky Security Center is installed, or on a different one.

► To install Kaspersky Security Center 13 Web Console:

1. Under an account with administrative privileges, run the KSCWebConsoleInstaller.<version number>.<build number>.exe executable file.
This starts the Setup Wizard.
2. Select a language for the Setup Wizard.
3. In the welcome window, click **Next**.
4. In the **License Agreement** window, read and accept the terms of the End User License Agreement. The installation continues after you accept the EULA, otherwise, the **Next** button is unavailable.
5. In the **Destination folder** window, select a folder where Kaspersky Security Center 13 Web Console will be installed (by default, %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center Web Console). If such a folder does not exist, it is created automatically during the installation.

You can change the destination folder by using the **Browse** button.

6. In the **Kaspersky Security Center 13 Web Console connection settings** window, specify the following information:
 - The address of Kaspersky Security Center 13 Web Console (by default, 127.0.0.1).
 - The port that Kaspersky Security Center 13 Web Console will use for incoming connections, that is, the port that gives access to Kaspersky Security Center 13 Web Console from a browser (by default, 8080).

We recommend that you leave the address and the port number as they are.

If you want, you can click **Test** to make sure if the selected port is available.

If you want to enable logging of Kaspersky Security Center 13 Web Console activities (see section "Kaspersky Security Center 13 Web Console activity logging" on page [1368](#)), select the appropriate option. If you do not select this option, Kaspersky Security Center 13 Web Console log files will not be created.

Certificates in PFX format are not supported by Kaspersky Security Center 13 Web Console. To use such a certificate, you must first convert it to the supported PEM format (see section "Converting a PFX certificate to the PEM format" on page [977](#)), using an OpenSSL-based cross-platform utility, such as OpenSSL for Windows.

7. In the **Account settings** window, specify the account names and passwords.
We recommend that you use default accounts.
8. In the **Client certificate** window, select one of the following:
 - **Generate new certificate.** This option is recommended if you do not have a browser certificate.
 - **Choose existing certificate.** You can select this option if you already have a browser certificate; in this case, specify the path to it.
9. In the **Trusted Administration Servers** window, make sure that your Administration Server is on the list and click **Next** to proceed to the last window of the installer.
10. In the last window of the installer, click **Install** to begin the installation.

After the installation successfully completes, a shortcut appears on your desktop, and you can log in (see section "Logging in to Kaspersky Security Center 13 Web Console and logging out" on page [991](#)) to Kaspersky Security Center 13 Web Console.

The Administration Server Quick Start Wizard (see section "Quick Start Wizard (Kaspersky Security Center 13 Web Console)" on page [993](#)) starts if you did not run it in the Microsoft Management Console based Administration Console.

Troubleshooting

► *If Kaspersky Security Center 13 Web Console is not displayed in your browser at the URL you typed, try the following:*

1. Check that you specified the correct host name or IP address of the device on which Kaspersky Security Center 13 Web Console is installed.
2. Check that the device that you want to operate has access to the device on which Kaspersky Security Center 13 Web Console is installed.
3. Check that firewall settings on the device on which Kaspersky Security Center 13 Web Console is installed allow incoming connections through port 8080 and for application node.exe.
4. In Windows, open **Services**. Check that the Kaspersky Security Center 13 Web Console service is running.
5. Check that you can access Kaspersky Security Center by using Administration Console.
6. In Windows, open **Event Viewer**, and then select **Applications and Services Logs** → **Kaspersky Event Log**. Make sure that the log does not contain errors.

See also:

Scenario: Installation and initial setup of Kaspersky Security Center 13 Web Console[962](#)

Installation of Kaspersky Security Center 13 Web Console on Linux platforms

This section describes features applicable only to Kaspersky Security Center 11.1 Web Console or a later version.

This section explains how to install Kaspersky Security Center 13 Web Console Server (also referred to as Kaspersky Security Center 13 Web Console) on devices running the Linux operating system (see the list of supported Linux distributions (see section "Hardware and software requirements for Kaspersky Security Center 13 Web Console" on page [955](#))).

In this chapter

Installing Kaspersky Security Center 13 Web Console on Linux platforms	969
Kaspersky Security Center 13 Web Console installation parameters	970

Installing Kaspersky Security Center 13 Web Console on Linux platforms

This section describes features applicable only to Kaspersky Security Center 11.1 Web Console or a later version.

This section describes how to install Kaspersky Security Center 13 Web Console Server (also referred to as Kaspersky Security Center 13 Web Console) on devices running the Linux operating system. Before installation, you must install a database management system (see section "Installing a database management system" on page [964](#)) and the Kaspersky Security Center (see section "Installing Kaspersky Security Center (Standard installation)" on page [966](#)) Administration Server.

Use the installation file—ksc-web-console-[version_number].deb or ksc-web-console-[version_number].x86_64.rpm—that corresponds to the Linux distribution installed on your device. You receive the installation file by downloading it from the Kaspersky website.

► To install Kaspersky Security Center 13 Web Console:

1. Make sure that the device on which you want to install Kaspersky Security Center 13 Web Console is running one of the supported Linux distributions (see section "Hardware and software requirements for Kaspersky Security Center 13 Web Console" on page [955](#)).
2. Read the End User License Agreement (EULA) that you downloaded together with the installation file. If you do not accept the terms of the License Agreement, do not install the application.
3. Create a response file (see section "Kaspersky Security Center 13 Web Console installation parameters" on page [970](#)) that contains parameters for connecting Kaspersky Security Center 13 Web Console to the Administration Server. Name this file ksc-web-console-setup.json and place it in the following directory: /etc/ksc-web-console-setup.json.

Example of a response file containing the minimal set of parameters and the default address and port:

```
{  
  "address": "127.0.0.1",  
  "port": 8080,  
  "trusted": "",  
  "acceptEula": true  
}
```

When you install Kaspersky Security Center 13 Web Console on the Linux ALT operating system, you must specify a port number other than 8080, because port 8080 is used by the operating system.

Kaspersky Security Center 13 Web Console cannot be updated by using the same .rpm installation file. If you want to change settings in a response file and use this file to reinstall the application, you must first remove the application, and then install it again with the new response file.

4. Under an account with root privileges, use the command line to run the setup file with the .deb or .rpm extension, depending on your Linux distribution.

- To install or upgrade Kaspersky Security Center 13 Web Console from a .deb file, run the following command:

```
$ sudo dpkg -i ksc-web-console-[version_number].deb
```

- To install Kaspersky Security Center 13 Web Console from an .rpm file, run the following command:

```
$ sudo rpm -ivh --nodeps ksc-web-console-  
[version_number].x86_64.rpm
```

To upgrade from a previous version of Kaspersky Security Center Web Console, run the following command:

```
$ sudo rpm -Uvh --nodeps --nopreun --force ksc-web-console-  
[version_number].x86_64.rpm
```

This starts unpacking of the setup file. Please wait until the installation is complete. Kaspersky Security Center 13 Web Console is installed to the following directory: `/var/opt/kaspersky/ksc-web-console`.

When the installation is complete, you can use your browser to open and log in to Kaspersky Security Center 13 Web Console (see section "Logging in to Kaspersky Security Center 13 Web Console and logging out" on page [991](#)).

Kaspersky Security Center 13 Web Console installation parameters

This section describes features applicable only to Kaspersky Security Center 11.1 Web Console or a later version.

For installing Kaspersky Security Center 13 Web Console Server on devices running Linux (see section "Installing Kaspersky Security Center 13 Web Console on Linux platforms" on page [969](#)), you must create a response file—a .json file that contains parameters for connecting Kaspersky Security Center 13 Web Console to the Administration Server.

Here is an example of a response file containing the minimal set of parameters and the default address and port:

```
{  
  "address": "127.0.0.1",  
  "port": 8080,  
  "trusted": "",  
  "acceptEula": true  
}
```

When you install Kaspersky Security Center 13 Web Console on Linux ALT operating system, you must specify a port number other than 8080, because port 8080 is used by the operating system.

The table below describes the parameters that can be specified in a response file.

Table 79. Parameters for installing Kaspersky Security Center 13 Web Console on devices running

Parameter	Description	Available values
address	Address of Kaspersky Security Center 13 Web Console Server (required).	String value.
port	Number of port that Kaspersky Security Center 13 Web Console Server uses to connect to the Administration Server (required).	Numerical value.
defaultLangId	Language of user interface (by default, 1033).	Numerical code of the language: <ul style="list-style-type: none"> • de-DE: 1031 • en-US: 1033 • es-ES: 3082 • es-MX: 2058 • fr-FR: 1036 • ja-JP: 1041 • kk-KZ: 1087 • pl-PL: 1045 • pt-BR: 1046 • ru-RU: 1049 • tr-TR: 1055 • zh-Hans: 4 • zh-Hant: 31748 If no value is specified, then English (en-US) language is used.
enableLog	Whether or not to enable Kaspersky Security Center 13 Web Console activity logging (on page 1368).	true—Logging is enabled (selected by default). false—Logging is disabled.
trusted	List of trusted Administration Servers allowed to connect to Kaspersky Security Center 13 Web Console. Each Administration Server must be defined with the following parameters: <ul style="list-style-type: none"> • Administration Server address • OpenAPI port that is used by Kaspersky Security Center 13 Web Console to connect to the Administration Server (by default, 13299) • Path to the certificate of the Administration Server • Administration Server name that will be displayed in the login window The parameters are separated with vertical bars. If several Administration Servers are specified, separate them with two vertical bars (pipes).	String value of the following format: "server address port certificate path server name". Example: "X.X.X.X 13299 /cert/server-1.cer Server 1 Y.Y.Y.Y 13299 /cert/server-2.cer Server 2".

Parameter	Description	Available values
<code>acceptEula</code>	Whether or not you want to accept the terms of the End User License Agreement (see section "About the End User License Agreement" on page 318) (EULA). The file containing the terms of the EULA is downloaded together with the installation file.	<code>true</code> —I have fully read, understand and accept the terms of the End User License Agreement (see section "About the End User License Agreement" on page 318). <code>false</code> —I do not accept the terms of the License Agreement (selected by default).
<code>certDomain</code>	If you want to generate a new certificate, use this parameter to specify the domain name for which a new certificate is to be generated.	String value.
<code>certPath</code>	If you want to use an existing certificate, use this parameter to specify the path to the certificate file.	String value.
<code>keyPath</code>	If you want to use an existing certificate, use this parameter to specify path to the key file.	String value.
<code>webConsoleAccount</code>	Name of the non-privileged account for working with Kaspersky Security Center 13 Web Console.	String value of the following format: "group name:user name". Example: "Group1:User1". If no value is specified, a new account is created.
<code>managementServiceAccount</code>	Name of the privileged account for working with Kaspersky Security Center 13 Web Console.	String value of the following format: "group name:user name". Example: "Group1:User1". If no value is specified, a new account is created.

See also:

Ports used by Kaspersky Security Center[65](#)

Upgrading Kaspersky Security Center Web Console

If you want to use a newer version of Kaspersky Security Center Web Console without removing your currently installed instance, you can use the standard upgrade procedure provided in the Kaspersky Security Center Web Console installer.

► *To upgrade Kaspersky Security Center Web Console:*

1. Under an account with administrator rights, run the KSCWebConsoleInstaller.<build number>.exe executable file, where <build number> stands for a Kaspersky Security Center Web Console build whose number is higher than that of your currently installed instance.
2. In the Setup Wizard window that opens, select a language, and then click **OK**.
3. In the welcome window, select the **Upgrade** option, and then click **Next**.
4. In the **License Agreement** window, read and accept the terms of the End User License Agreement. The installation continues after you accept the EULA; otherwise, the **Next** button is unavailable.
5. Progress through the steps of the Setup Wizard until you finish the installation. When progressing, you can also modify the Kaspersky Security Center Web Console settings that you specified during the previous installation (see section "Installing Kaspersky Security Center 13 Web Console" on page [967](#)). When you reach the **Ready for Kaspersky Security Center 13 Web Console modification** step, click the **Upgrade** button. Wait until the new settings are applied and on the next step of the Setup Wizard, click **Finish**. You can also click the **Start Kaspersky Security Center 13 Web Console in your browser** link to start the upgraded instance of Kaspersky Security Center Web Console immediately.

Modifying the Kaspersky Security Center Web Console settings during the upgrade is only available in Kaspersky Security Center Web Console version 12.2 or higher.

Your Kaspersky Security Center Web Console instance is upgraded.

Specifying certificates for trusted Administration Servers

The existing Administration Server certificate is automatically replaced with a new one before the certificate expiration date. You can also replace the existing Administration Server certificate with a custom one. Every time the certificate is changed, the new certificate must be specified in the settings of Kaspersky Security Center 13 Web Console. Otherwise, Kaspersky Security Center 13 Web Console will not be able to connect to the Administration Server.

If Kaspersky Security Center 13 Web Console and the Administration Server are installed on the same device, Kaspersky Security Center 13 Web Console receives the new certificate automatically. If Kaspersky Security Center 13 Web Console is installed on a different device, you must specify the local path to the new Administration Server certificate.

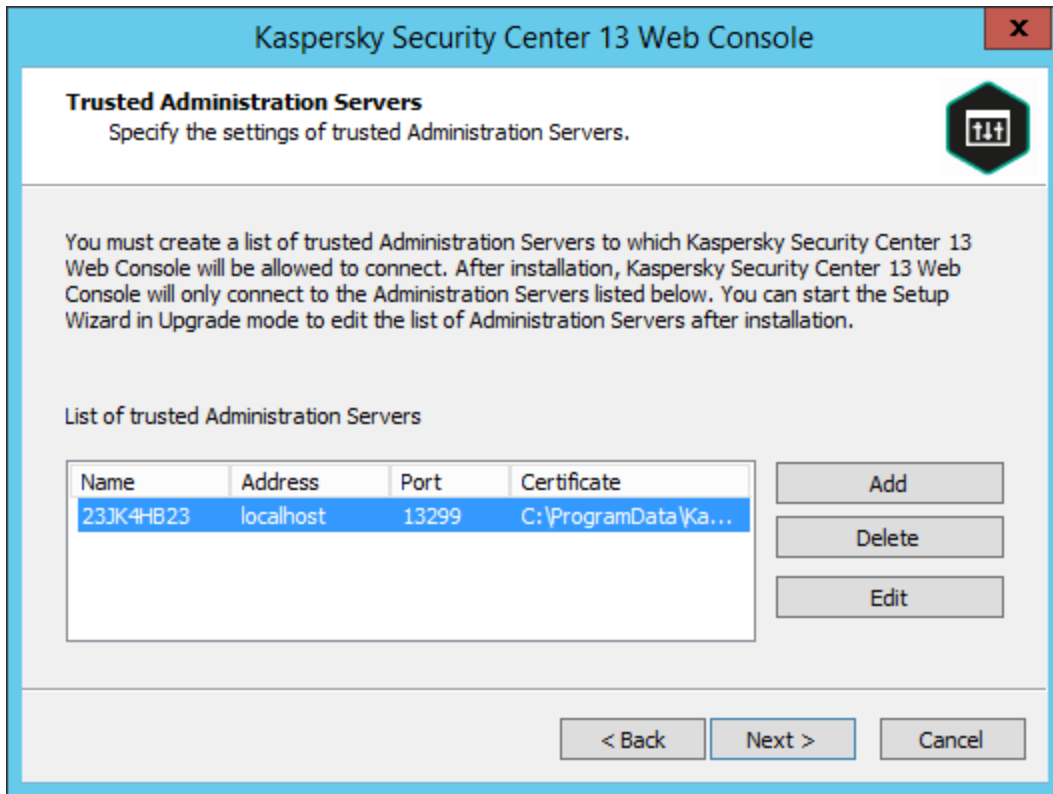
► *To specify a new certificate for the Administration Server:*

1. On the device where the Administration Server is installed, copy the certificate file, for example, to a mass storage device.

By default, the certificate file is stored in the ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert folder.
2. On the device where Kaspersky Security Center 13 Web Console is installed, place the certificate file in a local folder.
3. Run the KSCWebConsoleInstaller.<build number>.exe executable file under an account with administrative privileges.

This starts the Setup Wizard.
4. On the first page of the Wizard, select the **Upgrade** option.

- On the **Modification type** page, select the **Edit connection settings** option.
- On the **Trusted Administration Servers** page, select the required Administration Server and click the **Edit** button.



- On the page that opens, click the **Browse** button and specify the path to the new certificate file.
- On the last page of the Wizard, click **Modify** to apply the new settings.
- After the application reconfiguration successfully completes, click the **Finish** button.
- Log in (see section "Logging in to Kaspersky Security Center 13 Web Console and logging out" on page [991](#)) to Kaspersky Security Center 13 Web Console.

Kaspersky Security Center 13 Web Console works with the specified certificate.

See also:

Administration Server certificate [604](#)

Replacing certificate for Kaspersky Security Center 13 Web Console

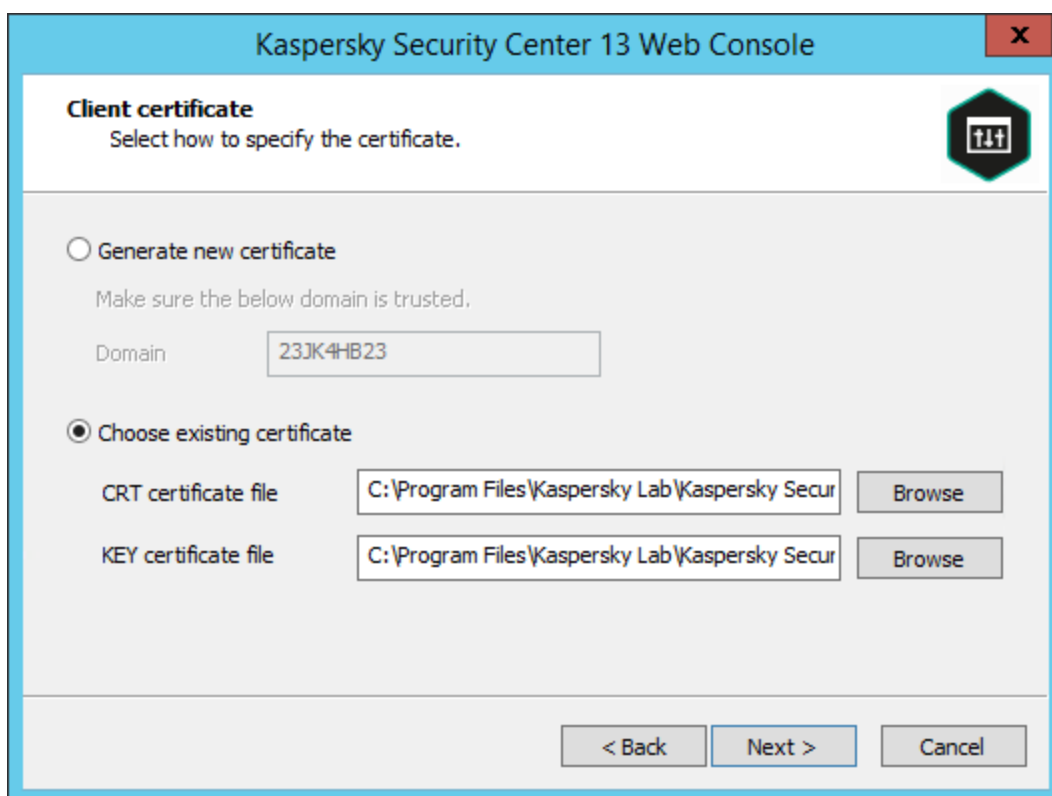
By default, when you install Kaspersky Security Center 13 Web Console Server (also referred to as Kaspersky Security Center 13 Web Console), a browser certificate for the application is generated automatically. You can replace the automatically generated certificate with a custom one.

► To replace the certificate for Kaspersky Security Center 13 Web Console with a custom one:

1. On the device where Kaspersky Security Center 13 Web Console is installed, run the KSCWebConsoleInstaller.12.0.<build number>.exe executable file under an account with administrative privileges.

This starts the Setup Wizard.

2. On the first page of the Wizard, select the **Upgrade** option.
3. On the **Modification type** page, select the **Edit connection settings** option.
4. On the **Client certificate** page, select the **Choose existing certificate** option and specify the path to the custom certificate.



5. On the last page of the Wizard, click **Modify** to apply the new settings.
6. After the application reconfiguration successfully completes, click the **Finish** button.

Kaspersky Security Center 13 Web Console works with the specified certificate.

Converting a PFX certificate to the PEM format

To use a PFX certificate in Kaspersky Security Center 13 Web Console, you must first convert it to the PEM format by using any convenient OpenSSL-based cross-platform utility (for more information, refer to the OpenSSL website).

► To convert a PFX certificate to the PEM format in Windows operating system:

1. In an OpenSSL-based cross-platform utility, execute the following commands:

```
openssl pkcs12 -in <filename.pfx> -clcerts -nokeys -out certificate.crt
```

```
openssl pkcs12 -in <filename.pfx> -nocerts -nodes -out private.key
```

2. Make sure that the certificate file and the private key are generated to the same folder where the .pfx file is stored.
3. If the certificate file or the private key contains the bag attributes, delete these attributes using any convenient text editing software and save the file.

The certificate file in PEM format and the private key file are ready to use, so you can specify them in the Kaspersky Security Center 13 Web Console installer.

► *To convert a PFX certificate to the PEM format in Linux operating system:*

1. In an OpenSSL-based cross-platform utility execute the following commands:

```
openssl pkcs12 -in <filename.pfx> -nocerts -nodes | sed -ne '/-BEGIN PRIVATE KEY-/,/-END PRIVATE KEY-/p' > private.key
```

```
openssl pkcs12 -in <filename.pfx> -clcerts -nokeys | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > certificate.crt
```

2. Make sure that the certificate file and the private key are generated to the same directory where the .pfx file is stored.

The certificate file in PEM format and the private key file are ready to use, so you can specify them in the Kaspersky Security Center 13 Web Console installer.

Reissuing the certificate for Kaspersky Security Center Web Console

This feature is only available in Kaspersky Security Center Web Console version 12.2 or higher.

Most web browsers impose a limit on the validity term of a certificate. To fall within this limit, the validity term of the Kaspersky Security Center Web Console certificate is limited to 397 days. You can replace an existing certificate received from a certification authority (CA) by issuing a new self-signed certificate manually. Alternatively, you can reissue your expired Kaspersky Security Center Web Console certificate.

If you already use a self-signed certificate, you can also reissue it by upgrading Kaspersky Security Center Web Console through the standard procedure in the installer (**Upgrade** option).

► *To issue a new certificate when you install Kaspersky Security Center Web Console for the first time:*

1. Run the routine installation of Kaspersky Security Center Web Console (see section "Installing Kaspersky Security Center 13 Web Console" on page [967](#)).
2. When you reach the **Client certificate** step of the Setup Wizard, select the **Generate new certificate** option, and then click the **Next** button.
3. Progress through the remaining steps of the Setup Wizard until you finish the installation.

A new certificate for Kaspersky Security Center Web Console is issued with a validity term of 397 days.

► *To reissue the expired Kaspersky Security Center Web Console certificate:*

1. Under an account with administrator rights, run the KSCWebConsoleInstaller.<build number>.exe executable file.
2. In the Setup Wizard window that opens, select a language, and then click **OK**.
3. In the welcome window, select the **Reissue certificate** option, and then click **Next**.
4. On the next step, wait until the reconfiguration of Kaspersky Security Center Web Console is complete, and then click **Finish**.

The Kaspersky Security Center Web Console certificate is reissued for another validity term of 397 days.



Migration to Kaspersky Security Center Cloud Console

This section describes the process of migration from Kaspersky Security Center 13 Web Console running on-premises to Kaspersky Security Center Cloud Console.

In this chapter

Methods of migration to Kaspersky Security Center Cloud Console	980
Scenario: Migration without a hierarchy of Administration Servers	981
Migration with a hierarchy of Administration Servers	987

Methods of migration to Kaspersky Security Center Cloud Console

This section provides information about the methods available for migration from Kaspersky Security Center running on-premises to Kaspersky Security Center Cloud Console.

By using the migration feature, you can transfer your networked devices from Kaspersky Security Center, under management by Kaspersky Security Center Cloud Console. Your managed devices will be switched without losing the principal settings, such as membership in administration groups; as well as the essential objects, such as policies and tasks related to the managed applications.

Migration to Kaspersky Security Center Cloud Console through the Migration Wizard is only applicable to managed devices running Windows operating systems. If you want to migrate managed devices running Linux or macOS operating systems, you must follow additional steps.

You can choose either of the two available methods to migrate your Administration Servers to Kaspersky Security Center Cloud Console:

- Migration without a hierarchy of Administration Servers (see section "Scenario: Migration without a hierarchy of Administration Servers" on page [981](#)):
 - Enables transfer of managed devices and related objects to Kaspersky Security Center Cloud Console, even if the Administration Server running on-premises is not a secondary in regard to Kaspersky Security Center Cloud Console.
 - May require transfer of files (on a removable drive, by email, through shared folders, or in any other convenient way) if Kaspersky Security Center Web Console and Kaspersky Security Center Cloud Console are opened on different physical devices.
- Migration using a hierarchy of Administration Servers:
 - Enables transfer of managed devices and related objects to Kaspersky Security Center Cloud Console by using only the interface of Kaspersky Security Center Cloud Console, so no physical transfer of files is needed.
 - Requires that the Administration Server running on-premises act as secondary to Kaspersky Security Center Cloud Console. You can create such a hierarchy, before starting the migration.

Scenario: Migration without a hierarchy of Administration Servers

This section describes the migration of the managed devices and related objects from Kaspersky Security Center Web Console running on-premises to Kaspersky Security Center Cloud Console. You can include a single administration group in the migration scope to restore the same administration group in Kaspersky Security Center Cloud Console.

After you finish the migration, all Network Agents within the migration scope are upgraded and managed by the Administration Server running in Kaspersky Security Center Cloud Console.

The steps listed in this section cover the migration process performed when no hierarchy of Administration Servers exists, that is, no connection has been established between Kaspersky Security Center Cloud Console and Kaspersky Security Center Web Console running on-premises.

Prerequisites

Before you start, make sure that the following prerequisites are met:

- Administration Server running on-premises is upgraded to version 13.
- Kaspersky Security Center Web Console is installed.
- Network Agent on managed devices is upgraded to version 10 Service Pack 3 or later.
- The web plug-ins for the applications that you intend to manage through Kaspersky Security Center Cloud Console are installed.
- The managed applications are upgraded to versions supported by Kaspersky Security Center Cloud Console (see section "List of supported Kaspersky applications" on page [41](#)).
- The managed applications are uninstalled from managed devices, if these applications are not supported by Kaspersky Security Center Cloud Console, and replaced with supported applications, if necessary.
- All the data (disk-level or file-level) that were encrypted by Kaspersky Endpoint Security for Windows on managed devices are decrypted; the encryption feature is disabled on the managed devices through the application policy or locally.

If a managed device still stores any files or folders encrypted through Kaspersky Endpoint Security for Windows, the Network Agent upgrade will be canceled during the migration process. A notification will prompt you to decrypt all data on the device and disable the encryption feature.

Kaspersky Security Center Cloud Console provides for a maximum of 10,000 managed devices per one Administration Server.

Migration stages

Migration to Kaspersky Security Center Cloud Console comprises the following stages:

a. Planning the migration scope and checking the prerequisites

Estimate the scope of the migration process, that is, the administration group to export, and assess the number of managed devices in it. Also, make sure that all the activities listed as migration prerequisites have been completed successfully.

b. Exporting managed devices, objects, and settings from Kaspersky Security Center Web Console

Use the Migration Wizard of Kaspersky Security Center Web Console running on-premises to export your managed devices together with group objects (see section "Step 1. Exporting managed devices, objects, and settings from Kaspersky Security Center Web Console" on page [983](#)).

The maximum export file size is 4 GB.

c. Importing the export file to Kaspersky Security Center Cloud Console

Transfer the information about your managed devices and objects to Kaspersky Security Center Cloud Console running in your workspace. For this purpose, use the Migration Wizard of Kaspersky Security Center Cloud Console to import the export file and create a Network Agent stand-alone installation package.

d. Re-installing Network Agent on managed devices

Go back to the Migration Wizard in Kaspersky Security Center Web Console running on-premises to create a remote installation task. You will be able to use this task (immediately or later) to re-install Network Agent on your managed devices and switch them under management of Kaspersky Security Center Cloud Console, thus completing the migration process.

To re-install Network Agent on managed devices running Linux or macOS, uninstall Network Agent on these devices before running the remote installation task.

Results

Upon finishing with the migration, you can make sure that migration was successful:

- Network Agent is re-installed on all managed devices.
- All devices are managed through Kaspersky Security Center Cloud Console.
- All object settings that were effective before migration are preserved.

See also:

About Kaspersky Security Center Cloud Console	43
Step 1. Exporting managed devices, objects, and settings from Kaspersky Security Center Web Console	983
Step 2. Importing the export file to Kaspersky Security Center Cloud Console	984
Step 3. Re-installing Network Agent on devices managed through Kaspersky Security Center Cloud Console	986

Step 1. Exporting managed devices, objects, and settings from Kaspersky Security Center Web Console

Migration of managed devices from Kaspersky Security Center Web Console to Kaspersky Security Center Cloud Console requires that you first create an export file containing information about the hierarchy of administration groups that are on your current Administration Server running on-premises. The export file must also contain information about the objects and their settings. This export file will be used for subsequent import to Kaspersky Security Center Cloud Console.

The maximum export file size is 4 GB.

► *To export objects and their settings from Kaspersky Security Center Web Console:*

1. In the main application window of Kaspersky Security Center Web Console running on-premises, click **OPERATIONS** → **MIGRATION**. The welcome page of the Migration Wizard opens.
2. On the welcome page of the Migration Wizard, click **Next**. The **Select administration group to export (all subgroups will also be exported)** page opens, displaying the entire hierarchy of administration groups of the corresponding Administration Server.
3. On the **Select administration group to export (all subgroups will also be exported)** page, click the chevron icon (➤) next to the **Managed devices** group name to expand the hierarchy of administration groups. Select the administration group that you want to export.
4. Select the managed applications whose policies and tasks must be transferred to Kaspersky Security Center Cloud Console together with group objects. To select the managed applications whose objects are to be exported, select the check boxes next to their names in the list.

Although Kaspersky Security Center 13 Administration Server is present on the list, selecting the corresponding check box does not result in the export of its policies.

To make sure that your managed applications are supported by Kaspersky Security Center Cloud Console, click the corresponding link. It will redirect you to the Online Help topic containing the list of applications managed by Kaspersky Security Center Cloud Console.

If you select applications that are not supported by Kaspersky Security Center Cloud Console, the policies and tasks of these applications will be exported anyway and then imported, but you will not be able to manage them in Kaspersky Security Center Cloud Console due to unavailability of the dedicated plug-ins.

5. View the list of group objects exported by default and specify non-group objects to be exported together with the selected administration group, if necessary. Configure the export scope by including or excluding various objects, such as global tasks (see section "About tasks" on page [1078](#)), custom device selections, reports, custom roles, internal users and security groups, and custom application categories. This page includes the following sections:
 - Global tasks
 - Device selections
 - Reports

- Group objects

The Migration Wizard checks the total number of managed devices included in the selected administration group. If this number exceeds 10 000, the error message appears. The **Next** button remains unavailable (dimmed) until the number of managed devices in the selected administration group falls within the limit.

6. After you defined the migration scope, click **Next** to start the export process. The **Creating the export file** page opens on which you can view the export progress for each type of object that you included in the migration scope. Wait until the refresh icons (🔄) next to all items in the list of objects are replaced with green check marks (✓). The export process finishes and the export file is automatically downloaded to the default download location defined in your browser settings. The name of the export file appears in the lower part of the browser window.
7. When the **Export has completed successfully** page is displayed, proceed to the next stage performed in Kaspersky Security Center Cloud Console.

If you use Kaspersky Security Center Web Console and Kaspersky Security Center Cloud Console on different devices, you will have to copy the export file to a removable drive or choose other ways of transferring the file.

See also:

About Kaspersky Security Center Cloud Console [43](#)

Step 2. Importing the export file to Kaspersky Security Center Cloud Console

To transfer information about managed devices, objects, and their settings that you exported from Kaspersky Security Center Web Console, you must import it to Kaspersky Security Center Cloud Console deployed in your workspace. This allows you to create a stand-alone installation package and use it for re-installation of Network Agent on your managed devices.

Before you start the Migration Wizard in Kaspersky Security Center Cloud Console, make sure its current localization language is the same as the Kaspersky Security Center Web Console language during the export process. Switch the language, if necessary.

If you have previously completed the Quick Start Wizard in your Kaspersky Security Center Cloud Console workspace, the **Managed devices** group includes policies and tasks created with the default settings. Delete these policies and tasks before importing the ones that you exported from Kaspersky Security Center Web Console.

► *To import the export file to Kaspersky Security Center Cloud Console:*

1. Proceed to Kaspersky Security Center Cloud Console and click **OPERATIONS** → **MIGRATION**. The welcome page of the Migration Wizard opens.

2. On the welcome page of the Migration Wizard, click **Import**. In the File Explorer window that opens, select the export file by browsing to the folder where it was saved, and click **Open**. Wait until the refresh icon (🔄) next to the file uploading status is replaced with the green check mark (✓).
3. Click **Next**. The next page opens, displaying the entire hierarchy of administration groups of the Administration Server in Kaspersky Security Center Cloud Console.
4. Select the check box next to the target administration group to which the group objects must be restored and click **Next**. The Migration Wizard displays a list of Network Agent installation packages available in Kaspersky Security Center Cloud Console.
5. Select the installation package (see section "Downloading and creating installation packages for Kaspersky applications" on page [1025](#)) containing the relevant version and localization of Network Agent and click **Next**.

Select the Kaspersky Network Agent for Windows installation package only if you have previously completed the Quick Start Wizard in your Kaspersky Security Center Cloud Console workspace.

Wait until the Migration Wizard creates a stand-alone installation package.

The maximum file size of the stand-alone installation package for Network Agent is 200 MB.

6. The file is unpacked; the non-group objects and the group objects are restored to the target administration group.

If the name of the object that you restore is identical to the name of an existing object, an incremental suffix is added to the restored object.

When the import completes, the exported structure of administration groups, including the details of devices, appears under the target administration group that you selected.

If you have imported the entire **Managed devices** group, we recommend that you rename the newly imported subgroup to avoid confusion:

- a. Go to the **HIERARCHY OF GROUPS** section.
- b. Click the name of the subgroup in the groups tree.
- c. In the properties window that opens, in the **Name** field enter a different name (for example, "Migrated devices").

We recommend that you check whether the objects (policies, tasks, and managed devices) included in the export scope have been successfully imported to Kaspersky Security Center Cloud Console. To do this, go to the **DEVICES** section and view whether the imported objects appear on the lists in the **POLICIES & PROFILES**, **TASKS**, and **MANAGED DEVICES** subsections.

You will not be able to minimize the Migration Wizard and perform any concurrent operations during the import. Wait until the refresh icons (🔄) next to all items in the list of objects are replaced with green check marks (✓) and the import finishes. After this, the devices start switching to Kaspersky Security Center Cloud Console.

7. Click **Finish** to close the Migration Wizard window.

8. Go to **DISCOVERY & DEPLOYMENT** → **DEPLOYMENT & ASSIGNMENT** → **INSTALLATION PACKAGES** and click the **View the list of stand-alone packages** button. In the list that opens, select the stand-alone installation package that you have created and click the **Download** button. The stand-alone installation package is automatically downloaded to the default download location defined in your browser settings.

If you use Kaspersky Security Center Web Console and Kaspersky Security Center Cloud Console on different devices, you must copy the stand-alone installation package to a removable drive or choose other ways of transferring the file.

See also:

About Kaspersky Security Center Cloud Console [43](#)

Step 3. Re-installing Network Agent on devices managed through Kaspersky Security Center Cloud Console

After you create the Network Agent stand-alone installation package, you can proceed to creation of a remote installation task. Performing this task allows you to re-install Network Agent on all managed devices so that these devices are switched under management through Kaspersky Security Center Cloud Console.

To reduce the risk of data loss, we recommend that you first perform the actions for a small administration group counting up to 20 managed devices located within the corporate network and including no physical servers. After finishing with these actions, check whether re-installation completed successfully and proceed to the full re-installation scope.

► To create a remote installation task and re-install Network Agent:

1. Go back to the Migration Wizard in Kaspersky Security Center Web Console running on-premises. Depending on the current state of the Migration Wizard, you can do one of the following:
 - If you have not closed the Migration Wizard after the export and your session has not expired, click the **Go to Step 3 of the Migration Wizard** button. Select the **Upload stand-alone installation package** check box and click the **Select stand-alone installation package** button. In the browser window that opens, specify the Network Agent stand-alone installation package.
 - If you have to start the Migration Wizard again for any reason, select the **Upload stand-alone installation package** check box and click the **Select stand-alone installation package** button. In the browser window that opens, specify the Network Agent stand-alone installation package. After that, the Migration Wizard again displays the hierarchy of administration groups of this Administration Server. Select the same group for which you created the export file and click **Next**.

The Migration Wizard checks again the total number of managed devices included in the selected administration group. If this number exceeds 10 000, you get the error message. The **Next** button remains unavailable (dimmed) until the number of managed devices in the selected administration group falls within the limit.

2. Wait until the stand-alone installation package is uploaded and click **Next**. The Migration Wizard creates a custom installation package and a remote installation task for it. The task scope will include the administration group that you selected on the **Select administration group to export (all subgroups will also be exported)** page; the task startup schedule will be set to **Manually** by default. The Migration Wizard displays the creation progress. Wait until the refresh icons (🔄) are replaced with the green check marks (✓) and click **Next**.
3. If necessary, select the **Run newly created remote installation task** check box (cleared by default) for the devices in the selected administration group of the Administration Server running on-premises and all of its subgroups. In this case, the devices will be switched under management of Kaspersky Security Center Cloud Console—but only after Network Agent installation completes. The full path will be displayed to the administration group in which the task will be run.

The task must only be started after the import to Kaspersky Security Center Cloud Console finishes. Otherwise, the device names may be duplicated in the list.

4. Click **Finish** to close the Migration Wizard and start the remote installation task for the following purposes:
 - Upgrading the Network Agent instances
 - Switching the Network Agent instances under management through Kaspersky Security Center Cloud Console

If you have left the **Run newly created remote installation task** check box cleared, you can start the task later manually, if necessary.

You can check whether the Network Agent instances from your migration scope have been switched under management through Kaspersky Security Center Cloud Console. To do this, connect to any migrated device, open the command prompt as administrator, and run the `klagchk.exe` utility with the `-sendhb` parameter. Make sure Network Agent has successfully connected to your Kaspersky Security Center Cloud Console workspace: the Administration Server address and connection port number have been received from Hosted Discovery Service, and Network Agent does not use port 13000 to connect to Administration Server in the workspace. If Network Agent has failed to connect to Administration Server in the workspace, make sure the ports used by Kaspersky Security Center Cloud Console (see section "Ports used by Kaspersky Security Center" on page 65) are allowed to access from your network.

See also:

- About Kaspersky Security Center Cloud Console43
- Manually checking the connection between a client device and the Administration Server. Klagchk utility643

Migration with a hierarchy of Administration Servers

This section describes the migration of the managed devices and related objects from Kaspersky Security Center Web Console running on-premises to Kaspersky Security Center Cloud Console. The process involves a hierarchy: Kaspersky Security Center Web Console running on-premises acts as the secondary Administration Server and Kaspersky Security Center Cloud Console acts as the primary Administration Server.

After you finish the migration, all Network Agents in the group within the migration scope are upgraded and managed through Kaspersky Security Center Cloud Console.

Before you start the migration process, make sure that the following prerequisites are met:

- The Administration Servers are combined into a hierarchy: Kaspersky Security Center Web Console running on-premises as the secondary Administration Server and Kaspersky Security Center Cloud Console as the primary Administration Server.
- Kaspersky Security Center Web Console running on-premises is upgraded to version 12 or a later version.
- Network Agent on managed devices is upgraded to version 10 Service Pack 3 or a later version.
- The managed applications are upgraded to versions supported by Kaspersky Security Center Cloud Console (see section "List of supported Kaspersky applications" on page [41](#)).
- The managed applications are uninstalled from managed devices, if these applications are not supported by Kaspersky Security Center Cloud Console, and replaced with supported applications, if necessary.

Kaspersky Security Center Cloud Console provides for a maximum of 10,000 managed devices per one Administration Server.

► *To perform migration to Kaspersky Security Center Cloud Console:*

1. Estimate the scope of the migration process, that is, the administration group to export, and assess the number of managed devices in it. Also, make sure that all of the activities listed as migration prerequisites have been completed successfully.
2. In the main application window of Kaspersky Security Center Cloud Console, click **OPERATIONS** → **MIGRATION**. The welcome page of the Migration Wizard opens.
3. On the welcome page of the Migration Wizard, click **Next**. The **Select administration group to export (all subgroups will also be exported)** page opens, displaying the entire hierarchy of administration groups of the secondary Administration Server.
4. On the **Select administration group to export (all subgroups will also be exported)** page, click the chevron icon (➤) next to the **Managed devices** group name and expand the hierarchy of administration groups. Select the administration group that you want to export.

The Migration Wizard checks the total number of managed devices included in the selected administration group. If this number exceeds 10,000, you get an error message. The **Next** button remains unavailable (dimmed) until the number of managed devices in the selected administration group falls within the limit.

5. Select the managed applications whose policies and tasks must be transferred to Kaspersky Security Center Cloud Console together with group objects. To select the managed applications whose objects are to be exported, select the check boxes next to their names in the list.

Although Kaspersky Security Center Administration Server is present on the list, selecting the corresponding check box does not result in the export of its policies.

To make sure that your managed applications are supported by Kaspersky Security Center Cloud Console, click the corresponding link. It will redirect you to the Online Help topic containing the list of applications managed by Kaspersky Security Center Cloud Console.

If you select applications that are not supported by Kaspersky Security Center Cloud Console, the policies and tasks of these applications will be migrated anyway, but you will not be able to manage them in Kaspersky Security Center Cloud Console, due to unavailability of the dedicated plug-ins.

6. View the list of group objects exported by default. You can also specify non-group objects to be exported together with the selected administration group, if necessary, such as global tasks (see section "About tasks" on page [1078](#)), custom device selections, reports, custom roles, internal users and security groups, and custom application categories with content added manually. This page includes the following sections:
 - Global tasks
 - Device selections
 - Reports
 - Group objects
7. After you define the migration scope, click **Next** to start the export process. The **Creating the export file** page opens, on which you can view the export progress for each type of object that you included in the migration scope. Wait until each refresh icon (↻), located next to each item in the list of objects, is replaced with a green check mark (✓). The export finishes and the export file is automatically saved to a temporary folder. The next page opens, displaying the entire hierarchy of administration groups in Kaspersky Security Center Cloud Console, which acts as the primary Administration Server.
8. Select the check box next to the administration group to which the group objects must be imported, and then click **Next**. The file is unpacked, and the non-group objects and the group objects are restored to the target administration group.

If the name of the object that you restore is identical to the name of an existing object, the restored object has an incremental suffix added.

When the import completes, the exported structure of administration groups, including the details of devices, appears under the target administration group that you selected. The non-group objects are also imported.

You cannot minimize the Migration Wizard and perform any concurrent operations during the import. Wait until each refresh icon (↻), located next to each item in the list of objects, is replaced with a green check mark (✓) and the import finishes. After this, the devices start switching to Kaspersky Security Center Cloud Console.

9. After the import completes, the Migration Wizard displays a list of Network Agent installation packages (for Windows only) available in Kaspersky Security Center Cloud Console. Select the installation package containing the relevant version and localization of Network Agent, and then click **Next**.

Select the Kaspersky Network Agent for Windows installation package only if you have previously completed the Quick Start Wizard in your Kaspersky Security Center Cloud Console workspace.

If any previously created stand-alone installation packages exist for the installation package that you have selected, the Migration Wizard displays the list of these stand-alone installation packages and prompts you to select one of the following options:

- **Use existing stand-alone installation package.** If you select this option, the Migration Wizard uses the stand-alone installation package that you have selected from the list, instead of creating a new one.
- **Create stand-alone installation package.** If you select this option, the Migration Wizard creates a new stand-alone installation package, based on the installation package that you have selected.
- **Rebuild existing stand-alone installation package.** If you select this option, the Migration Wizard creates a new stand-alone installation package to replace the existing one displayed in the list.

10. Click **Next**.

The Migration Wizard creates a new stand-alone installation package (or uses an existing one) and a custom installation package based on it, as well as the corresponding remote installation task. The task scope includes the administration group that you selected on the **Select administration group to export (all subgroups will also be exported)** page. The task startup schedule is set on **Manually** by default. The Migration Wizard displays the creation progress.

11. Wait until each refresh icon (🔄) is replaced with a green check mark (✓), and then click **Next**.

12. If necessary, select the **Run newly created remote installation task** check box (cleared by default) for the devices in the selected administration group in Kaspersky Security Center Web Console running on-premises and all of its subgroups. In this case, the devices are switched under management through Kaspersky Security Center Cloud Console—but only after the Network Agent installation completes. The full path is displayed to the administration group in which the task is to be run.

The remote installation task must only be started after the import to Kaspersky Security Center Cloud Console finishes. Otherwise, the device names may be duplicated in the list.

13. Click **Finish** to close the Migration Wizard and start the remote installation task for the following purposes:

- Upgrading the Network Agent instances
- Switching the Network Agent instances under management through Kaspersky Security Center Cloud Console

If you have left the **Run remote installation task** check box cleared, you can start the task later manually, if necessary.

You can check whether the Network Agent instances from your migration scope have been switched under management through Kaspersky Security Center Cloud Console. To do this, connect to any migrated device, open the command prompt as administrator, and run the `klagchk.exe` utility with the `-sendhb` parameter. Make sure Network Agent has successfully connected to your Kaspersky Security Center Cloud Console workspace: the Administration Server address and connection port number have been received from Hosted Discovery Service, and Network Agent does not use port 13000 to connect to Administration Server in the workspace. If Network Agent has failed to connect to Administration Server in the workspace, make sure the ports used by Kaspersky Security Center Cloud Console (see section "Ports used by Kaspersky Security Center" on page 65) are allowed to access from your network. You can check the connection and obtain detailed information about the settings of the connection between a client device and Administration Server by using the `klagchk` utility.

When Network Agent is installed on a device, the `klagchk` utility is automatically copied to the Network Agent

installation folder.

When started from the command line, the `klnagchk` utility can perform the following actions (depending on the keys in use):

- Displays on the screen or logs the values of the settings used for connecting the Network Agent installed on the device to Administration Server.
- Records into an event log file Network Agent statistics (since its last startup) and utility operation results, or displays the information on the screen.
- Makes an attempt to establish connection between Network Agent and Administration Server.
If the connection attempt fails, the utility sends an ICMP packet to check the status of the device on which Administration Server is installed.

► *To check the connection between a client device and Administration Server using the `klnagchk` utility:*

On the device, start the `klnagchk` utility from the command line.

Utility command line syntax:

```
klnagchk [-logfile <file name>] [-sp] [-savecert <path to certificate file>] [-restart]
```

Descriptions of the keys:

- `-logfile <file name>` —Record in a log file the values of the settings of connection between Network Agent and Administration Server and the utility operation results.
By default, information is saved in the standard output stream (stdout). If the key is not in use, settings, results, and error messages are displayed on the screen.
- `-sp` —Show the password for the user's authentication on the proxy server.
The setting is in use if connection to the Administration Server is established through a proxy server.
- `-savecert <file name>` —Save the certificate, used to access the Administration Server, in the specified file.
- `-restart` —Restart Network Agent after the utility has completed.

Logging in to Kaspersky Security Center 13 Web Console and logging out

You can log in to Kaspersky Security Center 13 Web Console after you install the Administration Server and Web Console Server (see section "Installation" on page [964](#)). You must know the web address of the Administration Server and the port number specified during installation (see section "Installing Kaspersky Security Center 13 Web Console" on page [967](#)) (by default, the port is 8080). In your browser, JavaScript must be enabled.

► *To log in to Kaspersky Security Center 13 Web Console:*

1. In your browser, go to `<Administration Server web address>:<Port number>`.
The login page is displayed.

2. If you added several trusted servers, in the Administration Servers list select the Administration Server that you want to connect to.

If you only added one Administration Server, only the Login and Password fields are displayed.

3. Log in with the user name and password of the local Administrator.

If the Administration Server does not respond, or if you entered incorrect credentials, an error message is displayed.

4. After login, the dashboard is displayed, containing the language and theme that you used last time.

If you log in to Kaspersky Security Center 13 Web Console for the first time, a tutorial is displayed in the lower part of the screen. You can follow the instructions of the tutorial or close it by clicking the **Close** button (X).

You can navigate through Kaspersky Security Center 13 Web Console and use it to work with Kaspersky Security Center.

► *To log out of Kaspersky Security Center 13 Web Console:*

1. Click your user name in the upper-right corner of the screen.
2. In the drop-down menu, select **Sign out**.

Kaspersky Security Center 13 Web Console is closed, and the login page is displayed.

Configuring domain authentication by using the NTLM and Kerberos protocols

Kaspersky Security Center 13 enables you to use domain authentication in OpenAPI by using the NTLM and Kerberos protocols. Using domain authentication allows a Windows user to enable secure authentication in Kaspersky Security Center 13 Web Console without having to re-enter the password on the corporate network.

Domain authentication in OpenAPI over the Kerberos protocol has the following restrictions:

- The user of Kaspersky Security Center 13 Web Console must be authenticated in Active Directory by using the Kerberos protocol. The user must have a valid Kerberos Ticket Granting Ticket (also referred to as a TGT). A TGT is issued automatically when you authenticate to the domain.
- You must configure Kerberos authentication in the browser. For details, refer to the documentation of the browser you are using.

If you want to use domain authentication by using Kerberos protocols, your network must meet the following conditions:

- Administration Server must be run under the domain account name.
- You must specify the following information for the Administration Server account:
 - "KLKscSrv/<server.fqnd.name>", where <server> is the network name of the Administration Server device.
 - "KLKscSrv/<server>", where <server.fqnd.name> is the FQDN name of the Administration Server device.
- When connecting on the MMC-based Administration Console or Kaspersky Security Center Web Console, the server address must be specified exactly as the address for which the Service Principal Name (SPN) is registered. You can specify either <serverhost.find.name> or <serverhost>.

- For a password-free login, the browser process in which the Kaspersky Security Center Web Console is open as browser must run under a domain account.

Kerberos and NTLM protocols are only supported in OpenAPI for Kaspersky Security Center 13. They are not supported in OpenAPI for Kaspersky Security Center Linux.

Quick Start Wizard (Kaspersky Security Center 13 Web Console)

This section provides information about the Administration Server Quick Start Wizard.


Kaspersky Security Center allows you to adjust a minimum selection of settings required to build a centralized management system for protecting your network against security threats. This configuration is performed through the Quick Start Wizard. When the Wizard is running, you can make the following changes to the application:

- Add key files or enter activation codes that can be automatically distributed to devices within administration groups.
- Configure interaction with Kaspersky Security Network (KSN). If you have allowed the use of KSN, the Wizard enables the KSN Proxy Server service, which ensures connection between KSN and devices.
- Set up email delivery of notifications of events that occur during operation of Administration Server and managed applications (successful notification delivery requires that the Messenger service run on the Administration Server and all recipient devices).
- Create a protection policy for workstations and servers, as well as virus scan tasks, update download tasks, and data backup tasks, for the top level of the hierarchy of managed devices.

The Quick Start Wizard creates policies only for those applications whose **MANAGED DEVICES** folder does not contain policies. The Quick Start Wizard does not create tasks if tasks with the same names have already been created for the top level in the hierarchy of managed devices.

The application automatically prompts you to run the Quick Start Wizard after Administration Server installation, at the first connection to it. You can also start the Quick Start Wizard manually at any time.

► *To start the Quick Start Wizard manually:*

1. In the main application window, click the **Settings** icon () next to the name of the Administration Server. The Administration Server properties window opens.
2. On the **General** tab, select the **General** section.
3. Click **Start Quick Start Wizard**.

The Wizard prompts you to perform initial configuration of the Administration Server. Follow the instructions of the Wizard. Proceed through the Wizard by using the **Next** button.

See also:

Scenario: Installation and initial setup of Kaspersky Security Center 13 Web Console	962
Scenario: Kaspersky applications deployment through Kaspersky Security Center 13 Web Console ...	1023
Getting acquainted with Quick Start Wizard	994
Step 1. Specifying the Internet connection settings	994
Step 2. Downloading required updates	995
Step 3. Selecting the protection scopes and platforms.....	995
Step 4. Selecting encryption in solutions	996
Step 5. Configuring installation of plug-ins for managed applications	996
Step 6. Installing the selected plug-ins	997
Step 7. Downloading distribution packages and creating installation packages	997
Step 8. Configuring Kaspersky Security Network	997
Step 9. Selecting the application activation method	998
Step 10. Specifying the third-party update management settings	999
Step 11. Creating a basic network protection configuration	1000
Step 12. Configuring email notifications.....	1000
Step 13. Performing a network poll.....	1000
Step 14. Closing the Quick Start Wizard.....	1001

Getting acquainted with Quick Start Wizard

Read information about the actions that Quick Start Wizard performs.

Step 1. Specifying the Internet connection settings

Specify the Internet access settings for Kaspersky Security Center.

Select the **Use proxy server** check box if you want to use a proxy server when connecting to the Internet. If this check box is selected, the fields are available for entering settings. Specify the following settings for proxy server connection:

- **Address**
- **Port number**
- **Bypass proxy server for local addresses**

No proxy server will be used to connect to devices in the local network.

- **Proxy server authentication**

If this check box is selected, in the entry fields you can specify the credentials for proxy server authentication.

This entry field is available if the **Use proxy server** check box is selected.

- **User name** (this field is available if the **Proxy server authentication** check box is selected)

User account under which connection to the proxy server is established (this field is available if the **Proxy server authentication** check box is selected).

- **Password** (this field is available if the **Proxy server authentication** check box is selected)

Password set by the user under whose account the proxy server connection is established (this field is available if the **Proxy server authentication** check box is selected).

To see the entered password, click and hold the **Show** button for as long as you require.

Step 2. Downloading required updates

The required updates are downloaded from the Kaspersky servers automatically.

Step 3. Selecting the protection scopes and platforms

Select the protection scopes and platforms that are in use on your network. When you select these options, you specify the filters for application management plug-ins and distribution packages on Kaspersky servers that you can download to install on client devices on your network. Select the options:

- **Areas**

You can select the following protection scopes:

- **Workstations.** Select this option if you want to protect workstations in your network. By default, the Workstation option is selected.
- **File Servers and Storage.** Select this option if you want to protect file servers in your network.
- **Mobile devices.** Select this option if you want to protect mobile devices owned by the company or by the company employees. If you select this option but you have not provided a license with the Mobile Device Management feature (see section "Kaspersky Security Center licensing options" on page [320](#)), a message is displayed informing you about necessity to provide a license with the Mobile Device Management feature. If you do not provide a license, you cannot use the Mobile device feature.
- **Virtualization.** Select this option if you want to protect virtual machines in your network.
- **Kaspersky Anti-Spam.** Select this option if you want to protect mail servers in your organization from spam, fraud and malware delivery.

- **Operating systems**

You can select the following platforms:

- Microsoft Windows
- Linux
- macOS
- Android
- iOS

After you have selected protection scopes and platforms, management plug-ins and distribution packages for Kaspersky applications automatically start to download.

Step 4. Selecting encryption in solutions

The **Encryption in solutions** window is displayed only if you have selected **Workstations** as a protection scope and **Microsoft Windows** as a platform.

Kaspersky Endpoint Security for Windows includes encryption tool for the information stored on client devices. The managed application includes encryption tools that have the Advanced Encryption Standard (AES) implemented with 256-bit or 56-bit key length. Download and usage of the distribution package with 256-bit key length must be performed in compliance with applicable laws and regulations. To download a distribution package of Kaspersky Endpoint Security for Windows valid for the needs of your organization, consult the legislation of the country where the client devices of your organization are located. In the **Encryption in solutions** window, select one of the following encryption types:

- Strong encryption. This encryption type uses 256-bit key length.
- Lite encryption. This encryption type uses 56-bit bit key length.

Step 5. Configuring installation of plug-ins for managed applications

Select plug-ins for managed applications to install. A list of plug-ins located on Kaspersky servers is displayed. The list is filtered according to the options selected on the previous step of the Wizard. By default, a full list includes plug-ins of all languages. To display only plug-in of specific language, use filter. The list of plug-ins includes the following columns:

- **Name**

The plug-ins depending of the components and platforms that you have selected on the previous step are selected.

- **Version**

The list includes plug-ins of all the versions placed on Kaspersky servers. By default, the plug-ins of the latest versions are selected.

- **Language**

By default, the localization language of a plug-in is defined by the Kaspersky Security Center language that you have selected at installation. You can specify other languages in **Show the Administration Console localization language** or drop-down list.

After the plug-ins are selected, click **Next** to start installation.

Step 6. Installing the selected plug-ins

The Quick Start Wizard automatically installs the plug-ins that you selected in the previous step (see section "Step 5. Configuring installation of plug-ins for managed applications" on page [996](#)). To install some plug-ins, you must accept the terms of the EULA. Read the text of EULA displayed, select the **I agree to use Kaspersky Security Network** check box and click the **Install** button. If you do not accept the terms of the EULA, the plug-in is not installed.

When all the selected plug-ins are installed, the Quick Start Wizard automatically takes you to the next step.

Step 7. Downloading distribution packages and creating installation packages

Select the distribution packages to download.

Updates of managed applications may require a specific minimum version of Kaspersky Security Center to be installed.

After you have selected an encryption type for Kaspersky Endpoint Security for Windows, a list of distribution packages of both encryption types is displayed. A distribution package with the selected encryption type is selected in the list. You can select distribution packages of any encryption type. The distribution package language corresponds to the Kaspersky Security Center language. If a distribution package of Kaspersky Endpoint Security for Windows for the Kaspersky Security Center language does not exist, the English distribution package is selected.

To finish downloading of some distribution packages you must accept EULA. When you click the **Accept** button, the text of EULA is displayed. To proceed to the next step of the Wizard, you must accept the terms and conditions of the EULA and the terms and conditions of Kaspersky Privacy Policy. If you do not accept the terms and conditions, the downloading of the package is canceled.

After you have accepted the terms and conditions of the EULA and the terms and conditions of Kaspersky Privacy Policy, the downloading of the distribution packages continues. Later, you can use installation packages to deploy Kaspersky applications on client devices.

Step 8. Configuring Kaspersky Security Network

Specify the settings for relaying information about Kaspersky Security Center operations to the Kaspersky Security Network knowledge base. Select one of the following options:

- **I agree to use Kaspersky Security Network**

Kaspersky Security Center and managed applications installed on client devices will automatically transfer their operation details to Kaspersky Security Network (see section "About KSN" on page [785](#)). Participation in Kaspersky Security Network ensures faster updates of databases containing information about viruses and other threats, which

ensures a faster response to emergent security threats.

- **I do not agree to use Kaspersky Security Network**

Kaspersky Security Center and managed applications will provide no information to Kaspersky Security Network.

If you select this option, the use of Kaspersky Security Network will be disabled.

Step 9. Selecting the application activation method

Select one of the following Kaspersky Security Center activation options:

- By entering your activation code

Activation code is a unique sequence of 20 alphanumeric characters. You enter an activation code to add a key that activates Kaspersky Security Center. You receive the activation code through the email address that you specified after purchasing Kaspersky Security Center.

To activate the application with an activation code, you need Internet access to establish connection with Kaspersky activation servers.

If you have selected this activation option, you can enable the **Automatically deploy license key to managed devices** option.

If this option is enabled, the license key will be deployed automatically to managed devices.

If this option is disabled, you can deploy license key to managed devices later, in the **Kaspersky Licenses** node of the Administration Console tree.

- By specifying a key file

Key file is a file with the .key extension provided to you by Kaspersky. A key file is intended for adding a key that activates the application.

You receive your key file through the email address that you specified after purchasing Kaspersky Security Center.

To activate the application using a key file, you do not have to connect to Kaspersky activation servers.

If you have selected this activation option, you can enable the **Automatically deploy license key to managed devices** option.

If this option is enabled, the license key will be deployed automatically to managed devices.

If this option is disabled, you can deploy license key to managed devices later, in the **Kaspersky Licenses** node of the Administration Console tree.

- By postponing the application activation

The application will operate with basic functionality, without Mobile Device Management and without Vulnerability and Patch Management.

If you chose to postpone application activation, you can add a license key later at any time by selecting **OPERATIONS** → **LICENSING**.

When working with Kaspersky Security Center deployed from a paid AMI or for a Usage-based monthly billed SKU (see section "Licensing options in a cloud environment" on page [826](#)), you cannot specify a key file or enter a code.

See also:

Scenario: Installation and initial setup of Kaspersky Security Center 13 Web Console[962](#)

Step 10. Specifying the third-party update management settings

This step is not displayed if you do not have the Vulnerability and Patch Management license (see section "Kaspersky Security Center licensing options" on page [320](#)) and the *Find vulnerabilities and required updates* task already exists.

For third-party software updates, select one of the following options:

- **Search for required updates**

The *Find vulnerabilities and required updates* task is created.

This option is selected by default.

- **Find and install required updates**

The *Find vulnerabilities and required updates* and *Install required updates and fix vulnerabilities* tasks are created automatically, if you do not have ones.

This option is only available under the Vulnerability and Patch Management license (see section "Kaspersky Security Center licensing options" on page [320](#)).

For Windows Update updates, select one of the following options:

- **Use the update sources defined in the domain policy**

- **Use Administration Server as a WSUS server**

Client devices will download Windows Update updates from the Administration Server. The *Perform Windows Update synchronization* task and Network Agent policy are created automatically, if you do not have ones.

This option is only available under the Vulnerability and Patch Management license (see section "Kaspersky Security Center licensing options" on page [320](#)).

See also:

Scenario: Updating third-party software	1208
Scenario: Finding and fixing vulnerabilities in third-party software	459
Creating the Find vulnerabilities and required updates task	1216
Creating the Install required updates and fix vulnerabilities task	1221
Creating the Perform Windows Update synchronization task	1234

Step 11. Creating a basic network protection configuration

You can check a list of policies and tasks that are created.

Wait for the creation of policies and tasks to complete before proceeding to the next step of the Wizard.

Step 12. Configuring email notifications

Configure the delivery of notifications about events registered during the operation of Kaspersky applications on client devices. These settings will be used as the default settings for application policies.

To configure the delivery of notifications about events occurring in Kaspersky applications, use the following settings:

- **Email addresses of recipients**

The email addresses of users to whom the application will send notifications. You can enter one or more addresses; if you enter more than one address, separate them with a semicolon.

- **SMTP server address**

The address or addresses of your organization's mail servers.

If you enter more than one address, separate them with a semicolon. You can use the IP address or the Windows network name (NetBIOS name) of a device as the address.

- **SMTP server port**

Communication port number of the SMTP server. The default port number is 25.

- **Use ESMTP authentication**

Enables support of ESMTP authentication. When the check box is selected, in the **User name** and **Password** fields you can specify the ESMTP authentication settings. By default, this check box is cleared, and the ESMTP authentication settings are not available.

You can test the new email notification settings by clicking the **Send test message** button.

Step 13. Performing a network poll

The Administration Server performs an initial poll. During the poll, a progress bar is displayed. When the poll is complete, the **View detected devices** link becomes available. You can click this link to view network devices detected by Administration Server. To return to the Quick Start Wizard, press the **ESCAPE** key.

See also:

Scenario: Discovering networked devices.....[1038](#)

Step 14. Closing the Quick Start Wizard

On the Quick Start Wizard completion page, select the **Run Protection Deployment Wizard** check box if you want to start automatic installation (see section "Protection Deployment Wizard" on page [1001](#)) of anti-virus applications or Network Agent on devices on your network.

To close the Wizard, click the **Finish** button.

Protection Deployment Wizard

To install Kaspersky applications, you can use the Protection Deployment Wizard. The Protection Deployment Wizard allows remote installation of applications either through specially created installation packages or directly from a distribution package.

Protection Deployment Wizard performs the following actions:

- Downloads an installation package for application installation (if it was not created earlier). The installation package is located at **DISCOVERY & DEPLOYMENT** → **DEPLOYMENT & ASSIGNMENT** → **INSTALLATION PACKAGES**. You can use this installation package for the application installation in the future.
- Creates and runs a remote installation task for specific devices or for an administration group. The newly created remote installation task is stored in the **Tasks** section. You can later launch this task manually. The task type is **Install application remotely**.

In this section

Starting Protection Deployment Wizard.....	1001
Step 1. Selecting the installation package.....	1002
Step 2. Selecting a method for distribution of key file or activation code	1002
Step 3. Selecting Network Agent version	1002
Step 4. Selecting devices	1002
Step 5. Specifying the remote installation task settings	1003
Step 6. Restart management.....	1004
Step 7. Removing incompatible applications before installation	1005
Step 8. Moving devices to Managed devices	1005
Step 9. Selecting accounts to access devices	1005
Step 10. Starting installation.....	1006

Starting Protection Deployment Wizard

The Protection Deployment Wizard starts automatically after you complete the Quick Start Wizard if you selected (see section "Step 14. Closing the Quick Start Wizard" on page [1001](#)) the **Run Protection Deployment Wizard** option. However, you can start the Protection Deployment Wizard manually at any time.

► *To start the Protection Deployment Wizard manually,*

In the main application window, click **DISCOVERY & DEPLOYMENT** → **DEPLOYMENT & ASSIGNMENT** → **PROTECTION DEPLOYMENT WIZARD**.

The Protection Deployment Wizard starts. Proceed through the Wizard by using the **Next** button.

Step 1. Selecting the installation package

Select the installation package of the application that you want to install.

If the installation package of the required application is not listed, click the **Add** button and then select the application from the list.

Step 2. Selecting a method for distribution of key file or activation code

Select a method for the distribution of the key file or the activation code:

- **Do not add license key to installation package**

The key is automatically distributed to all devices with which it is compatible:

- If automatic distribution (see section "Automatic distribution of a license key" on page [361](#)) has been enabled in the key properties.
- If the **Add key** task has been created.

- **Add license key to installation package**

The key is distributed to devices together with the installation package.

We do not recommend that you distribute the key using this method because shared read access is enabled to the packages repository.

If the installation package already includes a key file or an activation code, this window is displayed, but it only contains the license key details.

Step 3. Selecting Network Agent version

If you selected the installation package of an application other than Network Agent, you also have to install Network Agent, which connects the application with Kaspersky Security Center Administration Server.

Select the latest version of Network Agent.

Step 4. Selecting devices

Specify a list of devices on which the application will be installed:

- **Install on managed devices**

If this option is selected, the remote installation task is created for a group of devices.

- **Select devices for installation**

The task is assigned to devices included in a device selection. You can specify one of the existing selections.

For example, you may want to use this option to run a task on devices with a specific operating system version.

Step 5. Specifying the remote installation task settings

On the "**Remote installation**" **task settings** page, specify the settings for remote installation of the application.

In the **Force installation package download** settings group, specify how files that are required for the application installation are distributed to client devices:

- **Using Network Agent**

If this option is enabled, installation packages are delivered to client devices by Network Agent installed on those client devices.

If this option is disabled, installation packages are delivered using Microsoft Windows tools.

We recommend that you enable this option if the task has been assigned to devices with Network Agents installed.

By default, this option is enabled.

- **Using operating system resources through distribution points**

If this option is enabled, installation packages are transmitted to client devices using operating system tools through distribution points. You can select this option if there is at least one distribution point on the network.

If the **Using Network Agent** option is enabled, the files are delivered using operating system tools only if Network Agent tools are unavailable.

By default, this option is enabled for remote installation tasks that have been created on a virtual Administration Server.

- **Using operating system resources through Administration Server**

If this option is enabled, files will be transmitted to client devices by using Microsoft Windows tools through the Administration Server. You can enable this option if no Network Agent is installed on the client device, but the client device is in the same network as the Administration Server.

By default, this option is enabled.

Define the additional settings:

- **Do not re-install application if it is already installed**

If this option is enabled, the selected application will not be re-installed if it has already

been installed on this client device.

If this option is disabled, the application will be installed anyway.

By default, this option is enabled.

- **Assign package installation in Active Directory group policies**

If this option is enabled, an installation package is installed by using the Active Directory group policies.

This option is available if the Network Agent installation package is selected.

By default, this option is disabled.

Step 6. Restart management

Specify the action to be performed if the operating system must be restarted when you install the application:

- **Do not restart the device**

Client devices are not restarted automatically after the operation. To complete the operation, you must restart a device (for example, manually or through a device management task). Information about the required restart is saved in the task results and in the device status. This option is suitable for tasks on servers and other devices where continuous operation is critical.

- **Restart the device**

Client devices are always restarted automatically if a restart is required for completion of the operation. This option is useful for tasks on devices that provide for regular pauses in their operation (shutdown or restart).

- **Prompt user for action**

The restart reminder is displayed on the screen of the client device, prompting the user to restart it manually. Some advanced settings can be defined for this option: text of the message for the user, the message display frequency, and the time interval after which a restart will be forced (without the user's confirmation). This option is most suitable for workstations where users must be able to select the most convenient time for a restart.

By default, this option is selected.

- **Repeat prompt every (min)**

If this option is enabled, the application prompts the user to restart the operating system with the specified frequency.

By default, this option is enabled. The default interval is 5 minutes. Available values are between 1 and 1 440 minutes.

If this option is disabled, the prompt is displayed only once.

- **Restart after (min)**

After prompting the user, the application forces restart of the operating system upon expiration of the specified time interval.

By default, this option is enabled. The default delay is 30 minutes. Available values are between 1 and 1 440 minutes.

- **Wait time before forced closure of applications in blocked sessions (min)**

Running applications may prevent a restart of the client device. For example, if a document is being edited in a word processing application and is not saved, the application does not allow the device to restart.

If this option is enabled, such applications on a locked device are forced to close before the device restart. As a result, users may lose their unsaved changes.

If this option is disabled, a locked device is not restarted. The task status on this device states that a device restart is required. Users have to manually close all applications running on locked devices and restart these devices.

By default, this option is disabled.

Step 7. Removing incompatible applications before installation

This step is only present if the application that you deploy is known to be incompatible with some other applications.

Select the option if you want Kaspersky Security Center to automatically remove applications that are incompatible with the application you deploy.

The list of incompatible applications is also displayed.

If you do not select this option, the application will only be installed on devices that have no incompatible applications.

Step 8. Moving devices to Managed devices

Specify whether devices must be moved to an administration group after Network Agent installation.

- **Do not move devices**

The devices remain in the groups in which they are currently located. The devices that have not been placed in any group remain unassigned.

- **Move unassigned devices to group**

The devices are moved to the administration group that you select.

The **Do not move devices** option is selected by default. For security reasons, you might want to move the devices manually.

Step 9. Selecting accounts to access devices

If necessary, add the accounts that will be used to start the remote installation task:

- **No account required (Network Agent installed)**

If this option is selected, you do not have to specify the account under which the application installer will be run. The task will run under the account under which the Administration Server service is running.

If Network Agent has not been installed on client devices, this option is not available.

- **Account required (Network Agent is not used)**

If this option is selected, you can specify the account under which the application installer will be run. You can specify the user account if Network Agent has not been installed on the devices for which the task is assigned.

You can specify multiple user accounts if, for example, none of them have all the required rights on all devices for which this task is assigned. In this case, all accounts that have been added are used for running the task, in consecutive order, top-down.

If no accounts have been added, the task will be run under the account under which the Administration Server service is running.

Step 10. Starting installation

This page is the final step of the Wizard. At this step, the remote installation task has been successfully created and configured.

By default, the **Run the task after the Wizard finishes** option is not selected. If you select this option, the remote installation task will start immediately after you complete the Wizard. If you do not select this option, the remote installation task will not start. You can later start this task manually.

The task name corresponds to the name of the installation package for the application: **Remote installation of <Installation package name>**.

Click **OK** to complete the final step of the Protection Deployment Wizard.

Configuring Administration Server

This section describes the configuration process and properties of Kaspersky Security Center Administration Server.

In this chapter

Configuring the connection of Kaspersky Security Center 13 Web Console to Administration Server	1007
Viewing log of connections to the Administration Server	1008
Setting the maximum number of events in the event repository	1008
Modifying the Mobile Device Management settings	1009
Connection settings of UEFI protection devices	1010
Creating a virtual Administration Server	1010
Creating a hierarchy of Administration Servers: adding a secondary Administration Server	1011
Viewing the list of secondary Administration Servers	1013
Deleting a hierarchy of Administration Servers	1014
Configuring the interface	1014
Enabling account protection from unauthorized modification	1015
Two-step verification	1015

Configuring the connection of Kaspersky Security Center 13 Web Console to Administration Server

► *To set the connection ports of Administration Server:*

1. At the top of the screen, click the **Settings** icon () next to the name of the required Administration Server.

The Administration Server properties window opens.

2. On the **General** tab, select the **Connection ports** section.

The application displays the main connection settings of the selected server.

In earlier versions of Kaspersky Security Center, Administration Console was connected to Administration Server through SSL port TCP 13291, as well as SSL port TCP 13000. Starting from Kaspersky Security Center 10 Service Pack 2, the SSL ports used by the application are strictly separated and misuse of ports is not possible:


- SSL port TCP 13291 can only be used by Administration Console.
- SSL port TCP 13000 can only be used by Network Agent, a secondary Administration Server, and the primary Administration Server in the DMZ.
- Port TCP 14000 can be used for connecting Administration Console, distribution points, and secondary Administration Servers, as well as for receiving data from client devices.



Viewing log of connections to the Administration Server

The history of connections and attempts to connect to the Administration Server during its operation can be saved to a log file. The information in the file allows you to track not only connections inside your network infrastructure, but unauthorized attempts to access the server as well.

► *To log events of connection to the Administration Server:*

1. In the main application window, click the **Settings** icon () next to the name of the required Administration Server.

The Administration Server properties window opens.

2. On the **General** tab, select the **Connection ports** section.
3. Enable the **Log Administration Server connection events** option.


All further events of inbound connections to the Administration Server, authentication results, and SSL errors will be saved to the file %ProgramData%\KasperskyLab\adminikit\logs\sc.syslog.

Setting the maximum number of events in the event repository

In the **Events repository** section of the Administration Server properties window, you can edit the settings of events storage in the Administration Server database by limiting the number of event records and record storage term. When you specify the maximum number of events, the application calculates an approximate amount of storage space required for the specified number. You can use this approximate calculation to evaluate whether you have enough free space on the disk to avoid database overflow. The default capacity of the Administration Server database is 400,000 events. The maximum recommended capacity of the database is 45 million events.

If the number of events in the database reaches the maximum value specified by the administrator, the application deletes the oldest events and rewrites them with new ones. When the Administration Server deletes old events, it cannot save new events to the database. During this period of time, information about events that were rejected is written to the Kaspersky Event Log. The new events are queued and then saved to the database after the deletion operation is complete.


► *To limit the number of events that can be stored in the events repository on the Administration Server:*

1. At the top of the screen, click the **Settings** icon () next to the name of the required Administration Server.
The Administration Server properties window opens.
2. On the **General** tab, select the **Events repository** section.
3. Specify the maximum number of events stored in the database.
4. Click the **Save** button.

The number of events that can be stored to the database is limited to the specified value.

Modifying the Mobile Device Management settings

► *To modify the Mobile Device Management settings:*

1. In the main application window, click the **Settings** icon () next to the name of the required Administration Server.
The Administration Server properties window opens.
2. On the **General** tab, select the **Additional ports** section.
3. Modify the relevant settings (see section "Step 10. Connecting mobile devices" on page [272](#)):

- **Open port for mobile devices**

If this option is enabled, the port for mobile devices will be open on the Administration Server.

You can use the port for mobile devices only if the Mobile Device Management component is installed.

If this option is disabled, the port for mobile devices on the Administration Server will not be used.

By default, this option is disabled.

- **Port for mobile device synchronization**

Number of the port used for connection of mobile devices to the Administration Server. The default port number is 13292.

The decimal system is used for records.

- **Port for mobile device activation**

The port for connection of Kaspersky Endpoint Security for Android to activation servers of Kaspersky.

The default port number is 17100.

4. Click the **Save** button.

The mobile devices can now connect to the Administration Server.

Connection settings of UEFI protection devices

A *UEFI protection device* is a device with Kaspersky Anti-Virus for UEFI integrated at the BIOS level. Integrated protection ensures device security from the moment the system starts, while protection on devices without integrated software begins functioning only after the security application starts. Kaspersky Security Center supports management of these devices.

► *To modify the connection settings of UEFI protection devices:*

In the main application window, click the **Settings** icon () next to the name of the required Administration Server.

The Administration Server properties window opens.

1. On the **General** tab, select the **Additional ports** section.
2. Modify the relevant settings:

- **Open port for UEFI protection devices**

UEFI protection devices can connect to the Administration Server.

- **Port for UEFI protection devices**

You can change the port number if the **Open port for UEFI protection devices** option is enabled. The default port number is 13294.


3. Click the **Save** button.

The UEFI protection devices can now connect to the Administration Server.

Creating a virtual Administration Server

You can create virtual Administration Servers and add them to administration groups.

► *To create and add a virtual Administration Server:*

1. In the main application window, click the **Settings** icon () next to the name of the required Administration Server.
2. On the page that opens, proceed to the **Administration Servers** tab.
3. Select the administration group to which you want to add a virtual Administration Server.
4. In the menu line, click **New virtual Administration Server**.
5. On the page that opens, define the properties of the new virtual Administration Server:
 - **Name of virtual Administration Server.**
 - **Administration Server connection address** (you can specify the name or the IP address of your Administration Server).

6. On the same page, select virtual Administration Server administrator from the list of users.
If you want, you can edit one of the existing accounts before assigning it the administrator's role, or create a new user account.
7. Click **Save**.


The new virtual Administration Server is created, added to the administration group and displayed on the **Administration Servers** tab.

Creating a hierarchy of Administration Servers: adding a secondary Administration Server

Adding secondary Administration Server (performed on the future primary Administration Server)

You can add an Administration Server as a secondary Administration Server, thus establishing a "primary / secondary" hierarchy.

► *To add a secondary Administration Server that is available for connection through Kaspersky Security Center 13 Web Console:*

1. Make sure that port 13000 of the future primary Administration Server is available for receipt of connections from secondary Administration Servers.
2. On the future primary Administration Server, click the **Settings** icon (.
3. On the properties page that opens, click the **Administration Servers** tab.
4. Select the check box next to the name of the administration group to which you want to add the Administration Server.
5. In the menu line, click **Connect secondary Administration Server**.

The Connect secondary Administration Server Wizard starts.

6. On the first page of the Wizard, fill in the following fields:
 - **Secondary Administration Server display name**
Specify a name by which the secondary Administration Server will be displayed in the hierarchy.
 - **Secondary Administration Server address (optional)**
Specify the IP address or the domain name of the secondary Administration Server.
You can leave this field blank. In this case, you will have to add a secondary Administration Server while on the secondary Administration Server side, not on the primary Administration Server side.
 - **Administration Server SSL port**
Specify the number of the SSL port on the primary Administration Server. The default port number is 13000.
 - **Administration Server API port**
Specify the number of the port on the primary Administration Server for receiving connections over OpenAPI. The default port number is 13299.
 - **Connect primary Administration Server to secondary Administration Server in DMZ**

Select this option if the secondary Administration Server is in a demilitarized zone (DMZ).

- **Use proxy server**

Select this option if you use a proxy server to connect to the secondary Administration Server.

In this case, you also have to specify the following settings of the proxy server:

- **Address**
- **User name**
- **Password**

1. Follow the further instructions of the Wizard.

After the Wizard finishes, the "primary / secondary" hierarchy is built. The primary Administration Server starts receiving connection from the secondary Administration Server through port 13000. The tasks and policies from the primary Administration Server are received and applied. The secondary Administration Server is displayed on the primary Administration Server, in the administration group to which it was added.


Adding secondary Administration Server (performed on the future secondary Administration Server)

If you could not connect to the future secondary Administration Server (for example, because it was temporarily disconnected or unavailable), you are still able to add a secondary Administration Server.

► *To add as secondary an Administration Server that is not available for connection through Kaspersky Security Center 13 Web Console:*

1. Send the certificate file of the future primary Administration Server to the system administrator of the office where the future secondary Administration Server is located. (You can, for example, write the file to an external device, such as a flash drive, or send it by email.)

The certificate file is located on the future primary Administration Server, at %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminikit\1093\cert\klserver.cer.

2. Prompt the system administrator in charge of the future secondary Administration Server to do the following:
 - a. Click the **Settings** icon (.
 - b. On the properties page that opens, proceed to the **Hierarchy of Administration Servers** section of the **General** tab.
 - c. Select the **This Administration Server is secondary in the hierarchy** option.
 - d. In the **Primary Administration Server address** field, enter the network name of the future primary Administration Server.
 - e. Select the previously saved file with the certificate of the future primary Administration Server by clicking **Browse**.
 - f. If necessary, select the **Connect primary Administration Server to secondary Administration Server in DMZ** check box.
 - g. If the connection to the future secondary Administration Server is performed through a proxy server, select the **Use proxy server** check box and specify the connection settings.
 - h. Click **Save**.

The "primary / secondary" hierarchy is built. The primary Administration Server starts receiving connection from the secondary Administration Server using port 13000. The tasks and policies from the primary Administration


Server are received and applied. The secondary Administration Server is displayed on the primary Administration Server, in the administration group where it was added.

See also:

Hierarchy of Administration Servers with a secondary Administration Server in DMZ.....	115
Hierarchy of Administration Servers: primary Administration Server and secondary Administration Server.....	114
Ports used by Kaspersky Security Center	65

Viewing the list of secondary Administration Servers

► *To view the list of the secondary (including virtual) Administration Servers,*

In the main application window, click the name of the Administration Server, which is next to the **Settings** icon ().

The drop-down list of the secondary (including virtual) Administration Servers is displayed.

You can proceed to any of these Administration Servers by clicking its name.






Deleting a hierarchy of Administration Servers

If you no longer want to have a hierarchy of Administration Servers, you can disconnect them from this hierarchy.

► *To delete a hierarchy of Administration Servers:*

1. At the top of the screen, click the **Settings** icon () next to the name of the primary Administration Server.
2. On the page that opens, proceed to the **Administration Servers** tab.
3. In the administration group from which you want to delete the secondary Administration Server, select the secondary Administration Server.
4. In the menu line, click **Delete**.
5. In the window that opens, click **OK** to confirm that you want to delete the secondary Administration Server.

The former primary Administration Server and the former secondary Administration Server are now independent of each other. The hierarchy no longer exists.

Configuring the interface

You can configure the Kaspersky Security Center 13 Web Console interface to display and hide sections and interface elements, depending on the features being used.

► *To configure the Kaspersky Security Center 13 Web Console interface in accordance with the currently used set of features:*

1. In the main application window, click the account menu in the upper part of the screen.
2. In the drop-down menu, select **Interface options**.
3. In the **Interface options** window that opens, enable or disable the **Show Data encryption and protection** option.
4. Click **Save**.

The console displays the **DATA ENCRYPTION AND PROTECTION** section.

Enabling account protection from unauthorized modification

You can enable an additional option to protect a user account from unauthorized modification. If this option is enabled, modifying user account settings requires authorization of the user with the rights for modification.

► *To enable or disable account protection from unauthorized modification:*

1. Go to **USERS & ROLES** → **USERS**.
2. Click the name of the internal user account for which you want to specify account protection from unauthorized modification.
3. In the user settings window that opens, select the **Account protection** tab.
4. On the **Account protection** tab, select the **Request authentication to check permission to modify user accounts** option if you want to request credentials every time when account settings are changed or modified. Otherwise, select the **Allow users to modify this account without additional authentication** option.
5. Click the **Save** button.

Account protection from unauthorized modification is enabled for a user account.

Two-step verification

This section describes how you can use two-step verification to reduce the risk of unauthorized access to Administration Console.

In this section

Scenario: configuring two-step verification for all users	1015
About two-step verification.....	1017
Enabling two-step verification for your own account	1019
Enabling two-step verification for all users	1019
Disabling two-step verification for a user account	1020
Disabling two-step verification for all users	1020
Excluding accounts from two-step verification.....	1021
Generating a new secret key	1021
Editing the name of a security code issuer	1022

Scenario: configuring two-step verification for all users

This scenario describes how to enable two-step verification for all users and how to exclude user accounts from two-step verification. If you did not enable two-step verification for your account before you enable it for other users, the application opens the window for enabling two-step verification for your account, first. This scenario also describes how to enable two-step verification for your own account.

If you enabled two-step verification for your account, you may proceed to the stage of enabling of two-step verification for all users.

Prerequisites

Before you start:

- Make sure that your user account has the Modify object ACLs (see section "Access rights to application features" on page [684](#)) right of the **General features: User permissions** functional area for modifying security settings for other users' accounts.
- Make sure that the other users of Administration Server install an authenticator application on their devices.

Stages

Enabling two-step verification for all users proceeds in stages:

a. Installing an authenticator application on a device

You can install Google Authenticator, Microsoft Authenticator, or any other authenticator application that supports the Time-based One-time Password algorithm.

b. Synchronizing the authenticator application time with the time of the device on which Administration Server is installed

Ensure that the time set in the authenticator application is synchronized with the time of Administration Server.

c. Enabling two-step verification for your account and receiving the secret key for your account

How-to instructions:

For MMC-based Administration Console: Enabling two-step verification for your own account (on page [627](#))

For Kaspersky Security Center 13 Web Console: Enabling two-step verification for your own account (on page [1019](#))

After you enable two-step verification for your account, you can enable two-step verification for all users.

d. Enabling two-step verification for all users

Users with two-step verification enabled must use it to log in to Administration Server.

How-to instructions:

For MMC-based Administration Console: Enabling two-step verification for all users (on page [628](#))

For Kaspersky Security Center 13 Web Console: Enabling two-step verification for all users (on page [1019](#))

e. Editing the name of a security code issuer

If you have several Administration Servers with similar names, you may have to change the security code issuer names for better recognition of different Administration Servers.

How-to instructions:

For MMC-based Administration Console: Editing the name of a security code issuer (on page [630](#))

For Kaspersky Security Center 13 Web Console: Editing the name of a security code issuer (on page [1022](#))

f. Excluding user accounts for which you do not need to enable two-step verification

If required, exclude users from two-step verification. Users with excluded accounts do not have to use two-step verification to log in to Administration Server.

How-to instructions:

For MMC-based Administration Console: Excluding accounts from two-step verification (on page [629](#))

For Kaspersky Security Center 13 Web Console: Excluding accounts from two-step verification (on page [1021](#))

Results

Upon completion of this scenario:

- Two-step verification is enabled for your account.
- Two-step verification is enabled for all user accounts of the Administration Server, except for user accounts that were excluded.

See also:

About two-step verification.....	1017
Enabling two-step verification for your own account	1019
Enabling two-step verification for all users	1019
Disabling two-step verification for a user account	1020
Disabling two-step verification for all users	1020
Excluding accounts from two-step verification.....	1021

About two-step verification

Kaspersky Security Center provides two-step verification for users of Administration Console. When two-step verification is enabled for your own account, every time you log in to Administration Console, you enter your user name, password, and an additional single-use security code. If you use domain authentication (see section "Configuring domain authentication by using the NTLM and Kerberos protocols" on page [992](#)) for your account, you only have to enter an additional single-use security code. To receive a single-use security code, you must have an authenticator application on your computer or your mobile device.

A security code has an identifier referred to as *issuer name*. The security code issuer name is used as an identifier of the Administration Server in the authenticator application. You can change the name of the security code issuer name. The security code issuer name has a default value that is the same as the name of the Administration Server. The issuer name is used as an identifier of the Administration Server in the authenticator application. If you change the security code issuer name, you must issue a new secret key and pass it to the authenticator application. A security code is single-use and valid for 30 seconds.

Any user for whom two-step verification is enabled can reissue his or her own secret key. When a user authenticates with the reissued secret key and uses it for logging in, Administration Server saves the new secret key for the user account. If the user enters the new secret key incorrectly, Administration Server does not save the new secret key and leaves the current secret key valid for the further authentication.

Any authentication software that supports the Time-based One-time Password algorithm (TOTP) can be used as an authenticator application, for example, Google Authenticator. In order to generate the security code, you must synchronize the time set in the authenticator application with the time set for Administration Server.

An authenticator application generates the security code as follows:

1. Administration Server generates a special secret key and QR code.
2. You pass the generated secret key or QR code to the authenticator application.
3. The authenticator application generates a single-use security code that you pass to the authentication window of Administration Server.

We highly recommend that you install an authenticator application on more than one device. Save the secret key (or QR code) and keep it in a safe place. This will help you to restore access to Administration Console in case you lose access to your mobile device.

To secure the usage of Kaspersky Security Center, you can enable two-step verification for your own account and enable two-step verification for all users.

You can exclude (see section "Excluding accounts from two-step verification" on page [1021](#)) accounts from two-step verification. This can be necessary for service accounts that cannot receive a security code for authentication.

Two-step verification works according to the following rules:

- Only a user account that has the Modify object ACLs (see section "Access rights to application features" on page [684](#)) right in the **General features: User permissions** functional area can enable two-step verification for all users.
- Only a user that enabled two-step verification for his or her own account can enable the option of two-step verification for all users.
- Only a user that enabled two-step verification for his or her own account can exclude other user accounts from the list of two-step verification enabled for all users.
- A user can enable two-step verification only for his or her own account.
- A user account that has the Modify object ACLs (see section "Access rights to application features" on page [684](#)) right in the **General features: User permissions** functional area and is logged in to Administration Console by using two-step verification can disable two-step verification: for any other user only if two-step verification for all users is disabled, for a user excluded from the list of two-step verification that is enabled for all users.
- Any user that logged in to Administration Console by using two-step verification can reissue his or her own secret key.
- You can enable the two-step verification for all users option for the Administration Server you are currently working with. If you enable this option on the Administration Server, you also enable this option for the user accounts of its virtual Administration Servers (on page [135](#)) and do not enable two-step verification for the user accounts of the secondary Administration Servers.

If two-step verification is enabled for a user account on Kaspersky Security Center 13 Administration Server, the user will not be able to log in to the Kaspersky Security Center Web Console of versions 12, 12.1 or 12.2.

Enabling two-step verification for your own account

You can enable two-step verification only for your own account.

Before you start enabling two-step verification for your account, ensure that an authenticator application is installed on your mobile device. Ensure that the time set in the authenticator application is synchronized with the time set of the device on which Administration Server is installed.

► *To enable two-step verification for a user account:*

1. Go to **USERS & ROLES** → **USERS**.
2. Click the name of your account.
3. In the user settings window that opens, select the **Account protection** tab.
4. On the **Account protection** tab:
 - Select the **Request user name, password, and security code (two-step verification)** option if you want to enable two-step verification for a user account:
 - In the two-step verification window that opens, enter the secret key in the authenticator application or scan the QR code and receive one-time security code.
You can specify the secret key into the authenticator application manually or scan the QR code by your mobile device.
 - In the two-step verification window, specify the security code generated by the authenticator application, and then click the **Check and apply** button.
5. Click the **Save** button.

Two-step verification is enabled for your account.

Enabling two-step verification for all users

You can enable two-step verification for all users of Administration Server if your account has the Modify object ACLs (see section "Access rights to application features" on page 684) right in the **General features: User permissions** functional area and if you are authenticated by using two-step verification. If you did not enable two-step verification for your account before enabling it for all users, the application opens the window for enabling two-step verification for your own account (on page 1019).

► *To enable two-step verification for all users:*

1. In the main application window, click the **Settings** icon () next to the name of the required Administration Server.

The Administration Server properties window opens.

2. On the **Authentication security** tab of the properties window, switch the toggle button of the **two-step verification for all users** option to the enabled position.

Two-step verification is enabled for all users. From now on, users of the Administration Server, including the users that were added after enabling two-step verification for all users, have to configure two-step verification for their accounts, except for users that are excluded (see section "Excluding accounts from two-step verification" on page [1021](#)) from two-step verification.

Disabling two-step verification for a user account

You can disable two-step verification for your own account, as well as for an account of any other user.

You can disable two-step verification of another user's account if your account has the Modify object ACLs (see section "Access rights to application features" on page [684](#)) right in the **General features: User permissions** functional area.

► *To disable two-step verification for a user account:*


1. Go to **USERS & ROLES** → **USERS**.
2. Click the name of the internal user account for whom you want to disable two-step verification. This may be your own account or an account of any other user.
3. In the user settings window that opens, select the **Account protection** tab.
4. On the **Account protection** tab, select the **Request only user name and password** option if you want to disable two-step verification for a user account.
5. Click the **Save** button.

Two-step verification is disabled for the user account.

Disabling two-step verification for all users

You can disable two-step verification for all users if two-step verification is enabled for your account and your account has the Modify object ACLs (see section "Access rights to application features" on page [684](#)) right in the **General features: User permissions** functional area. If two-step verification is not enabled for your account, you must enable two-step verification for your account (see section "Enabling two-step verification for your own account" on page [1019](#)) before disabling it for all users.

► *To disable two-step verification for all users:*

1. In the main application window, click the **Settings** icon () next to the name of the required Administration Server.
The Administration Server properties window opens.
2. On the **Authentication security** tab of the properties window, switch the toggle button of the **two-step verification for all users** option to disabled position.
3. Enter the credentials of your account in the authentication window.

Two-step verification is disabled for all users.


Excluding accounts from two-step verification

You can exclude user accounts from two-step verification if you have the Modify object ACLs (see section "Access rights to application features" on page [684](#)) right in the **General features: User permissions** functional area.

If a user account is excluded from the list of two-step verification for all users, this user does not have to use two-step verification.

Excluding accounts from two-step verification can be necessary for service accounts that cannot pass the security code during authentication.

► *If you want to exclude some user accounts from two-step verification:*

1. You must perform Active Directory polling (on page [308](#)) first, in order to refresh the list of Administration Server users. If you want to exclude an Active Directory account.
2. In the main application window, click the **Settings** icon () next to the name of the required Administration Server.
The Administration Server properties window opens.
3. On the **Authentication security** tab of the properties window, in the two-step verification exclusions table click the **Add** button.
4. In the window that opens:
 - a. Select the user accounts that you want to exclude.
 - b. Click the **OK** button.

The selected user accounts are excluded from two-step verification.

Generating a new secret key

You can generate a new secret key for a two-step verification for your account only if you are authorized by using two-step verification.

► *To generate a new secret key for a user account:*

1. Go to **USERS & ROLES** → **USERS**.
2. Click the name of the user account for whom you want to generate a new secret key for two-step verification.
3. In the user settings window that opens, select the **Account protection** tab.
4. In the **Account protection** tab, click the **Generate a new secret key** link.
5. In the two-step verification window that opens, specify a new security key generated by the authenticator application.
6. Click the **Check and apply** button.


A new secret key is generated for the user.

Editing the name of a security code issuer

You can have several identifiers (they are called issuers) for different Administration Servers. You can change the name of a security code issuer in case, for example, if the Administration Server already uses a similar name of security code issuer for another Administration Server. By default, the name of a security code issuer is the same as the name of the Administration Server.

After you change the security code issuer name you have to reissue a new secret key and pass it to the authenticator application.

► *To specify a new name of security code issuer:*

1. In the main application window, click the **Settings** icon () next to the name of the required Administration Server.

The Administration Server properties window opens.

2. In the user settings window that opens, select the **Account protection** tab.
3. On the **Account protection** tab, click the **Edit** link.

The **Edit Security code issuer** section opens.

4. Specify a new security code issuer name.
5. Click the **OK** button.

A new security code issuer name is specified for the Administration Server.

Kaspersky applications deployment through Kaspersky Security Center 13 Web Console

This section describes Kaspersky applications deployment on client devices in your organization by means of Kaspersky Security Center 13 Web Console.

In this chapter

Scenario: Kaspersky applications deployment through Kaspersky Security Center 13 Web Console.....	1023
Getting plug-ins for Kaspersky applications	1025
Downloading and creating installation packages for Kaspersky applications	1025
Changing the limit on the size of custom installation package data	1027
Downloading distribution packages for Kaspersky applications.....	1027
Checking Kaspersky Endpoint Security for Windows for success	1028
Creating stand-alone installation packages.....	1028
Viewing the list of stand-alone installation packages	1030
Creating custom installation packages.....	1031
Specifying settings for remote installation on Unix devices.....	1034
Replacing third-party security applications	1035

Scenario: Kaspersky applications deployment through Kaspersky Security Center 13 Web Console

This scenario explains how to deploy Kaspersky applications through Kaspersky Security Center 13 Web Console. You can use the Quick Start Wizard (see section "Quick Start Wizard (Kaspersky Security Center 13 Web Console)" on page [993](#)) and Protection Deployment Wizard, or you can complete all necessary steps manually.

Prerequisites

The following applications are available for deployment by using Kaspersky Security Center 13 Web Console:

- Kaspersky Endpoint Security 11.1 for Windows
- Kaspersky Endpoint Security 11.1.1 for Windows
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 1 for Linux

Kaspersky applications deployment proceeds in stages:

a. Downloading management plug-in for the application

This stage is handled by the Quick Start Wizard. If you choose not to run the Wizard, download (see section "Getting plug-ins for Kaspersky applications" on page [1025](#)) the plug-in for Kaspersky Endpoint Security for Windows manually.

b. Downloading and creating installation packages

This stage is handled by the Quick Start Wizard.

The Quick Start Wizard allows you to download the installation package with the management plug-in. If you did not select this option when running the Wizard, or if you did not run the Wizard at all, you must download the package manually (see section "Downloading and creating installation packages for Kaspersky applications" on page [1025](#)).

If you cannot install Kaspersky applications by means of Kaspersky Security Center on some devices, for example, on remote employees' devices, you can create stand-alone installation packages (see section "Creating stand-alone installation packages" on page [1028](#)) for applications. If you use stand-alone packages to install Kaspersky applications, stage 3 and stage 4 below can be disregarded.

c. Creating, configuring, and running the remote installation task

For Kaspersky Endpoint Security for Windows, this step is part of the Protection Deployment Wizard, which starts automatically after the Quick Start Wizard has finished. If you choose not to run the Protection Deployment Wizard, you must create this task manually (see section "Creating a task" on page [1080](#)) and configure it manually.

You also can manually create several remote installation tasks for different administration groups or different device selections. You can deploy different versions of one application in these tasks.

Make sure that all the devices on your network are discovered; then run the remote installation task (or tasks).

d. Creating and configuring tasks

The *Install update task* of Kaspersky Endpoint Security for Windows must be configured.

This step is part of the Quick Start Wizard: the task is created and configured automatically with the default settings. If you did not run the Wizard, you must create this task manually (see section "Creating a task" on page [1080](#)) and configure it manually. If you use the Quick Start Wizard, make sure that the schedule for the task (see section "General task settings" on page [1081](#)) meets your requirements. (By default, the scheduled start for the task is set to **Manually**, but you might want to choose another option.)

Other Kaspersky applications might have other default tasks. Please refer to the documentation of the corresponding applications for details.

Make sure that the schedule for each task that you create meets your requirements.

e. Creating policies

Create the policy for each application manually (see section "Creating a policy" on page [1118](#)) or (in case of Kaspersky Endpoint Security for Windows) through the Quick Start Wizard. You can use the default settings of the policy; you can also modify the default settings (see section "Creating a policy" on page [1118](#)) of the policy according to your needs at any time.

f. Verifying the results

Make sure (see section "Checking Kaspersky Endpoint Security for Windows for success" on page [1028](#)) that deployment was completed successfully: you have policies and tasks for each application, and these applications are installed on the managed devices.

Results

Completion of the scenario yields the following:

- All required policies and tasks for the selected applications are created.
- The schedules of tasks are configured according to your needs.
- The selected applications are deployed, or scheduled to be deployed, on the selected client devices.

See also:

Scenario: Installation and initial setup of Kaspersky Security Center 13 Web Console	962
Scenario: Regular updating Kaspersky databases and applications	1174

Getting plug-ins for Kaspersky applications

To deploy a Kaspersky application, such as Kaspersky Endpoint Security 11 for Windows, you must download the management plug-in for the application.

To download a management plug-in for a Kaspersky application:

1. In the **Console settings** drop-down list, select **Web plug-ins**.
A list of available management plug-ins is displayed.
2. Click **Add**.
The list of available plug-ins is displayed.
3. In the list of available plug-ins, select the plug-in you want to download (for example, Kaspersky Endpoint Security 11 for Windows) by clicking on its name.
A plug-in description page is displayed.
4. On the plug-in description page, click **Install plug-in**.
5. When the installation is complete, click **OK**.

The management plug-in is downloaded with the default configuration and displayed in the list of management plug-ins.

See also:

Management web plug-in	50
Scenario: Kaspersky applications deployment through Kaspersky Security Center 13 Web Console ...	1023

Downloading and creating installation packages for Kaspersky applications

You can create installation packages for Kaspersky applications from Kaspersky web servers if your Administration Server has access to the internet.

► *To download and create installation package for Kaspersky application:*

1. Do one of the following:
 - Go to **DISCOVERY & DEPLOYMENT** → **DEPLOYMENT & ASSIGNMENT** → **INSTALLATION PACKAGES**.
 - Go to **OPERATIONS** → **REPOSITORIES** → **INSTALLATION PACKAGES**packages.

You can also view notifications about new packages for Kaspersky applications in the list of onscreen notifications (see section "Viewing onscreen notifications" on page [1293](#)). If there are notifications about a new package, you can click the link next to the notification and proceed to the list of available installation packages.

A list of installation packages available on Administration Server is displayed.

2. Click **Add**.

The New Package Wizard starts. Proceed through the Wizard by using the **Next** button.

3. On the first page of the Wizard, select **Create an installation package for a Kaspersky application**.

A list of available installation packages on Kaspersky web servers appears. The list contains installation packages only for those applications that are compatible with the current version of Kaspersky Security Center.

4. Click the name of an installation package, for example, Kaspersky Endpoint Security for Windows (11.1.0).

A window opens with information about the installation package.

5. Read the information and click the **Download and create installation package** button.

If a distribution package can not be converted to an installation package, the **Download distribution package** button instead of the **Download and create installation package** is displayed.

The downloading of the installation package to Administration Server starts. You can close the Wizard's window or proceed to the next step of the instruction. If you close the Wizard's window, the download process will continue in background mode.

If you want to track an installation package download process:

- a. Go to **OPERATIONS** → **REPOSITORIES** → **INSTALLATION PACKAGES** → **In progress ()**.
- b. Track the operation progress in the **Download progress** column and the **Download status** column of the table.

When the process is complete, the installation package is added to the list on the **Downloaded** tab. If the download process stops and the download status switches to **Accept EULA**, then click the installation package name, and then proceed to the next step of the instruction.

If the size of data contained in the selected distribution package exceeds the current limit, an error message is displayed. You can change the limit value and then proceed with the installation package creation.

6. For some Kaspersky applications, during the download process the **Show EULA** button is displayed. If it is displayed, do the following:
 - a. Click the **Show EULA** button to read the End User License Agreement (EULA).
 - b. Read the EULA that is displayed on the screen, and click **Accept**.

The downloading continues after you accept the EULA. If you click **Decline**, the download is stopped.

7. When the downloading is complete, click the **Close** button.

The selected installation package is downloaded to the Administration Server shared folder, to the Packages subfolder. After downloading, the installation package is displayed in the list of installation packages.

See also:

Creating an installation package	344
Viewing onscreen notifications	1293
Scenario: Kaspersky applications deployment through Kaspersky Security Center 13 Web Console ...	1023

Changing the limit on the size of custom installation package data

This section describes features applicable only to Kaspersky Security Center 12.1 or a later version.

The total size of data unpacked during creation of a custom installation package is limited. The default limit is 400 megabytes (MB).

If you attempt to upload an archive file that contains data exceeding the current limit, an error message is displayed. You might have to increase this limit value when creating installation packages from large distribution packages.

► To change the limit value for the custom installation package size:

1. Open the system registry of the Administration Server device (for example, locally, using the `regedit` command in the **Start** → **Run** menu).
2. Go to the following hive:
 - For a 64-bit system:
HKEY_LOCAL_MACHINE\SOFTWAREWow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags
 - For a 32-bit system:
HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags
3. Create a new DWORD key following the standard registry procedure, assign it the `MaxArchivePkgSize` name, and set the required limit value.

The limit on the size of custom installation package data is changed.

Downloading distribution packages for Kaspersky applications

In Kaspersky Security Center 13 Web Console, you can download and save distribution packages for Kaspersky applications. You can use the distribution packages to install the applications manually, without using Kaspersky Security Center.

► To download and save distribution packages for Kaspersky applications:

1. On the **Operations** tab, select **Kaspersky applications** → **Current application versions**.

A list of available distribution packages, plug-ins, and patches opens. Kaspersky Security Center displays only those items that are compatible with its current version.

2. In the list, click the name of the package that you want to download.

The description of the package opens.

3. Read the description and click the **Download and create installation package** button.

If a distribution package cannot be converted to an installation package, the **Download distribution package** button is displayed instead of the **Download and create installation package**.

The download of the installation package to Administration Server starts.

The selected installation or distribution package is downloaded to the Administration Server shared folder, to the **Packages** subfolder. After it is downloaded, the installation package is displayed in the list of installation packages.

Checking Kaspersky Endpoint Security for Windows for success

- *To ensure that you have correctly deployed Kaspersky applications, such as Kaspersky Endpoint Security:*

1. Using Kaspersky Security Center 13 Web Console, make sure that you have the following:
 - A policy for Kaspersky Endpoint Security and/or other security applications that you use.
 - Tasks for Kaspersky Endpoint Security for Windows: Quick virus scan task and *Install update* task (if you use Kaspersky Endpoint Security for Windows).
 - Tasks for other security applications that you use.
2. On one of the managed devices, selected for installation, make sure of the following:
 - Kaspersky Endpoint Security or another Kaspersky security application is installed.
 - In Kaspersky Endpoint Security, the File Threat Protection, Web Threat Protection, and Mail Threat Protection settings match the policy that you created for this device.
 - Kaspersky Endpoint Security service can be stopped and started manually.
 - Group tasks can be stopped and started manually.

See also:

Scenario: Kaspersky applications deployment through Kaspersky Security Center 13 Web Console ... [1023](#)

Creating stand-alone installation packages

You and device users in your organization can use stand-alone installation packages to install applications on devices manually.

A stand-alone installation package is an executable file (installer.exe) that you can store on Web Server, in a shared folder, send by email, or transfer to a client device by another method. On the client device, the user can run the received file locally to install an application without involving Kaspersky Security Center. You can create stand-alone installation packages for Kaspersky applications and for third-party applications for Windows, macOS,

and Linux platforms. To create a stand-alone installation package for a third-party application, you must create a custom installation package (see section "Creating custom installation packages" on page [1031](#)).

Be sure that the stand-alone installation package is not available for unauthorized persons.

► *To create a stand-alone installation package:*

1. Do one of the following:

- Go to **DISCOVERY & DEPLOYMENT** → **DEPLOYMENT & ASSIGNMENT** → **INSTALLATION PACKAGES**.
- Go to **OPERATIONS** → **REPOSITORIES** → **INSTALLATION PACKAGES**.

A list of installation packages available on Administration Server is displayed.

2. In the list of installation packages, select an installation package and, above the list, click the **Deploy** button.

3. Select the **Using a stand-alone package** option.

Stand-alone Installation Package Creation Wizard starts. Proceed through the Wizard by clicking the **Next** button.

4. On the first page of the Wizard, make sure that the **Install Network Agent together with this application** option is enabled if you want to install Network Agent together with the selected application.

By default, the option is enabled. We recommend enabling this option if you are not sure whether Network Agent is installed on the device. If Network Agent is already installed on the device, after the stand-alone installation package with Network Agent is installed, Network Agent will be updated to the newer version.

If you disable this option, Network Agent will not be installed on the device and the device will be unmanaged.

If a stand-alone installation package for the selected application already exists on Administration Server, the Wizard informs you about this fact. In this case, you must select one of the following actions:

- **Create stand-alone installation package.** Select this option if, for example, you want to create a stand-alone installation package for a new application version and also want to retain a stand-alone installation package that you created for a previous application version. The new stand-alone installation package is placed in another folder.
- **Use existing stand-alone installation package.** Select this option if you want to use an existing stand-alone installation package. The process of package creation will not be started.
- **Rebuild existing stand-alone installation package.** Select this option if you want to create a stand-alone installation package for the same application again. The stand-alone installation package is placed in the same folder.

5. On the **Move to list of managed devices** page of the Wizard, by default the **Do not move devices** option is selected. If you do not want to move the client device to any administration group after Network Agent installation, leave this option selected.

If you want to move the client device after Network Agent installation, select the **Move unassigned devices to this group** option and specify an administration group to which you want to move the client device. By default, the device is moved to the **Managed devices** group.

6. On the next page of the Wizard, when the process of the stand-alone installation package creation is finished, click the **FINISH** button.

The Stand-alone Installation Package Creation Wizard closes.

The stand-alone installation package is created and placed in the PkgInst subfolder of the Administration Server shared folder (see section "Defining a shared folder" on page [224](#)). You can view the list of stand-alone packages by clicking the **View the list of stand-alone packages** button above the list of installation packages.

See also:

Scenario: Kaspersky applications deployment through Kaspersky Security Center 13 Web Console ... [1023](#)

Viewing the list of stand-alone installation packages

You can view the list of stand-alone installation packages and properties of each stand-alone installation package.

- *To view the list of stand-alone installation packages for all installation packages:*

Above the list, click the **View the list of stand-alone packages** button.

In the list of stand-alone installation packages the following their properties are displayed:

- **Package name.** Stand-alone installation package name that is automatically formed as the application name included in the package and the application version.
 - **Application name.** Application name included in the stand-alone installation package.
 - **Application version.**
 - **Network Agent installation package name.** The property is displayed only if Network Agent is included in the stand-alone installation package.
 - **Network Agent version.** The property is displayed only if Network Agent is included in the stand-alone installation package.
 - **Size.** File size in MB.
 - **Group.** Name of the group to which the client device is moved after Network Agent installation.
 - **Created.** Date and time of the stand-alone installation package creation.
 - **Modified.** Date and time of the stand-alone installation package modification.
 - **Path.** Full path to the folder where the stand-alone installation package is located.
 - **Web address.** Web address of the stand-alone installation package location.
 - **File hash.** The property is used to certify that the stand-alone installation package was not changed by third-party persons and a user has the same file you have created and transferred to the user.
- *To view the list of stand-alone installation packages for specific installation package:*

Select the installation package in the list and, above the list, click the **View the list of stand-alone packages** button.

In the list of stand-alone installation packages you can:

- Publish a stand-alone installation package on the Web Server by clicking the **Publish** button. Published stand-alone installation package is available for downloading for users whom you sent the link to the stand-alone installation package.
- Cancel publication of a stand-alone installation package on the Web Server by clicking the **Unpublish** button. Unpublished stand-alone installation package is available for downloading only for you and other administrators.
- Download a stand-alone installation package to your device by clicking the **Download** button.
- Send email with the link to a stand-alone installation package by clicking the **Send by email** button.
- Remove a stand-alone installation package by clicking the **Remove** button.

Creating custom installation packages

You can use custom installation packages to do the following:

- To install any application (such as a text editor) on a client device, for example, by means of a task (see section "Tasks" on page [1078](#)).
- To create a stand-alone installation package (see section "Creating stand-alone installation packages" on page [1028](#)).

A custom installation package is a folder with a set of files. The source to create a custom installation package is an *archive file*. The archive file contains a file or files that must be included in the custom installation package. While creating a custom installation package, you can specify command-line parameters, for example, to install the application in silent mode.

If you have an active license key for the Vulnerability and Patch Management (VAPM) feature, you can convert your default installation settings for the relevant custom installation package and use the values recommended by Kaspersky experts. The settings are automatically converted during the creation of the custom installation package only if the corresponding executable file is included in the Kaspersky database of third-party applications.

► *To create a custom installation package:*

1. Do one of the following:
 - Go to **DISCOVERY & DEPLOYMENT** → **DEPLOYMENT & ASSIGNMENT** → **INSTALLATION PACKAGES**.
 - Go to **OPERATIONS** → **REPOSITORIES** → **INSTALLATION PACKAGES**.

A list of installation packages available on the Administration Server is displayed.

2. Click **Add**.
The New Package Wizard starts. Proceed through the Wizard by using the **Next** button.
3. On the first page of the Wizard, select **Create an installation package from a file**.
4. On the next page of the Wizard, specify the package name and click the **Browse** button.

A standard Windows **Open** window in your browser opens to let you choose a file to create the installation package.

5. Choose an archive file located on the available disks.

You can choose one of the following file types: ZIP, CAB, TAR, or TAR.GZ.

It is not possible to create an installation package from an SFX (self-extracting archive) file.

If you want the settings to be converted during the package installation, make sure the **Convert settings to recommended values for applications recognized by Kaspersky Security Center after the Wizard finishes** check box is selected, and then click **Next**.

File upload to the Kaspersky Security Center 13 Administration Server starts.

If you enabled the use of the recommended installation settings, Kaspersky Security Center 13 checks whether the executable file is included in the Kaspersky database of third-party applications. If the check is successful, you get a notification informing you that the file is recognized. The settings are converted and the custom installation package is created. No further actions are required. Click the **Finish** button to close the Wizard.

6. On the next page of the Wizard, select a file (from the list of files that are extracted from the chosen archive file) and specify the command-line parameters of an executable file.

You can specify command-line parameters to install the application from the installation package in a silent mode. Specifying command-line parameters is optional.

The process to create the installation package is started.

The Wizard informs you when the process is finished.

If the installation package is not created, an appropriate message is displayed.

7. Click the **Finish** button to close the Wizard.

The installation package that you created is downloaded to the Packages subfolder of the Administration Server shared folder (see section "Defining a shared folder" on page [224](#)). After downloading, the installation package appears in the list of installation packages.

In the list of installation packages available on Administration Server, by clicking the link with the name of a custom installation package, you can:

- View the following properties of an installation package:
 - **Name.** Custom installation package name.
 - **Source.** Application vendor name.
 - **Application.** Application name packed into the custom installation package.
 - **Version.** Application version.
 - **Language.** Language of the application packed into the custom installation package.
 - **Size (MB).** Size of the installation package.
 - **Operating system.** Type of the operating system for which the installation package is intended.

- **Created.** Installation package creation date.
- **Modified.** Installation package modification date.
- **Type.** Type of the installation package.
- Change the package name and command-line parameters. This feature is available only for packages that are not created on the basis of Kaspersky applications.

If you have converted the package installation settings to the recommended values for the custom package creation process, two additional sections may appear on the **Settings** tab of the custom installation package properties: **Settings** and **Installation procedure**.

The **Settings** section contains the following properties, shown in a table:

- **Name.** This column shows the name assigned to an installation parameter.
- **Type.** This column shows the type of an installation parameter.
- **Value.** This column shows the type of data defined by an installation parameter (Bool, Filepath, Numeric, Path, or String).

The **Installation procedure** section contains a table that describes the following properties of the update included in the custom installation package:

- **Name.** The name of the update.
- **Description.** The description of the update.
- **Source.** The source of the update, that is, whether it was released by Microsoft or by a different third-party developer.
- **Type.** The type of the update, that is, whether it is intended for a driver or an application.
- **Category.** The Windows Server Update Services (WSUS) category displayed for Microsoft updates (Critical Updates, Definition Updates, Drivers, Feature Packs, Security Updates, Service Packs, Tools, Update Rollups, Updates, or Upgrade).
- **Importance level according to MSRC.** The importance level of the update, as defined by Microsoft Security Response Center (MSRC).
- **Importance level.** The importance level of the update, as defined by Kaspersky.
- **Patch importance level (for patches intended for Kaspersky applications).** The importance level of the patch if it is intended for a Kaspersky application.
- **Article.** The identifier (ID) of the article in the Knowledge Base describing the update.
- **Bulletin.** The ID of the security bulletin describing the update.
- **Not assigned for installation.** Displays whether the update has the Not assigned for installation status.
- **To be installed.** Displays whether the update has the To be installed status.
- **Installing.** Displays whether the update has the Installing status.
- **Installed.** Displays whether the update has the Installed status.
- **Failed.** Displays whether the update has the Failed status.
- **Restart is required.** Displays whether the update has the Restart is required status.

- **Registered.** Displays the date and time when the update was registered.
- **Installed in interactive mode.** Displays whether the update requires interaction with the user during installation.
- **Revoked.** Displays the date and time when the update was revoked.
- **Update approval status.** Displays whether the update is approved for installation.
- **Revision.** Displays the current revision number of the update.
- **Update ID.** Displays the ID of the update.
- **Application version.** Displays the version number that the application will be updated to.
- **Superseded.** Displays other update(s) that can supersede the update.
- **Superseding.** Displays other update(s) that can be superseded by the update.
- **You must accept the terms of the License Agreement.** Displays whether the update requires acceptance of the terms of an End User License Agreement (EULA).
- **Vendor.** Displays the name of the update vendor.
- **Application family.** Displays the name of the family of applications to which the update belongs.
- **Application.** Displays the name of the application to which the update belongs.
- **Language.** Displays the language of the update localization.
- **Not assigned for installation (new version).** Displays whether the update has the Not assigned for installation (new version) status.
- **Requires prerequisites installation.** Displays whether the update has the Requires prerequisites installation status.
- **Download mode.** Displays the mode of the update download.
- **Is a patch.** Displays whether the update is a patch.
- **Not installed.** Displays whether the update has the Not installed status.

See also:

Creating an installation package	344
Viewing onscreen notifications	1293

Specifying settings for remote installation on Unix devices

When you install an application on a Unix device by using a remote installation task, you can specify Unix-specific settings for the task. These settings are available in the task properties after the task is created.

► *To specify Unix-specific settings for a remote installation task:*

1. Go to **DEVICES** → **TASKS**.
2. Click the name of the remote installation task for which you want to specify the Unix-specific settings.
The task properties window opens.

3. Go to **Application settings** → **Unix-specific settings**.
4. Specify the following settings:
 - **Password for root account (only for deployment through SSH)**
 - **Path to temporary folder with Execute permissions on target device (only for deployment through SSH)**
5. Click the **Save** button.

The specified task settings are saved.

See also:

General task settings	1081
Scenario: Kaspersky applications deployment through Kaspersky Security Center 13 Web Console ...	1023
Scenario: Monitoring and reporting	1279

Replacing third-party security applications

Installation of Kaspersky security applications through Kaspersky Security Center may require removal of third-party software incompatible with the application being installed. Kaspersky Security Center provides several ways of removing the third-party applications.

Removing incompatible applications by using the installer

This option is available in Microsoft Management Console-based Administration Console only.

The installer method of removing incompatible applications is supported by various types of installation. Before the security application installation, all incompatible applications are removed automatically if the properties window of the installation package of this security application (**Incompatible applications** section) has the **Uninstall incompatible applications automatically** check box selected.

Removing incompatible applications when configuring remote installation of an application

You can enable the **Uninstall incompatible applications automatically** option when you configure remote installation of a security application. In Microsoft Management Console (MMC) based Administration Console, this option is available in the Remote Installation Wizard. In Kaspersky Security Center 13 Web Console, you can find this option in the Protection Deployment Wizard. When this option is enabled, Kaspersky Security Center removes incompatible applications before installing a security application on a managed device.

How-to instructions:

- Administration Console: Installing applications using Remote Installation Wizard (on page [338](#))
or
- Kaspersky Security Center 13 Web Console: Removing incompatible applications before installation (see section "Step 7. Removing incompatible applications before installation" on page [1005](#))

Removing incompatible applications through a dedicated task

To remove incompatible applications, use the **Uninstall application remotely** task. This task should be run on devices before the security application installation task. For example, in the installation task you can select **On completing another task** as the schedule type where the other task is **Uninstall application remotely**.

This method of uninstallation is useful when the security application installer cannot properly remove an incompatible application.

How-to instructions:

- Administration Console: Creating a task (on page [374](#))

Discovering networked devices

This section describes search and discovery of networked devices.

Kaspersky Security Center allows you to find devices on the basis of specified criteria. You can save search results to a text file.

The search and discovery feature allows you to find the following devices:

- Managed devices in administration groups of Kaspersky Security Center Administration Server and its secondary Administration Servers.
- Unassigned devices managed by Kaspersky Security Center Administration Server and its secondary Administration Servers.

In this chapter

Device selections.....	1037
Scenario: Discovering networked devices.....	1038
Device discovery.....	1039
Device tags.....	1046
Application tags.....	1052

Device selections

Device selections are a tool for filtering devices according to specific conditions. You can use device selections to manage several devices: for example, to view a report about only these devices or to move all of these devices to another group.

Kaspersky Security Center provides a broad range of *predefined selections* (for example, **Devices with Critical status, Protection is disabled, Active threats are detected**). Predefined selections cannot be deleted. You can also create and configure additional *user-defined selections*.

In user-defined selections, you can set the search scope and select all devices, managed devices, or unassigned devices. Search parameters are specified in the conditions. In the device selection you can create several conditions with different search parameters. For example, you can create two conditions and specify different IP ranges in each of them. If several conditions are specified, a selection displays the devices that meet any of the conditions. By contrast, search parameters within a condition are superimposed. If both an IP range and the name of an installed application are specified in a condition, only those devices will be displayed where both the application is installed and the IP address belongs to the specified range.

► To view the device selection:

1. Go to **DEVICES** → **DEVICE SELECTIONS** or **DISCOVERY & DEPLOYMENT** → **DEVICE SELECTIONS** section.
2. In the selection list, click the name of the relevant selection.

The device selection result is displayed.

See also:

Using event selections.....	1289
Scenario: Installation and initial setup of Kaspersky Security Center 13 Web Console	962

Scenario: Discovering networked devices

You must perform device discovery before installation of the security applications. When all networked devices are discovered, you can receive information about them and manage them through policies. Regular network polls are needed to discover if there are any new devices and whether previously discovered devices are still on the network.

Discovery of networked devices proceeds in stages:

a. Initial device discovery

The Quick Start Wizard guides you through initial device discovery (see section "Step 13. Device discovery" on page [277](#)), and helps you find networked devices such as computers, tablets, and mobile phones. You can also perform device discovery manually (see section "Device discovery" on page [304](#)).

b. Configuring future polls

Decide which type(s) of discovery (see section "Device discovery" on page [304](#)) you want to use regularly. Make sure that this type is enabled and that the poll schedule meets the needs of your organization. When configuring the poll schedule, use the recommendations for network polling frequency.

c. Setting up rules for adding discovered devices to administration groups (optional)

If new devices appear on your network, they are discovered during regular polls and are automatically included in the **Unassigned devices** group. If you want, you can set up the rules for automatically moving these devices (see section "Device moving rules" on page [401](#)) to the **Managed devices** group. You can also establish retention rules (see section "Configuring retention rules for unassigned devices" on page [311](#)).

If you skip this rule-setting stage, all the newly discovered devices go to the **Unassigned devices** group and stay there. If you want, you can move these devices to the **Managed devices** group manually. If you move the devices to the **Managed devices** group manually, you can analyze information about each device and decide whether you want to move it to an administration group, and, if so, to which group.

Results

Completion of the scenario yields the following:

- Kaspersky Security Center Administration Server discovers the devices that are on the network and provides you with information about them.
- Future polls are set up and are conducted according to the specified schedule.

The newly discovered devices are arranged according to the configured rules. (Or, if no rules are configured, the devices stay in the **Unassigned devices** group).

Device discovery

This section describes the types of device discovery available in Kaspersky Security Center and provides information using each type.

The Administration Server receives information about the structure of the network and devices on this network through regular polling. The information is recorded to the Administration Server database. Administration Server can use the following types of polling:

- **Windows network polling.** The Administration Server can perform two kinds of Windows network poll: quick and full. During a quick poll, the Administration Server only retrieves information from the list of the NetBIOS names of devices in all network domains and workgroups. During a full poll, more information is requested from each client device, such as operating system name, IP address, DNS name, and NetBIOS name. By default, both quick poll and full poll are enabled. Windows network polling may fail to discover devices, for example, if the ports UDP 137, UDP 138, TCP 139 are closed on the router or by the firewall.
- **Active Directory polling.** The Administration Server retrieves information about the Active Directory unit structure and about DNS names of the devices from Active Directory groups. By default, this type of polling is enabled. We recommend that you use Active Directory polling if you use Active directory; otherwise, the Administration Server does not discover any devices. If you use Active Directory but some of the networked devices are not listed as members, these devices cannot be discovered by Active Directory polling.
- **IP range polling.** The Administration Server polls the specified IP ranges using ICMP packets and compiles a complete set of data on devices within those IP ranges. By default, this type of polling is disabled. It is not recommended to use this type of polling if you use Windows network polling and/or Active Directory polling.

If you set up and enabled device moving rules (on page [401](#)), the newly discovered devices are automatically included in the **Managed devices** group. If no moving rules have been enabled, the newly discovered devices are automatically included in the **Unassigned devices** group.

You can modify device discovery settings for each type. For example, you may want to modify the polling schedule or to set whether to poll the entire Active Directory forest or only a specific domain.

See also:

Scenario: Discovering networked devices	303
Windows network polling	1039
Active Directory polling	1041
IP range polling	1042
Adding and modifying an IP range	1044
Configuring retention rules for unassigned devices	1045

Windows network polling

About Windows network polling

During a quick poll, the Administration Server only retrieves information from the list of the NetBIOS names of devices in all network domains and workgroups. During a full poll, the following information is requested from each client device:

- Operating system name
- IP address
- DNS name
- NetBIOS name

Both quick polls and full polls require the following:

- Ports UDP 137/138, TCP 139, UDP 445, TCP 445 must be available in the network.
- The Microsoft Computer Browser service must be used, and the master browser computer must be enabled on the Administration Server.
- The Microsoft Computer Browser service must be used, and the master browser computer must be enabled on the client devices:
 - On at least one device, if the number of networked devices does not exceed 32.
 - On at least one device for each 32 networked devices.

The full poll can run only if the quick poll has run at least once.

Viewing and modifying the settings for Windows network polling

► *To modify the properties of Windows network polling:*

1. Go to **DISCOVERY & DEPLOYMENT** → **DISCOVERY** → **WINDOWS DOMAINS**.
2. Click the **Properties** button.
The Windows domain properties window opens.
3. Enable or disable Windows network polling by using the **Enable Windows network polling** toggle button.
4. Configure the poll schedule. By default, the quick polling runs every 15 minutes and the full polling runs every 60 minutes.

Polling schedule options:

- **Every N days**

The polling runs regularly, with the specified interval in days, starting from the specified date and time.

By default, the polling runs every day, starting from the current system date and time.

- **Every N minutes**

The polling runs regularly, with the specified interval in minutes, starting from the specified time.

- **By days of week**

The polling runs regularly, on the specified days of week, and at the specified time.

- **Every month on specified days of selected weeks**

The polling runs regularly, on the specified days of each month, and at the specified time.

- **Run missed tasks**

If the Administration Server is switched off or unavailable during the time for which the poll is scheduled, the Administration Server can either start the poll immediately after it is switched on, or wait for the next time for which the poll is scheduled.

If this option is enabled, the Administration Server starts polling immediately after it is switched on.

If this option is disabled, the Administration Server waits for the next time for which the polling is scheduled.

By default, this option is disabled.

5. Click the **Save** button.

The properties are saved and applied to all of the discovered Windows domains and workgroups.

Running the poll manually

► *To run the poll immediately,*

Click **Start quick poll** or **Start full poll**.

When the polling is complete, you can view the list of discovered devices on the **WINDOWS DOMAINS** page by selecting the check box next to a domain name, and then clicking the **Devices** button.

Active Directory polling

Use Active Directory polling if you use Active Directory; otherwise, it is recommended to use other poll types. If you use Active Directory but some of the networked devices are not listed as members, these devices cannot be discovered by using Active Directory polling.

Kaspersky Security Center sends a request to the domain controller and receives the Active Directory device structure. Active Directory polling is performed hourly.

Viewing and modifying the settings for Active Directory polling

► *To view and modify the settings for Active Directory polling:*

1. Go to **DISCOVERY & DEPLOYMENTy & Deployment** → **DISCOVERY** → **ACTIVE DIRECTORY**.
2. Click the **Properties** button.

The Active Directory properties window opens.

3. In the Active Directory properties window, you can configure the following settings:

- a. Turn Active Directory polling on or off by using the toggle button.
- b. Change the polling schedule.

The default period is one hour. The data received at the next polling completely replaces the old data.

- c. Configure advanced settings to select the polling scope:
 - Active Directory domain to which the Kaspersky Security Center belongs
 - Domain forest to which the Kaspersky Security Center belongs
 - Specified list of Active Directory domains

To add a domain to the polling scope, select a domain option, click the **Add** button, and then specify the address of the domain controller and the name and password of the account for accessing it.

4. To apply the new settings, click the **Save** button.

The new settings are applied to the Active Directory polling.

Running the poll manually

- ▶ *To run the poll immediately,*

click **Start poll**.

Viewing the results of Active Directory polling

- ▶ *To view the results of Active Directory polling:*

1. Go to **DISCOVERY & DEPLOYMENT** → **DISCOVERY** → **ACTIVE DIRECTORY**.

The list of discovered organizational units is displayed.

2. If you want, select an organizational unit, and then click the **Devices** button.

The list of devices in the organizational unit is displayed.

You can search the list and filter the results.

IP range polling

Kaspersky Security Center attempts to perform reverse name resolution for every address from the specified range to a DNS name using standard DNS requests. If this operation succeeds, the server sends an `ICMP ECHO REQUEST` (the same as the ping command) to the received name. If the device responds, the information about it is added to the Kaspersky Security Center database. The reverse name resolution is necessary to exclude the network devices that can have an IP address but are not computers, for example, network printers or routers.

This polling method relies upon a correctly configured local DNS service. It must have a reverse lookup zone. If this zone is not configured, IP subnet polling will yield no results. In the networks where Active Directory is used, such a zone is maintained automatically. But in these networks, IP subnet polling does not provide more information than Active Directory polling. Moreover, administrators of small networks often do not configure the reverse lookup zone because it is not necessary for the work of many network services. For these reasons, IP subnet polling is disabled by default.

Initially, Kaspersky Security Center gets IP ranges for polling from the network settings of the device on which it is installed. If the device address is 192.168.0.1 and the subnet mask is 255.255.255.0, Kaspersky Security Center includes the network 192.168.0.0/24 in the list of polling address automatically. Kaspersky Security Center polls all addresses from 192.168.0.1 to 192.168.0.254.

It is not recommended to use IP range polling if you use Windows network polling and/or Active Directory polling.

Viewing and modifying the settings for IP range polling

► *To view and modify the properties of IP range polling:*

1. Go to **DISCOVERY & DEPLOYMENT** → **DISCOVERY** → **IP RANGES**.
2. Click the **Properties** button.

The IP polling properties window opens.

3. Enable or disable IP polling by using the **Allow polling** toggle button.
4. Configure the poll schedule. By default, IP polling runs every 420 minutes (seven hours).

When specifying the polling interval, make sure that this setting does not exceed the value of the IP address lifetime parameter (see section "Adding and modifying an IP range" on page [1044](#)). If an IP address is not verified by polling during the IP address lifetime, this IP address is automatically removed from the polling results. By default, the life span of the polling results is 24 hours, because dynamic IP addresses (assigned using Dynamic Host Configuration Protocol (DHCP)) change every 24 hours.

Polling schedule options:

- **Every N days**

The polling runs regularly, with the specified interval in days, starting from the specified date and time.

By default, the polling runs every day, starting from the current system date and time.

- **Every N minutes**

The polling runs regularly, with the specified interval in minutes, starting from the specified time.

- **By days of week**

The polling runs regularly, on the specified days of week, and at the specified time.

- **Every month on specified days of selected weeks**

The polling runs regularly, on the specified days of each month, and at the specified time.

- **Run missed tasks**

If the Administration Server is switched off or unavailable during the time for which the poll is scheduled, the Administration Server can either start the poll immediately after it is switched on, or wait for the next time for which the poll is scheduled.

If this option is enabled, the Administration Server starts polling immediately after it is switched on.

If this option is disabled, the Administration Server waits for the next time for which the polling is scheduled.

By default, this option is disabled.

5. Click the **Save** button.

The properties are saved and applied to all IP ranges.

Running the poll manually

► *To run the poll immediately,*

click **Start poll**.

Adding and modifying an IP range

Initially, Kaspersky Security Center gets IP ranges for polling from the network settings of the device on which it is installed. If the device address is 192.168.0.1 and the subnet mask is 255.255.255.0, Kaspersky Security Center includes the network 192.168.0.0/24 in the list of polling address automatically. Kaspersky Security Center polls all addresses from 192.168.0.1 to 192.168.0.254. You can modify the automatically defined IP ranges or add custom IP ranges.

► *To add a new IP range:*

1. Go to **DISCOVERY & DEPLOYMENT** → **DISCOVERY** → **IP RANGES**.

2. To add a new IP range, click the **Add** button.

3. In the window that opens, specify the following settings:

- **IP range name**

A name of the IP range. You might want to specify the IP range itself as its name, for example, "192.168.0.0/24".

- **IP interval or subnet address and mask**

Set the IP range by specifying either the start and end IP addresses or the subnet address and subnet mask. You can also select one of the already existing IP ranges by clicking the **Browse** button.

- **IP address lifetime (hours)**

When specifying this parameter make sure that it exceeds the polling interval set in the polling schedule (see section "IP range polling" on page [1042](#)). If an IP address is not verified by polling during the IP address lifetime, this IP address is automatically removed from the polling results. By default, the life span of the polling results is 24 hours, because dynamic IP addresses (assigned using Dynamic Host Configuration Protocol (DHCP)) change every 24 hours.

4. Select **Enable IP range polling** if you want to poll the subnet or interval that you have added. Otherwise, the subnet or interval that you have added will not be polled.

5. Click the **Save** button.

The new IP range is added to the list of IP ranges.

You can run polling of each IP range separately by using the **Start poll** button. When the polling is complete, you can view the list of discovered devices by using the **Devices** button. By default, the life span of the polling results is 24 hours and it is equal to the IP address lifetime setting.

► *To add a subnet to an existing IP range:*

1. Go to **DISCOVERY & DEPLOYMENT** → **DISCOVERY** → **IP RANGES**.

2. Click the name of the IP range to which you want to add a subnet.

3. In the window that opens, click the **Add** button.

4. Specify a subnet by using either its address and mask, or by using the first and last IP address in the IP range. Or, add an existing subnet by clicking the **Browse** button.
5. Click the **Save** button.

The new subnet is added to the IP range.

6. Click the **Save** button.

The new settings of the IP range are saved.

You can add as many subnets as you need. Named IP ranges are not allowed to overlap, but unnamed subnets inside an IP range have no such restrictions. You can enable and disable polling independently for every IP range.

Configuring retention rules for unassigned devices

After Windows network polling is complete, the found devices are placed into subgroups of the Unassigned devices administration group. This administration group can be found at **DISCOVERY & DEPLOYMENT** → **DISCOVERY** → **WINDOWS DOMAINS**. The **WINDOWS DOMAINS** folder is the parent group. It contains child groups named after the corresponding domains and workgroups that have been found during the poll. The parent group may also contain the administration group of mobile devices. You can configure the retention rules of the unassigned devices for the parent group and for each of the child groups. The retention rules do not depend on the device discovery settings and work even if the device discovery is disabled.

► *To configure retention rules for unassigned devices:*

1. Go to **DISCOVERY & DEPLOYMENT** → **DISCOVERY** → **WINDOWS DOMAINS**.
2. Do one of the following:

- To configure settings of the parent group, click the **Properties** button.

The Windows domain properties window opens.

- To configure settings of a child group, click its name.

The child group properties window opens.

3. Configure the following settings:

- **Remove the device from the group if it has been inactive for longer than (days)**

If this option is enabled, you can specify the time interval after which the device is automatically removed from the group. By default, this option is also distributed to the child groups. The default time interval is 7 days.

By default, this option is enabled.

- **Inherit from parent group**

If this option is enabled, the retention period for the devices in the current group is inherited from the parent group and cannot be changed.

This option is available only for child groups.

By default, this option is enabled.

- **Force inheritance in child groups**

The setting values will be distributed to child groups but in the properties of the child groups these settings are locked.

By default, this option is disabled.

4. Click the **Accept** button.

Your changes are saved and applied.

Device tags

This section describes device tags, and provides instructions for creating and modifying them as well as for tagging devices manually or automatically.

See also:

Application tags	1052
About device tags	1046
Creating a device tag.....	1047
Renaming a device tag	1047
Deleting a device tag	1047
Viewing devices to which a tag is assigned.....	1048
Viewing tags assigned to a device	1048
Tagging a device manually	1048
Removing an assigned tag from a device	1049
Viewing rules for tagging devices automatically	1049
Editing a rule for tagging devices automatically	1049
Creating a rule for tagging devices automatically.....	1050
Running rules for auto-tagging devices	1051
Deleting a rule for tagging devices automatically	1051

About device tags

Kaspersky Security Center allows you to *tag* devices. A tag is the label of a device that can be used for grouping, describing, or finding devices. Tags assigned to devices can be used for creating selections (see section "Device selections" on page [1037](#)), for finding devices, and for distributing devices among administration groups (on page [49](#)).

You can tag devices manually or automatically. You may use manual tagging when you want to tag an individual device. Auto-tagging is performed by Kaspersky Security Center in accordance with the specified tagging rules.

Devices are tagged automatically when specified rules are met. An individual rule corresponds to each tag. Rules are applied to the network properties of the device, operating system, applications installed on the device, and

other device properties. For example, if you have a hybrid infrastructure of physical machines, Amazon EC2 instances, and Microsoft Azure virtual machines, you can set up a rule that will assign the [Azure] tag to all Microsoft Azure virtual machines. Then, you can use this tag when creating a device selection; this will help you sort all Microsoft Azure virtual machines and assign them a task.

A tag is automatically removed from a device in the following cases:

- When the device stops meeting conditions of the rule that assigns the tag.
- When the rule that assigns the tag is disabled or deleted.

The list of tags and the list of rules on each Administration Server are independent of all other Administration Servers, including a primary Administration Server or subordinate virtual Administration Servers. A rule is applied only to devices from the same Administration Server on which the rule is created.

See also:

Scenario: Installation and initial setup of Kaspersky Security Center 13 Web Console[962](#)

Creating a device tag

► *To create a device tag:*

1. Go to **DEVICES**, select **TAGS** → **DEVICE TAGS** in the drop-down list.
2. Click **Add**.
A new tag window opens.
3. In the **Tag** field, enter the tag name.
4. Click **Save** to save the changes.

The new tag appears in the list of device tags.

Renaming a device tag

► *To rename a device tag:*

1. Go to **DEVICES**, select **TAGS** → **DEVICE TAGS** in the drop-down list.
2. Click the name of the tag that you want to rename.
A tag properties window opens.
3. In the **Tag** field, change the tag name.
4. Click **Save** to save the changes.

The updated tag appears in the list of device tags.

Deleting a device tag

► *To delete a device tag:*

1. Go to **DEVICES**, select **TAGS** → **DEVICE TAGS** in the drop-down list.

2. In the list, select the radio button next to the device tag that you want to delete.
3. Click the **Delete** button.
4. In the window that opens, click **Yes**.

The device tag is deleted. The deleted tag is automatically removed from all of the devices to which it was assigned.

The tag that you have deleted is not removed automatically from auto-tagging rules. After the tag is deleted, it will be assigned to a new device only when the device first meets the conditions of a rule that assigns the tag.

Viewing devices to which a tag is assigned

► *To view devices to which a tag is assigned:*

1. Go to **DEVICES**, select **TAGS** → **DEVICE TAGS** in the drop-down list.
 2. Click the **View devices** link next to the tag for which you want to view assigned devices.
- If you do not see the **View devices** link next to a tag, the tag is not assigned to any devices.

The list of devices that appears shows only those devices to which the tag is assigned.

To return to the list of device tags, click the **Back** button of your browser.

Viewing tags assigned to a device

► *To view tags assigned to a device:*

1. Go to **DEVICES** → **MANAGED DEVICES**.
2. Click the name of the device whose tags you want to view.
3. In the device properties window that opens, click the **Tags** tab.

The list of tags assigned to the selected device is displayed.

You can assign another tag (see section "Tagging a device manually" on page [1048](#)) to the device or remove an already assigned tag (see section "Removing an assigned tag from a device" on page [1049](#)). You can also see all device tags that exist on the Administration Server.

Tagging a device manually

► *To assign a tag to a device manually:*

1. View tags assigned to the device to which you want to assign another tag (see section "Viewing tags assigned to a device" on page [1048](#)).
2. Click **Add**.
3. In the window that opens, do either of the following:
 - To create and assign a new tag, select **Create new tag**, and then specify the name of the new tag.

- To select an existing tag, select **Assign existing tag**, and then select the necessary tag in the drop-down list.
4. Click **OK** to apply the changes.
 5. Click **Save** to save the changes.

The selected tag is assigned to the device.

Removing an assigned tag from a device

► *To remove a tag from a device:*

1. View tags assigned to the device from which you want to remove a tag. (see section "Viewing tags assigned to a device" on page [1048](#))
2. Select the check box next to the tag that you want to remove.
3. Click the **Unassign tag** button.
4. In the window that opens, click **Yes**.

The tag is removed from the device.

The unassigned device tag is not deleted. If you want, you can delete it manually (see section "Deleting a device tag" on page [1047](#)).

Viewing rules for tagging devices automatically

► *To view rules for tagging devices automatically,*

Do any of the following:

- Go to **DEVICES** → **TAGS** → **AUTO-TAGGING RULES**.
- Go to **DEVICES** → **TAGS**, and then click the **Set up auto-tagging rules** link.
- View tags assigned to a device (see section "Viewing tags assigned to a device" on page [1048](#)) and then click the **Settings** button.

The list of rules for auto-tagging devices appears.

Editing a rule for tagging devices automatically

► *To edit a rule for tagging devices automatically:*

1. View rules for tagging devices automatically (see section "Viewing rules for tagging devices automatically" on page [1049](#)).
2. Click the name of the rule that you want to edit.

A rule settings window opens.

3. Edit the general properties of the rule:
 - a. In the **Rule name** field, change the rule name.

The name cannot be more than 256 characters long.

- b. Do any of the following:
 - Enable the rule by switching the toggle button to **Rule enabled**.
 - Disable the rule by switching the toggle button to **Rule disabled**.
4. Do any of the following:
 - If you want to add a new condition, click the **Add** button, and specify the settings of the new condition (see section "Creating a rule for tagging devices automatically" on page [1050](#)) in the window that opens.
 - If you want to edit an existing condition, click the name of the condition that you want to edit, and then edit the condition settings (see section "Creating a rule for tagging devices automatically" on page [1050](#)).
 - If you want to delete a condition, select the check box next to the name of the condition that you want to delete, and then click **Delete**.
5. Click **OK** in the conditions settings window.
6. Click **Save** to save the changes.

The edited rule is shown in the list.

Creating a rule for tagging devices automatically

► *To create a rule for tagging devices automatically:*

1. View rules for tagging devices automatically (see section "Viewing rules for tagging devices automatically" on page [1049](#)).
2. Click **Add**.

A new rule settings window opens.
3. Configure the general properties of the rule:
 - a. In the **Rule name** field, enter the rule name.

The name cannot be more than 256 characters long.
 - b. Do either of the following:
 - Enable the rule by switching the toggle button to **Rule enabled**.
 - Disable the rule by switching the toggle button to **Rule disabled**.
 - c. In the **Tag** field, enter the new device tag name or select one of the existing device tags from the list.

The name cannot be more than 256 characters long.
4. In the conditions section, click the **Add** button to add a new condition.

A new condition settings window opens.
5. Enter the condition name.

The name cannot be more than 256 characters long. The name must be unique within a rule.
6. Set up the triggering of the rule according to the following conditions. You can select multiple conditions.
 - **Network**—Network properties of the device, such as the device name on the Windows network, or device inclusion in a domain or an IP subnet.

- **Applications**—Presence of Network Agent on the device, operating system type, version, and architecture.
 - **Virtual machines**—Device belongs to a specific type of virtual machine.
 - **Active Directory**—Presence of the device in an Active Directory organizational unit and membership of the device in an Active Directory group.
 - **Applications registry**—Presence of applications of different vendors on the device.
7. Click **OK** to save the changes.

If necessary, you can set multiple conditions for a single rule. In this case, the tag will be assigned to a device if it meets at least one condition.

8. Click **Save** to save the changes.

The newly created rule is enforced on devices managed by the selected Administration Server. If the settings of a device meet the rule conditions, the device is assigned the tag.

Later, the rule is applied in the following cases:

- Automatically and periodically, depending on the server workload
- After you edit the rule (see section "Editing a rule for tagging devices automatically" on page [1049](#))
- When you run the rule manually (see section "Running rules for auto-tagging devices" on page [1051](#))
- After the Administration Server detects a change in the settings of a device that meets the rule conditions or the settings of a group that contains such device

You can create multiple tagging rules. A single device can be assigned multiple tags if you have created multiple tagging rules and if the respective conditions of these rules are met simultaneously. You can view the list of all assigned tags (see section "Viewing tags assigned to a device" on page [1048](#)) in the device properties.

Running rules for auto-tagging devices

When a rule is run, the tag specified in properties of this rule is assigned to devices that meet conditions specified in properties of the same rule. You can run only active rules.

► *To run rules for auto-tagging devices:*

1. View rules for tagging devices automatically (see section "Viewing rules for tagging devices automatically" on page [1049](#)).
2. Select check boxes next to active rules that you want to run.
3. Click the **Run rule** button.

The selected rules are run.

Deleting a rule for tagging devices automatically

► *To delete a rule for tagging devices automatically:*

1. View rules for tagging devices automatically (see section "Viewing rules for tagging devices automatically" on page [1049](#)).
2. Select the check box next to the rule that you want to delete.
3. Click **Delete**.

4. In the window that opens, click **Delete** again.

The selected rule is deleted. The tag that was specified in properties of this rule is unassigned from all of the devices that it was assigned to.

The unassigned device tag is not deleted. If you want, you can delete it manually (see section "Deleting a device tag" on page [1047](#)).

Application tags

This section describes application tags, and provides instructions for creating and modifying them as well as for tagging third-party applications.

See also:

Device tags	1046
About application tags	1052
Creating an application tag	1052
Renaming an application tag	1053
Assigning tags to an application	1053
Removing assigned tags from an application	1053
Deleting an application tag	1054

About application tags

Kaspersky Security Center allows you to *tag* third-party applications (applications made by software vendors other than Kaspersky). A tag is the label of an application that can be used for grouping or finding applications. A tag assigned to applications can serve as a condition in device selections (on page [1037](#)).

For example, you can create the [Browsers] tag and assign it to all browsers (Microsoft Internet Explorer, Google Chrome, Mozilla Firefox, etc.).

Creating an application tag

► *To create an application tag:*

1. Go to **OPERATIONS** → **THIRD-PARTY APPLICATIONS** → **APPLICATION TAGS**.
2. Click **Add**.
A new tag window opens.
3. Enter the tag name.
4. Click **OK** to save the changes.

The new tag appears in the list of application tags.

Renaming an application tag

► *To rename an application tag:*

1. Go to **OPERATIONS** → **THIRD-PARTY APPLICATIONS** → **APPLICATION TAGS**.
2. Select the check box next to the tag that you want to rename, and then click **Edit**.
A tag properties window opens.
3. Change the tag name.
4. Click **OK** to save the changes.

The updated tag appears in the list of application tags.

Assigning tags to an application

► *To assign one or several tags to an application:*

1. Go to **OPERATIONS** → **THIRD-PARTY APPLICATIONS** → **APPLICATIONS REGISTRY**.
2. Click the name of the application to which you want to assign tags.
3. Click the **Tags** tab.
The tab displays all application tags that exist on the Administration Server. For tags assigned to the selected application, the check box in the **Tag assigned** column is selected.
4. For tags that you want to assign, select check boxes in the **Tag assigned** column.
5. Click **Save** to save the changes.

The tags are assigned to the application.

Removing assigned tags from an application

► *To remove one or several tags from an application:*

1. Go to **OPERATIONS** → **THIRD-PARTY APPLICATIONS** → **APPLICATIONS REGISTRY**.
2. Click the name of the application from which you want to remove tags.
3. Click the **Tags** tab.
The tab displays all application tags that exist on the Administration Server. For tags assigned to the selected application, the check box in the **Tag assigned** column is selected.
4. For tags that you want to remove, clear check boxes in the **Tag assigned** column.
5. Click **Save** to save the changes.

The tags are removed from the application.

The removed application tags are not deleted. If you want, you can delete them manually (see section "Deleting an application tag" on page [1054](#)).

Deleting an application tag

► *To delete an application tag:*

1. Go to **OPERATIONS** → **THIRD-PARTY APPLICATIONS** → **APPLICATION TAGS**.
2. In the list, select the application tag that you want to delete.
3. Click the **Delete** button.
4. In the window that opens, click **OK**.

The application tag is deleted. The deleted tag is automatically removed from all of the applications to which it was assigned.

Kaspersky applications: licensing and activation

This section describes the features of Kaspersky Security Center related to working with the license keys of managed Kaspersky applications.

Kaspersky Security Center allows you to perform centralized distribution of license keys for Kaspersky applications on client devices, monitor their use, and renew licenses.

When adding a license key using Kaspersky Security Center, the settings of the license key are saved on the Administration Server. Based on this information, the application generates a license key usage report and notifies the administrator of license expirations and violation of license restrictions that are set in the properties of license keys. You can configure notifications of the use of license keys within the Administration Server settings.

See also:

Scenario: Installation and initial setup of Kaspersky Security Center 13 Web Console	962
Licensing of managed applications	1054
Adding a license key to the Administration Server repository	1056
Deploying a license key to client devices	1057
Automatic distribution of a license key	1057
Viewing information about license keys in use	1058
Deleting a license key from the repository.....	1058
Revoking consent with an End User License Agreement	1059

Licensing of managed applications

The Kaspersky applications installed on managed devices must be licensed by applying a key file or activation code to each of the applications. A key file or activation code can be deployed in the following ways:

- Automatic deployment
- The installation package of a managed application

- The Add license key task for a managed application
- Manual activation of a managed application

Automatic deployment

If you use different managed applications and you have to deploy a specific key file or activation code to devices, opt for other ways of deploying that activation code or key file.

Kaspersky Security Center allows you to automatically deploy available license keys to devices. For example, three license keys are stored in the Administration Server repository. You have enabled the **Deploy license key automatically** option for all three license keys. A Kaspersky security application—for example, Kaspersky Endpoint Security for Windows—is installed on the organization's devices. A new device is discovered to which a license key must be deployed. The application determines, for instance, that two of the license keys from the repository can be deployed to the device: license key named *Key_1* and license key named *Key_2*. One of these license keys is deployed to the device. In this case, it cannot be predicted which of the two license keys will be deployed to the device because automatic deployment of license keys does not provide for any administrator activity.

When a license key is deployed, the devices are recounted for that license key. You must make sure that the number of devices to which the license key was deployed does not exceed the license limit. If the number of devices exceeds the license limit (see section "Events of the licensing limit exceeded" on page [329](#)), all devices that were not covered by the license will be assigned *Critical* status.

Before deployment, the key file or activation code must be added to the Administration Server repository.

How-to instructions:

- Administration Console:
 - Adding a license key to the Administration Server repository (on page [360](#))
 - Automatic distribution of a license key (on page [361](#))
- or
- Kaspersky Security Center 13 Web Console:
 - Adding a license key to the Administration Server repository (on page [1056](#))
 - Automatic distribution of a license key (on page [1057](#))

Adding a key file or activation code to the installation package of a managed application

For security reasons, this option is not recommended. A key file or activation code added to an installation package may be compromised.

If you install a managed application using an installation package, you can specify an activation code or key file in this installation package or in the policy of the application. The license key will be deployed to managed devices at the next synchronization of the device with the Administration Server.

How-to instructions:

- Administration Console:

- Creating an installation package (on page [344](#))
- Installing applications on client devices (on page [719](#))

or

- Kaspersky Security Center 13 Web Console: Adding a license key to an installation package (see section "Step 2. Selecting a method for distribution of key file or activation code" on page [1002](#))

Deployment through the Add license key task for a managed application

If you opt for using the Add license key task for a managed application, you can select the license key that must be deployed to devices and select the devices in any convenient way—for example, by selecting an administration group or a device selection.

Before deployment, the key file or activation code must be added to the Administration Server repository.

How-to instructions:

- Administration Console:
 - Adding a license key to the Administration Server repository (on page [360](#))
 - Deploying a license key to client devices (on page [361](#))or
- Kaspersky Security Center 13 Web Console:
 - Adding a license key to the Administration Server repository (on page [1056](#))
 - Deploying a license key to client devices (on page [1057](#))

Adding an activation code or a key file manually to the devices

You can activate the installed Kaspersky application locally, by using the tools provided in the application interface. Please refer to the documentation of the installed application.

Adding a license key to the Administration Server repository

► *To add a license key to the Administration Server repository:*

1. Go to **OPERATIONS** → **LICENSING** → **KASPERSKY LICENSES**.
2. Click the **Add** button.
3. Choose what you want to add:
 - **Add key file**
Click the **Select key file** button and browse to the .key file that you want to add.
 - **Enter activation code**
Specify the activation code in the text field and click the **Send** button.
4. Click the **Close** button.

The license key or several license keys are added to the Administration Server repository.

See also:

Scenario: Installation and initial setup of Kaspersky Security Center 13 Web Console [962](#)

Deploying a license key to client devices

Kaspersky Security Center 13 Web Console allows you to distribute a license key to client devices through the License key distribution task.

► *To distribute a license key to client devices:*

1. Go to **DEVICES** → **TASKS**.
2. Click **Add**.
The New Task Wizard starts.
3. Select the application for which you want to add a license key.
4. From the **Task type** list, select **Add license key**.
5. Follow the Wizard steps.
6. If on the **Finish task creation** page you enable the **Open task details when creation is complete** option, you can modify the default task settings. If you do not enable this option, the task is created with the default settings. You can modify the default settings later, at any time.
7. Click the **Create** button.
The task is created and displayed in the list of tasks.
8. To run the task, select it in the task list and click the **Start** button.

When the task is performed, the license key is deployed to the selected devices.

Automatic distribution of a license key

Kaspersky Security Center allows automatic distribution of license keys to managed devices if they are located in the license keys repository on the Administration Server.

► *To distribute a license key to managed devices automatically:*

1. Go to **OPERATIONS** → **LICENSING** → **KASPERSKY LICENSES**.
2. Click the name of the license key that you want to distribute to devices automatically.
3. In the license key properties window that opens, switch the toggle button to **Deploy license key automatically**.
4. Click the **Save** button.

The license key will be automatically distributed as the active or reserve license key to all compatible devices.

License key distribution is performed by means of Network Agent. No reserve license key distribution tasks are created for the application.

During automatic distribution of a license key as the active or reserve license key, the licensing limit on the number of devices is taken into account. (The licensing limit is set in the properties of the license key.) If the licensing limit is reached, distribution of this license key on devices ceases automatically.

Viewing information about license keys in use

► *To view the list of the license keys added to the Administration Server repository:*

Go to **OPERATIONS** → **LICENSING** → **KASPERSKY LICENSES**.

The displayed list contains the key files and activation codes added to the Administration Server repository.

► *To view detailed information about a license key:*

1. Go to **OPERATIONS** → **LICENSING** → **KASPERSKY LICENSES**.
2. Click the name of the required license key.

In the license key properties window that opens, you can view:

- On the **General** tab—The main information about the license key
- On the **Devices** tab—The list of client devices where the license key was used for activation of the installed Kaspersky application

► *To view which license keys are deployed to a specific client device:*

1. Go to **DEVICES** → **MANAGED DEVICES**.
2. Click the name of the required device.
3. In the device properties window that opens, click the **Applications** tab.
4. Click the name of the application for which you want to view the information about the license key.
5. In the application properties window that opens, click the **General** tab, and then open the **License** section.

The main information about the active and reserve license keys is displayed.

To define the up-to-date settings of virtual Administration Server license keys, the Administration Server sends a request to Kaspersky activation servers at least once per day.

Deleting a license key from the repository

When you delete the active license key for an additional feature of Administration Server, for example Vulnerability and Patch Management (see section "Kaspersky Security Center licensing options" on page [320](#)) or Mobile Device Management (see section "Kaspersky Security Center licensing options" on page [320](#)), the corresponding feature becomes unavailable. If a reserve license key has been added, the reserve license key automatically becomes the active license key after the former active license key is deleted.

When you delete the active license key deployed to a managed device, the application will continue working on the managed device.

► *To delete a key file or activation code from the Administration Server repository:*

1. Go to **OPERATIONS** → **LICENSING** → **KASPERSKY LICENSES**.
2. Select the key file or activation code that you want to delete from the repository.
3. Click the **Delete** button.
4. Confirm the operation by clicking the **OK** button.

The selected key file or activation code is deleted from the repository.

You can add (see section "Adding a license key to the Administration Server repository" on page [1056](#)) a deleted license key again or add a new license key.

Revoking consent with an End User License Agreement

This section describes features applicable only to Kaspersky Security Center 12.1 or a later version.

If you decide to stop protecting some of your client devices, you can revoke the End User License Agreement (EULA) for any managed Kaspersky application. You must uninstall the selected application before revoking its EULA.

► *To revoke a EULA for managed Kaspersky applications:*

1. Open the Administration Server properties window and on the **General** tab select the **End User License Agreements** section.

A list of EULAs—accepted upon creation of installation packages, at the seamless installation of updates, or upon deployment of Kaspersky Security for Mobile—is displayed.

2. In the list, select the EULA that you want to revoke.

You can view the following properties of the EULA:

- Date when the EULA was accepted
- Name of the user who accepted the EULA

3. Click the acceptance date of any EULA to open its properties window that displays the following data:

- Name of the user who accepted the EULA
- Date when the EULA was accepted
- Unique identifier (UID) of the EULA
- Full text of the EULA
- List of objects (installation packages, seamless updates, mobile apps) linked to the EULA, and their respective names and types

4. In the lower part of the EULA properties window, click the **Revoke License Agreement** button.

If there exist any objects (installation packages and their respective tasks) that prevent the EULA from being revoked, the corresponding notification is displayed. You cannot proceed with revocation until you delete these objects.

In the window that opens, you are informed that you must first uninstall the Kaspersky application corresponding to the EULA.

5. Click the button to confirm revocation.

The EULA is revoked. It is no longer displayed in the list of License Agreements in the **End User License Agreements** section. The EULA properties window closes; the application is no longer installed.

Configuring network protection

This section contains information about manual configuration of policies, tasks, and other settings of Administration Server, and information about the distribution point, building an administration group structure and hierarchy of tasks, and other settings.

In this chapter

Scenario: Configuring network protection.....	1061
About device-centric and user-centric security management approaches.....	1063
Policy setup and propagation: Device-centric approach	1064
Policy setup and propagation: User-centric approach.....	1066
Manual setup of Kaspersky Endpoint Security policy.....	1068
Manual setup of the group update task for Kaspersky Endpoint Security.....	1073
Granting offline access to the external device blocked by Device Control.....	1073
Removing applications or software updates remotely.....	1074
Rolling back an object to a previous revision	1076
Tasks	1078
Managing client devices	1090
Policies and policy profiles.....	1110
Data encryption and protection.....	1133
Users and user roles.....	1137
Kaspersky Security Network (KSN).....	1168

Scenario: Configuring network protection

The Quick Start Wizard creates policies and tasks with the default settings. These settings may turn out to be sub-optimal or even disallowed by the organization. Therefore, we recommend that you fine-tune these policies and tasks and create other policies and tasks, if they are necessary for your network.

Prerequisites

Before you start, make sure that you have done the following:

- Installed Kaspersky Security Center 13 Administration Server (see section "Installing Kaspersky Security Center (Standard installation)" on page [966](#))
- Installed Kaspersky Security Center 13 Web Console (see section "Installing Kaspersky Security Center 13 Web Console" on page [967](#)) (optional)
- Completed the Kaspersky Security Center main installation scenario (see section "Main installation scenario" on page [59](#))
- Completed the Quick Start Wizard (see section "Quick Start Wizard (Kaspersky Security Center 13 Web Console)" on page [993](#)) or manually created the following policies and tasks in the **Managed devices** administration group:
 - Policy of Kaspersky Endpoint Security
 - Group task for updating Kaspersky Endpoint Security
 - Policy of Network Agent
 - *Find vulnerabilities and required updates* task

Configuring network protection proceeds in stages:

a. Setup and propagation of Kaspersky application policies and policy profiles

To configure and propagate settings for Kaspersky applications installed on the managed devices, you can use two different security management approaches (see section "About device-centric and user-centric security management approaches" on page [367](#))—device-centric or user-centric. These two approaches can also be combined. To implement device-centric security management (see section "Policy setup and propagation: Device-centric approach" on page [365](#)), you can use tools provided in Microsoft Management Console-based Administration Console or Kaspersky Security Center 13 Web Console. User-centric security management (see section "Policy setup and propagation: User-centric approach" on page [1066](#)) can be implemented through Kaspersky Security Center 13 Web Console only.

b. Configuring tasks for remote management of Kaspersky applications

Check the tasks created with the Quick Start Wizard and fine-tune them, if necessary.

How-to instructions:

- Administration Console:
 - Setting up the group task for updating Kaspersky Endpoint Security (see section "Manual setup of the group update task for Kaspersky Endpoint Security" on page [371](#))
 - Scheduling the Find vulnerabilities and required updates task (on page [372](#))

or

- Kaspersky Security Center 13 Web Console:
 - Setting up the group task for updating Kaspersky Endpoint Security (see section "Manual setup of the group update task for Kaspersky Endpoint Security" on page [1073](#))
 - Find vulnerabilities and required updates task settings (on page [1219](#))

If necessary, create additional tasks (see section "Managing tasks" on page [373](#)) to manage the Kaspersky applications installed on the client devices.

c. Evaluating and limiting the event load on the database

Information about events during the operation of managed applications is transferred from a client device and registered in the Administration Server database. To reduce the load on the Administration Server, evaluate and limit the maximum number of events that can be stored in the database.

How-to instructions:

- Administration Console: Setting the maximum number of events (see section "Setting the maximum number of events in the event repository" on page [372](#))

or

- Kaspersky Security Center 13 Web Console: Setting the maximum number of events (see section "Setting the maximum number of events in the event repository" on page [1008](#))

Results

Upon completion of this scenario, your network will be protected by configuration of Kaspersky applications, tasks, and events received by the Administration Server:

- The Kaspersky applications are configured according to the policies and policy profiles.
- The applications are managed through a set of tasks.
- The maximum number of events that can be stored in the database is set.

When the network protection configuration is complete, you can proceed to configuring regular updates to Kaspersky databases and applications (see section "Scenario: Regular updating Kaspersky databases and applications" on page [1174](#)).

See also:

Scenario: Installation and initial setup of Kaspersky Security Center 13 Web Console	962
Scenario: Regular updating Kaspersky databases and applications	1174

About device-centric and user-centric security management approaches

You can manage security settings from the standpoint of device features and from the standpoint of user roles. The first approach is called *device-centric security management* and the second is called *user-centric security management*. To apply different application settings to different devices you can use either or both types of management in combination. To implement device-centric security management, you can use tools provided in Microsoft Management Console-based Administration Console or Kaspersky Security Center 13 Web Console. User-centric security management can be implemented through Kaspersky Security Center 13 Web Console only.

Device-centric security management (see section "Policy setup and propagation: Device-centric approach" on page [365](#)) enables you to apply different security application settings to managed devices depending on device-specific features. For example, you can apply different settings to devices allocated in different administration groups. You can also differentiate the devices by usage of those devices in Active Directory, or their hardware specifications.

User-centric security management (see section "Policy setup and propagation: User-centric approach" on page [1066](#)) enables you to apply different security application settings to different user roles. You can create several user roles, assign an appropriate user role to each user, and define different application settings to the devices owned by users with different roles. For example, you may want to apply different application settings to devices of accountants and human resources (HR) specialists. As a result, when user-centric security management is implemented, each department—accounts department and HR department—has its own settings configuration for

Kaspersky applications. A settings configuration defines which application settings can be changed by users and which are forcibly set and locked by the administrator.

By using user-centric security management you can apply specific application settings to individual users. This may be required when an employee has a unique role in the company or when you want to monitor security incidents related to devices of a specific person. Depending on the role of this employee in the company, you can expand or limit the rights of this person to change application settings. For example, you might want to expand the rights of a system administrator who manages client devices in a local office.

You can also combine the device-centric and user-centric security management approaches. For example, you can configure a specific application policy for each administration group, and then create policy profiles (see section "Policy profiles in a hierarchy of policies" on page [1113](#)) for one or several user roles of your enterprise. In this case the policies and policy profiles are applied in the following order:

1. The policies created for device-centric security management are applied.
2. They are modified by the policy profiles according to the policy profile priorities.
3. The policies are modified by the policy profiles associated with user roles (see section "Associating policy profiles with roles" on page [1167](#)).

Policy setup and propagation: Device-centric approach

When you complete this scenario, the applications will be configured on all of the managed devices in accordance with the application policies and policy profiles that you define.

Prerequisites

Before you start, make sure that you have successfully installed Kaspersky Security Center Administration Server (see section "Installing Kaspersky Security Center (Standard installation)" on page [966](#)) and Kaspersky Security Center 13 Web Console (see section "Installing Kaspersky Security Center 13 Web Console" on page [967](#)) (optional). If you installed Kaspersky Security Center 13 Web Console, you might also want to consider user-centric (see section "Policy setup and propagation: User-centric approach" on page [1066](#)) security management as an alternative or additional option to the device-centric approach.

Stages

The scenario of device-centric management of Kaspersky applications consists of the following steps:

a. Configuring application policies

Configure settings for Kaspersky applications installed on the managed devices by creating a policy (see section "Creating a policy" on page [1118](#)) for each application. The set of policies will be propagated to the client devices.

When you configure the protection of your network in Quick Start Wizard, Kaspersky Security Center creates the default policy for Kaspersky Endpoint Security for Windows. If you completed the configuration process by using this Wizard, you do not have to create a new policy for this application. Proceed to the manual setup of Kaspersky Endpoint Security policy (on page [368](#)).

If you have a hierarchical structure of several Administration Servers and/or administration groups, the secondary Administration Servers and child administration groups inherit the policies from the primary Administration Server by default. You can force the inheritance by the child groups and secondary Administration Servers to prohibit any modifications of the settings configured in the upstream policy. If you want only part of the settings to be forcibly inherited, you can lock them in the upstream policy. The rest

unlocked settings will be available for modification in the downstream policies. The created hierarchy of policies (on page [385](#)) will allow you to effectively manage devices in the administration groups.

How-to instructions:

- Administration Console: Creating a policy (on page [388](#))

or

- Kaspersky Security Center 13 Web Console: Creating a policy (on page [1118](#))

b. Creating policy profiles (optional)

If you want devices within a single administration group to run under different policy settings, create policy profiles (see section "Policy profiles in a hierarchy of policies" on page [1113](#)) for those devices. A policy profile is a named subset of policy settings. This subset is distributed on target devices together with the policy, supplementing it under a specific condition called the *profile activation condition*. Profiles only contain settings that differ from the "basic" policy, which is active on the managed device.

By using profile activation conditions, you can apply different policy profiles, for example, to the devices located in a specific unit or security group of Active Directory, having a specific hardware configuration, or marked with specific tags (see section "About device tags" on page [1046](#)). Use tags to filter devices that meet specific criteria. For example, you can create a tag called *Windows*, mark all devices running Windows operating system with this tag, and then specify this tag as an activation condition for a policy profile. As a result, Kaspersky applications installed on all devices running Windows will be managed by their own policy profile.

How-to instructions:

- Administration Console:
 - Creating a policy profile (on page [395](#))
 - Creating a policy profile activation rule (on page [397](#))

or

- Kaspersky Security Center 13 Web Console:
 - Creating a policy profile (on page [1128](#))
 - Creating a policy profile activation rule (on page [1129](#))

c. Propagating policies and policy profiles to the managed devices

By default, the Administration Server automatically synchronizes with managed devices every 15 minutes. During the synchronization, the new or changed policies and policy profiles are propagated to the managed devices. You can circumvent auto-synchronization and run the synchronization manually by using the Force synchronization (see section "Forced synchronization" on page [646](#)) command. When synchronization is complete, the policies and policy profiles are delivered and applied to the installed Kaspersky applications.

If you use Kaspersky Security Center 13 Web Console, you can check whether the policies and policy profiles were delivered to a device. Kaspersky Security Center specifies the delivery date and time in the properties of the device.

How-to instructions:

- Administration Console: Forced synchronization (on page [646](#))

or

- Kaspersky Security Center 13 Web Console: Forced synchronization (on page [1123](#))

Results

When the device-centric scenario is complete, the Kaspersky applications are configured according to the settings specified and propagated through the hierarchy of policies.

The configured application policies and policy profiles will be applied automatically to the new devices added to the administration groups.

See also:

Main installation scenario	59
Hierarchy of Administration Servers	45
Administration groups	49
Policies.....	51
Policy profiles.....	52
Hierarchy of policies	385
About user roles.....	1137
Scenario: Configuring network protection.....	364

Policy setup and propagation: User-centric approach

This section describes the scenario of user-centric approach to the centralized configuration of Kaspersky applications installed on the managed devices. When you complete this scenario, the applications will be configured on all of the managed devices in accordance with the application policies and policy profiles that you define.

This scenario can only be implemented through Kaspersky Security Center 13 Web Console.

Prerequisites

Before you start, make sure that you have successfully installed Kaspersky Security Center Administration Server (see section "Installing Kaspersky Security Center (Standard installation)" on page [966](#)) and Kaspersky Security Center 13 Web Console (see section "Installing Kaspersky Security Center 13 Web Console" on page [967](#)), and completed the main installation scenario (on page [59](#)). You might also want to consider device-centric security management (see section "Policy setup and propagation: Device-centric approach" on page [365](#)) as an alternative or additional option to the user-centric approach. Learn more about two management approaches (see section "About device-centric and user-centric security management approaches" on page [367](#)).

Process

The scenario of user-centric management of Kaspersky applications consists of the following steps:

a. Configuring application policies

Configure settings for Kaspersky applications installed on the managed devices by creating a policy (see section "Managing policies" on page [387](#)) for each application. The set of policies will be propagated to the client devices.

When you configure the protection of your network in Quick Start Wizard, Kaspersky Security Center creates the default policy for Kaspersky Endpoint Security. If you completed the configuration process by using this Wizard, you do not have to create a new policy for this application. Proceed to the manual setup of Kaspersky Endpoint Security policy (on page [1068](#)).

If you have a hierarchical structure of several Administration Servers and/or administration groups, the secondary Administration Servers and child administration groups inherit the policies from the primary Administration Server by default. You can force the inheritance by the child groups and secondary Administration Servers to prohibit any modifications of the settings configured in the upstream policy. If you want only part of the settings to be forcibly inherited, you can lock them in the upstream policy (see section "About lock and locked settings" on page [1111](#)). The rest unlocked settings will be available for modification in the downstream policies. The created hierarchy of policies (on page [1112](#)) will allow you to effectively manage devices in the administration groups.

How-to instructions: Creating a policy (on page [1118](#))

b. Specifying owners of the devices

Assign the managed devices to the corresponding users.

How-to instructions: Assigning a user as a device owner (on page [1164](#))

c. Defining user roles typical for your enterprise

Think about different kinds of work that the employees of your enterprise typically perform. You must divide all employees in accordance with their roles. For example, you can divide them by departments, professions, or positions. After that you will need to create a user role for each group. Keep in mind that each user role will have its own policy profile containing application settings specific for this role.

d. Creating user roles

Create and configure a user role for each group of employees that you defined on the previous step or use the predefined user roles. The user roles will contain set of rights of access to the application features.

How-to instructions: Creating a user role (on page [1165](#))

e. Defining the scope of each user role

For each of the created user roles, define users and/or security groups and administration groups. Settings associated with a user role apply only to devices that belong to users who have this role, and only if these devices belong to groups associated with this role, including child groups.

How-to instructions: Editing the scope of a user role (on page [1165](#))

f. Creating policy profiles

Create a policy profile (see section "Policy profiles in a hierarchy of policies" on page [1113](#)) for each user role in your enterprise. The policy profiles define which settings will be applied to the applications installed on users' devices depending on the role of each user.

How-to instructions: Creating a policy profile (on page [1128](#))

g. Associating policy profiles with the user roles

Associate the created policy profiles with the user roles. After that: the policy profile becomes active for a user that has the specified role. The settings configured in the policy profile will be applied to the Kaspersky applications installed on the user's devices.

How-to instructions: Associating policy profiles with roles (on page [1167](#))

h. Propagating policies and policy profiles to the managed devices

By default, the Administration Server automatically synchronizes with managed devices every 15 minutes. During the synchronization, the new or changed policies and policy profiles are propagated to the managed

devices. You can circumvent auto-synchronization and run the synchronization manually by using the Force synchronization command. When synchronization is complete, the policies and policy profiles are delivered and applied to the installed Kaspersky applications.

You can check whether the policies and policy profiles were delivered to a device. Kaspersky Security Center specifies the delivery date and time in the properties of the device.

How-to instructions: Forced synchronization (on page [1123](#))

Results

When the user-centric scenario is complete, the Kaspersky applications are configured according to the settings specified and propagated through the hierarchy of policies and policy profiles.

For a new user, you will have to create a new account, assign the user one of the created user roles, and assign the devices to the user. The configured application policies and policy profiles will be automatically applied to the devices of this user.

See also:

Main installation scenario	59
Hierarchy of Administration Servers	45
Administration groups	49
Policies.....	51
Policy profiles.....	52
Hierarchy of policies	385
About user roles.....	1137
Scenario: Configuring network protection.....	364

Manual setup of Kaspersky Endpoint Security policy

This section provides recommendations on how to configure the Kaspersky Endpoint Security policy, which is created by the Quick Start Wizard of Kaspersky Security Center 13 Web Console. Setup is performed in the policy properties window.

When editing a setting, please keep in mind that you must click the lock icon above the relevant setting in order to allow using its value on a workstation.

In this section

Configuring the policy in the Advanced Threat Protection section	1069
Configuring the policy in the Essential Threat Protection section	1069
Configuring the policy in the General Settings section.....	1070
Configuring the policy in the Event configuration section.....	1071

Configuring the policy in the Advanced Threat Protection section

This section describes additional setup actions, which we recommend that you perform in the policy properties window of Kaspersky Endpoint Security for Windows, in the **Advanced Threat Protection** section.

For a full description of the settings in this section please refer to the [Kaspersky Endpoint Security for Windows documentation](#).

► *To specify recommended KSN settings:*

1. Go to **DEVICES** → **POLICIES & PROFILES**.
2. Click the policy for Kaspersky Endpoint Security for Windows.
The properties window of the selected policy opens.
3. In the policy properties, go to **Application settings** → **Advanced Threat Protection** → **Kaspersky Security Network**.
4. Make sure that the **Use KSN Proxy** option is enabled. Using KSN Proxy helps to increase the reliability of malware detection.
5. [optional] Enable use of KSN servers if the KSN Proxy service is not available. KSN servers may be located either on the side of Kaspersky (when Global KSN is used) or on the side of third parties (when Private KSN is used).
6. Click **OK**.

The recommended KSN settings are specified.

Configuring the policy in the Essential Threat Protection section

For a full description of the settings in this section please refer to the [Kaspersky Endpoint Security for Windows documentation](#).

Described below are additional setup actions, which we recommend that you perform in the policy properties window of Kaspersky Endpoint Security for Windows, in the **Essential Threat Protection** section.

Essential Threat Protection section, Firewall subsection

Check the list of networks in the policy properties. The list may not contain all networks.

► *To check the list of networks:*

1. Go to **DEVICES** → **POLICIES & PROFILES**.
2. Click the policy for Kaspersky Endpoint Security for Windows.
The properties window of the selected policy opens.
3. In the policy properties, go to **Application settings** → **Essential Threat Protection** → **Firewall**.

4. Under **Firewall settings**, click the **Networks** link.

This opens the **Network connections** window. This window displays the list of networks.

Essential Threat Protection section, File Threat Protection subsection

Enabling the scanning of network drives can place a significant load on network drives. It is more convenient to perform indirect scanning, on file servers.

► *To disable scanning of network drives:*

1. Go to **DEVICES** → **POLICIES & PROFILES**.
2. Click the policy for Kaspersky Endpoint Security for Windows.
The properties window of the selected policy opens.
3. In the policy properties, go to **Application settings** → **Essential Threat Protection** → **File Threat Protection**.
4. Under **Protection scope**, disable the **All network drives** option.
5. Click **OK**.

Scanning of network drives is disabled.

Configuring the policy in the General Settings section

For a full description of the settings in this section please refer to the Kaspersky Endpoint Security for Windows documentation.

Described below are advanced setup actions, which we recommend that you perform in the policy properties window of Kaspersky Endpoint Security for Windows, in the **General Settings** section.

General Settings section, Reports and Storage subsection

► *To disable saving information about installed software modules:*

1. Go to **DEVICES** → **POLICIES & PROFILES**.
2. Click the policy for Kaspersky Endpoint Security for Windows.
The properties window of the selected policy opens.
3. In the policy properties, go to **Application settings** → **General Settings** → **Reports and Storage**.
4. Under **Data transfer to Administration Server**, clear the **About started applications** check box if it is still selected in the top-level policy.

When this check box is selected, the Administration Server database saves information about all versions of all software modules on the networked devices. This information may require a significant amount of disk space in the Kaspersky Security Center database (dozens of gigabytes).

The information about installed software modules is no longer saved to the Administration Server database.

General Settings section, Interface subsection

If the Anti-Virus protection on the organization's network must be managed in centralized mode through Administration Console, specify the interface settings as described below.

► *To specify recommended interface settings:*

1. On the **DEVICES** tab, select **POLICIES & PROFILES**.
2. Click the policy for Kaspersky Endpoint Security for Windows.
The properties window of the selected policy opens.
3. In the policy properties, go to **Application settings** → **General Settings** → **Interface**.
4. Under **Interaction with user**, select the **No interface** option. This disables the display of the Kaspersky Endpoint Security for Windows user interface on workstations.
5. Under **Password protection**, enable the toggle switch. This reduces the risk of unauthorized or unintended changes in settings of Kaspersky Endpoint Security for Windows on workstations.

The recommended settings for the interface of Kaspersky Endpoint Security for Windows are specified.

Configuring the policy in the Event configuration section

To avoid the Administration Server database overflow, we recommend that you save only important events to the database.

► *To configure registration of important events in the Administration Server database:*

1. Go to **DEVICES** → **POLICIES & PROFILES**.
2. Click the policy for Kaspersky Endpoint Security for Windows.
The properties window of the selected policy opens.
3. In the policy properties, open the **Event configuration** tab.
4. In the **Critical** section, click **Add events** and select check boxes next to the following events only:
 - License Agreement violated
 - Application autorun is disabled
 - Activation error
 - Active threat detected. Start Advanced Disinfection
 - Disinfection not possible
 - Previously opened dangerous link detected
 - Process terminated
 - Network activity blocked
 - Network attack detected
 - Application startup prohibited
 - Access denied
 - Local update error

- Cannot start two tasks at the same time
 - Error in interaction with Kaspersky Security Center
 - Not all components were updated
 - Error applying file encryption / decryption rules
 - Error enabling portable mode
 - Error disabling portable mode
 - Could not load encryption module
 - Policy cannot be applied
 - Application content modification error
5. Click **OK**.
 6. In the **Functional failure** section, click **Add events** and select check boxes next to the following events only:
 - Task settings error. Settings not applied
 7. Click **OK**.
 8. In the **Warning** section, click **Add events** and select check boxes next to the following events only:
 - Self-Defense is disabled
 - Protection components are disabled
 - Incorrect reserve activation code
 - Legitimate software that can be used to harm your computer or personal data was detected
 - Object deleted
 - Object disinfected
 - User has opted out of the encryption policy
 - File restored from Quarantine
 - File moved to Quarantine
 - Application startup blockage message to administrator
 - Device access blockage message to administrator
 - Web page access blockage message to administrator
 9. Click **OK**.
 10. In the **Info** section, click **Add events** and select check boxes next to the following events only:
 - A backup copy of the object was created
 - Application startup prohibited in test mode
 11. Click **OK**.

Registration of important events in the Administration Server database is configured.

Manual setup of the group update task for Kaspersky Endpoint Security

The optimal and recommended schedule option for Kaspersky Endpoint Security is **When new updates are downloaded to the repository** when the **Use automatically randomized delay for task starts** check box is selected.

Granting offline access to the external device blocked by Device Control

In Device Control component of Kaspersky Endpoint Security for Windows policy, you can manage user access to external devices that are installed on or connected to the client device (for example, hard drives, cameras, or Wi-Fi modules). This lets you protect the client device from infection when such external devices are connected, and prevent loss or leaks of data.

If you need to grant temporary access to the external device blocked by Device Control but it is not possible to add the device to the list of trusted devices, you can grant temporary offline access to the external device. Offline access means that the client device has not access to the network.

You can grant offline access to the external device blocked by Device Control only if in the settings of Kaspersky Endpoint Security for Windows policy, in the Device Control section, the **Allow request for temporary access** option is enabled.

Granting offline access to the external device blocked by Device Control includes the following stages:

1. In the Kaspersky Endpoint Security for Windows dialog window, device user who wants to have access to the blocked external device, generates request access file and sends it Kaspersky Security Center administrator.
2. Getting this request, Kaspersky Security Center administrator creates an access key file and send it to the device user.
3. In the Kaspersky Endpoint Security for Windows dialog window, the device user activates the access key file and obtains temporary access to the external device.

► *To grant temporary access to the external device blocked by Device Control:*

1. Select **DEVICES** → **MANAGED DEVICES**.
The list of managed devices is displayed.
2. In the list of managed devices, select the user device that requests access to the external device blocked by Device Control.
You can select only one device.
3. Above the list of managed devices, click the **Grant access to the device in offline mode** button.
The **Grant access in offline mode** window opens.
4. In the **Grant access in offline mode** window, on the **Device Control** tab, click the **Browse** button.

The standard **Select request access file** window of Microsoft Windows opens.

5. In the **Select request access file** window, select the request access file that you have received from the user and click the **Open** button.

The details of the locked device to which the user has requested access is displayed.

6. Specify the value of the **Access duration** setting.

This setting defines the length of time for which you grant the user access to the locked device. The default value is the value that was specified by the user when creating the request access file.

7. Specify the value of the **Activation period** setting.

This setting defines the time period during which the user can activate access to the blocked device by using the provided access key.

8. Click the **Save** button.

This opens the standard **Save access key** window of Microsoft Windows.

9. Select the destination folder in which you want to save the file containing the access key for the blocked device.

10. Click the **Save** button.

As a result, when you send the user the access key file and the user activates it in the Kaspersky Endpoint Security for Windows dialog window, the user has temporary access to the blocked device for the specific period.

Removing applications or software updates remotely

► *To remove applications or software updates remotely from selected devices:*

1. In the main application window, go to **DEVICES** → **TASKS**.

2. Click **Add**.

The Add Task Wizard starts. Proceed through the Wizard by using the **Next** button.

3. For the Kaspersky Security Center application, select the **Uninstall application remotely** task type.

4. Specify the name for the task that you are creating.

A task name cannot be more than 100 characters long and cannot include any special characters ("*<>?\\:|).

5. Select the devices to which the task will be assigned.

6. Select what kind of software you want to remove, and then select specific applications, updates, or patches that you want to remove:

- **Uninstall managed application**
- **Uninstall incompatible application**
- **Uninstall application from applications registry**
- **Uninstall the specified application update, patch, or third-party application**

7. Specify how client devices will download the Uninstallation utility:

- **Using Network Agent**
- **Using operating system resources through Administration Server**

- **Using operating system resources through distribution points**
- **Maximum number of concurrent downloads**
- **Maximum number of uninstallation attempts**
- **Verify operating system type before downloading**

8. Specify the operating system restart settings:

- **Do not restart the device**

Client devices are not restarted automatically after the operation. To complete the operation, you must restart a device (for example, manually or through a device management task). Information about the required restart is saved in the task results and in the device status. This option is suitable for tasks on servers and other devices where continuous operation is critical.

- **Restart the device**

Client devices are always restarted automatically if a restart is required for completion of the operation. This option is useful for tasks on devices that provide for regular pauses in their operation (shutdown or restart).

- **Prompt user for action**

The restart reminder is displayed on the screen of the client device, prompting the user to restart it manually. Some advanced settings can be defined for this option: text of the message for the user, the message display frequency, and the time interval after which a restart will be forced (without the user's confirmation). This option is most suitable for workstations where users must be able to select the most convenient time for a restart.

By default, this option is selected.

- **Repeat prompt every (min)**

If this option is enabled, the application prompts the user to restart the operating system with the specified frequency.

By default, this option is enabled. The default interval is 5 minutes. Available values are between 1 and 1 440 minutes.

If this option is disabled, the prompt is displayed only once.

- **Restart after (min)**

After prompting the user, the application forces restart of the operating system upon expiration of the specified time interval.

By default, this option is enabled. The default delay is 30 minutes. Available values are between 1 and 1 440 minutes.

- **Wait time before forced closure of applications in blocked sessions (min)**

Running applications may prevent a restart of the client device. For example, if a document is being edited in a word processing application and is not saved, the application does not allow the device to restart.

If this option is enabled, such applications on a locked device are forced to close before the device restart. As a result, users may lose their unsaved changes.

If this option is disabled, a locked device is not restarted. The task status on this device

states that a device restart is required. Users have to manually close all applications running on locked devices and restart these devices.

By default, this option is disabled.

1. If necessary, add the accounts that will be used to start the remote uninstallation task:

- **No account required (Network Agent installed)**

If this option is selected, you do not have to specify the account under which the application installer will be run. The task will run under the account under which the Administration Server service is running.

If Network Agent has not been installed on client devices, this option is not available.

- **Account required (Network Agent is not used)**

If this option is selected, you can specify the account under which the application installer will be run. You can specify the user account if Network Agent has not been installed on the devices for which the task is assigned.

You can specify multiple user accounts if, for example, none of them have all the required rights on all devices for which this task is assigned. In this case, all accounts that have been added are used for running the task, in consecutive order, top-down.

If no accounts have been added, the task will be run under the account under which the Administration Server service is running.

2. If you want to modify the default task settings, enable the **Open task details when creation is complete** option on the **Finish task creation** page. If you do not enable this option, the task is created with the default settings. You can modify the default settings later, at any time.
3. Click the **Finish** button.
The task is created and displayed in the list of tasks.
4. Click the name of the created task to open the task properties window.
5. In the task properties window, specify the general task settings (on page [1081](#)).
6. Click the **Save** button.
7. Run the task manually or wait for it to launch according to the schedule you specified in the task settings.

Upon completion of the remote uninstallation task, the selected application will be removed from the selected devices.

See also:

Replacing third-party security applications [333](#)

Rolling back an object to a previous revision

You can roll back changes made to an object, if necessary. For example, you may have to revert the settings of a policy to their state on a specific date.

► *To roll back changes made to an object:*

1. In the object's properties window, open the **Revision history** tab.

2. In the list of object revisions, select the revision that you want to roll back changes for.
3. Click the **Roll back** button.
4. Click **OK** to confirm the operation.

The object is now rolled back to the selected revision. The list of object revisions displays a record of the action that was taken. The revision description displays information about the number of the revision to which you reverted the object.

Rolling back operation is available only for policy and task objects.

Tasks

This section describes tasks used by Kaspersky Security Center.

In this chapter

About tasks	1078
About task scope	1079
Creating a task.....	1080
Starting a task manually	1080
Viewing the task list	1081
General task settings	1081
Starting the wizard for changing tasks password	1087

About tasks

Kaspersky Security Center manages Kaspersky security applications installed on devices by creating and running *tasks*. Tasks are required for installing, launching, and stopping applications, scanning files, updating databases and software modules, and performing other actions on applications.

Tasks for a specific application can be created using Kaspersky Security Center 13 Web Console only if the management plug-in for that application is installed on Kaspersky Security Center 13 Web Console Server.

Tasks can be performed on the Administration Server and on devices.

The tasks that are performed on the Administration Server include the following:

- Automatic distribution of reports
- Downloading of updates to the repository
- Backup of Administration Server data
- Maintenance of the database

The following types of tasks are performed on devices:

- *Local tasks*—Tasks that are performed on a specific device
Local tasks can be modified either by the administrator, using Administration Console tools, or by the user of a remote device (for example, through the security application interface). If a local task has been modified simultaneously by the administrator and the user of a managed device, the changes made by the administrator will take effect because they have a higher priority.
- *Group tasks*—Tasks that are performed on all devices of a specific group

Unless otherwise specified in the task properties, a group task also affects all subgroups of the selected group. A group task also affects (optionally) devices that have been connected to secondary and virtual Administration Servers deployed in the group or any of its subgroups.

- *Global tasks*—Tasks that are performed on a set of devices, regardless of whether they are included in any group.

For each application, you can create any number of group tasks, global tasks, or local tasks.

You can make changes to the settings of tasks, view the progress of tasks, and copy, export, import, and delete tasks.

A task is started on a device only if the application for which the task was created is running.

Execution results of tasks are saved in the operating system event log on each device, in the operating system event log on the Administration Server, and in the Administration Server database.

Do not include private data in task settings. For example, avoid specifying the domain administrator password.

See also:

Scenario: Installation and initial setup of Kaspersky Security Center 13 Web Console[962](#)

About task scope

The *scope of a task* (see section "*About tasks*" on page [1078](#)) is the set of devices on which the task is performed. The types of scope are as follows:

- For a *local task*, the scope is the device itself.
- For an *Administration Server task*, the scope is the Administration Server.
- For a *group task*, the scope is the list of devices included in the group.

When creating a *global task*, you can use the following methods to specify its scope:

- Specifying certain devices manually.

You can use an IP address (or IP range), NetBIOS name, or DNS name as the device address.

- Importing a list of devices from a .txt file with the device addresses to be added (each address must be placed on an individual line).

If you import a list of devices from a file or create a list manually, and if devices are identified by their names, the list can only contain devices for which information has already been entered into the Administration Server database. Moreover, the information must have been entered when those devices were connected or during device discovery.

- Specifying a device selection.

Over time, the scope of a task changes as the set of devices included in the selection change. A selection of devices can be made on the basis of device attributes, including software installed on a device, and on

the basis of tags assigned to devices. Device selection is the most flexible way to specify the scope of a task.

Tasks for device selections are always run on a schedule by the Administration Server. These tasks cannot be run on devices that lack connection to the Administration Server. Tasks whose scope is specified by using other methods are run directly on devices and therefore do not depend on the device connection to the Administration Server.

Tasks for device selections are not run on the local time of a device; instead, they are run on the local time of the Administration Server. Tasks whose scope is specified by using other methods are run on the local time of a device.

Creating a task

► *To create a task:*

1. Go to **DEVICES** → **TASKS**.
2. Click **Add**.

The New Task Wizard starts. Follow its instructions.

3. If on the **Finish task creation** page you enable the **Open task details when creation is complete** option, you can modify the default task settings. If you do not enable this option, the task is created with the default settings. You can modify the default settings later, at any time.
4. Click the **Finish** button.

The task is created and displayed in the list of tasks.

See also:

General task settings	1081
Scenario: Kaspersky applications deployment through Kaspersky Security Center 13 Web Console ...	1023
Scenario: Monitoring and reporting	1279

Starting a task manually

The application starts tasks according to the schedule settings specified in the properties of each task. You can start a task manually at any time.

► *To start a task manually:*

1. Go to **DEVICES** → **TASKS**.
2. In the task list, select the check box next to the task that you want to start.
3. Click the **Start** button.

The task starts. You can check the task status in the **Status** column or by clicking the **Result** button.

See also:

About tasks.....	1078
Creating a task	1080
General task settings	1081

Viewing the task list

You can view the list of tasks that are created in Kaspersky Security Center.

- ▶ *To view the list of tasks,*

Go to **DEVICES** → **TASKS**.

The list of tasks is displayed. The tasks are grouped by the names of applications to which they are related. For example, the Uninstall application remotely task is related to the Administration Server, and the Find vulnerabilities and required updates task refers to the Network Agent.

- ▶ *To view properties of a task,*

Click the name of the task.

The task properties window is displayed with several named tabs (see section "General task settings" on page [1081](#)). For example, the **Task type** is displayed on the **General** tab, and the task schedule—on the **Schedule** tab.

General task settings

This section lists the settings that you can view and specify for tasks.

Settings specified during task creation

You can specify the following settings when creating a task. Some of these settings can also be modified in the properties of the created task.

- Operating system restart settings:
 - **Do not restart the device**

Client devices are not restarted automatically after the operation. To complete the operation, you must restart a device (for example, manually or through a device management task). Information about the required restart is saved in the task results and in the device status. This option is suitable for tasks on servers and other devices where continuous operation is critical.
 - **Restart the device**

Client devices are always restarted automatically if a restart is required for completion of the operation. This option is useful for tasks on devices that provide for regular pauses in their operation (shutdown or restart).
- **Prompt user for action**

The restart reminder is displayed on the screen of the client device, prompting the user to restart it manually. Some advanced settings can be defined for this option: text of the message for the user, the message display frequency, and the time interval after which a restart will be forced (without the user's confirmation). This option is most suitable for workstations where users must be able to select the most convenient time for a restart.

By default, this option is selected.

- **Repeat prompt every (min)**

If this option is enabled, the application prompts the user to restart the operating system with the specified frequency.

By default, this option is enabled. The default interval is 5 minutes. Available values are between 1 and 1 440 minutes.

If this option is disabled, the prompt is displayed only once.

- **Restart after (min)**

After prompting the user, the application forces restart of the operating system upon expiration of the specified time interval.

By default, this option is enabled. The default delay is 30 minutes. Available values are between 1 and 1 440 minutes.

- **Wait time before forced closure of applications in blocked sessions (min)**

Running applications may prevent a restart of the client device. For example, if a document is being edited in a word processing application and is not saved, the application does not allow the device to restart.

If this option is enabled, such applications on a locked device are forced to close before the device restart. As a result, users may lose their unsaved changes.

If this option is disabled, a locked device is not restarted. The task status on this device states that a device restart is required. Users have to manually close all applications running on locked devices and restart these devices.

By default, this option is disabled.

- Task scheduling settings:
 - **Scheduled start**

Select the schedule according to which the task runs, and configure the selected schedule.

- **Every N hours**

The task runs regularly, with the specified interval in hours, starting from the specified date and time.

By default, the task runs every six hours, starting from the current system date and time.

- **Every N days**

The task runs regularly, with the specified interval in days. Additionally, you can specify a date and time of the first task run. These additional options become available, if they are supported by the application for which you create the task.

By default, the task runs every day, starting from the current system date and time.

- **Every N weeks**

The task runs regularly, with the specified interval in weeks, on the specified day of week

and at the specified time.

By default, the task runs every Monday at the current system time.

- **Every N minutes**

The task runs regularly, with the specified interval in minutes, starting from the specified time on the day that the task is created.

By default, the task runs every 30 minutes, starting from the current system time.

- **Daily (daylight saving time is not supported)**

The task runs regularly, with the specified interval in days. This schedule does not support observance of daylight saving time (DST). It means that when clocks jump one hour forward or backward at the beginning or ending of DST, the actual task start time does not change.

We do not recommend that you use this schedule. It is needed for backward compatibility of Kaspersky Security Center.

By default, the task starts every day at the current system time.

- **Weekly**

The task runs every week on the specified day and at the specified time.

- **By days of week**

The task runs regularly, on the specified days of week, at the specified time.

By default, the task runs every Friday at 6:00:00 P.M.

- **Monthly**

The task runs regularly, on the specified day of the month, at the specified time.

In months that lack the specified day, the task runs on the last day.

By default, the task runs on the first day of each month, at the current system time.

- **Manually**

The task does not run automatically. You can only start it manually.

- **Every month on specified days of selected weeks**

The task runs regularly, on the specified days of each month, at the specified time.

By default, no days of month are selected; the default start time is 6:00:00 P.M.

- **When new updates are downloaded to the repository**

The task runs after updates are downloaded to the repository. For example, you may want to use this schedule for the find vulnerabilities and required updates task.

- **On virus outbreak**

The task runs after a *Virus outbreak* event occurs. Select application types that will monitor virus outbreaks. The following application types are available:

- Anti-virus for workstations and file servers
- Anti-virus for perimeter defense
- Anti-virus for mail systems

By default, all application types are selected.

You may want to run different tasks depending on the anti-virus application type that

reports a virus outbreak. In this case, remove the selection of the application types that you do not need.

- **On completing another task**

The current task starts after another task completes. You can select how the previous task must complete (successfully or with error) to trigger the start of the current task. For example, you may want to run the Manage devices task with the **Turn on the device** option and, after it completes, run the Virus scan task.

- **Run missed tasks**

This option determines the behavior of a task if a client device is not visible on the network when the task is about to start.

If this option is enabled, the system attempts to start the task the next time the Kaspersky application is run on the client device. If the task schedule is **Manually, Once** or **Immediately**, the task is started immediately after the device becomes visible on the network or immediately after the device is included in the task scope.

If this option is disabled, only scheduled tasks run on client devices; for **Manually, Once** and **Immediately**, tasks run only on those client devices that are visible on the network. For example, you may want to disable this option for a resource-consuming task that you want to run only outside of business hours.

By default, this option is enabled.

- **Use automatically randomized delay for task starts**

If this option is enabled, the task is started on client devices randomly within a specified time interval, that is, *distributed task start*. A distributed task start helps to avoid a large number of simultaneous requests by client devices to the Administration Server when a scheduled task is running.

The distributed start time is calculated automatically when a task is created, depending on the number of client devices to which the task is assigned. Later, the task is always started on the calculated start time. However when task settings are edited or the task is started manually, the calculated value of the task start time changes.

If this option is disabled, the task starts on client devices according to the schedule.

- **Use randomized delay for task starts within an interval of (min)**

If this option is enabled, the task is started on client devices randomly within the specified time interval. A distributed task start helps to avoid a large number of simultaneous requests by client devices to the Administration Server when a scheduled task is running.

If this option is disabled, the task starts on client devices according to the schedule.

By default, this option is disabled. The default time interval is one minute.

- Devices to which the task will be assigned:

- **Select networked devices detected by Administration Server**

The task is assigned to specific devices. The specific devices can include devices in administration groups as well as unassigned devices.

For example, you may want to use this option in a task of installing Network Agent on unassigned devices.

- **Specify device addresses manually or import addresses from list**

You can specify NetBIOS names, DNS names, IP addresses, and IP subnets of devices

to which you want to assign the task.

You may want to use this option to execute a task for a specific subnet. For example, you may want to install a certain application on devices of accountants or to scan devices in a subnet that is probably infected.

- **Assign task to a device selection**

The task is assigned to devices included in a device selection. You can specify one of the existing selections.

For example, you may want to use this option to run a task on devices with a specific operating system version.

- **Assign task to an administration group**

The task is assigned to devices included in an administration group. You can specify one of the existing groups or create a new one.

For example, you may want to use this option to run a task of sending a message to users if the message is specific for devices included in a specific administration group.

- Account settings:

- **Default account**

The task will be run under the same account as the application that performs this task.

By default, this option is selected.

- **Specify an account**

Fill in the **Account** and **Password** fields to specify the details of an account under which the task is run. The account must have sufficient rights for this task.

- **Account**

Account under which the task is run.

- **Password**

Password of the account under which the task will be run.

Settings specified after task creation

You can specify the following settings only after a task is created.

- Advanced scheduling settings:

- **Activate the device before the task is started through Wake-on-LAN (min)**

The operating system on the device starts at the specified time before the task is started. The default time period is five minutes.

Enable this option if you want the task to run on all of the client devices from the task scope, including those devices that are turned off when the task is about to start.

If you want the device to be automatically turned off after the task is complete, enable the **Shut down device when task is complete** option. This option can be found in the same window.

By default, this option is disabled.

- **Turn off device after task completion**

For example, you may want to enable this option for an install update task that installs updates to client devices each Friday after business hours, and then turns off these devices for the weekend.

By default, this option is disabled.

- **Stop task if it has been running longer than (min)**

After the specified time period expires, the task is stopped automatically, whether it is completed or not.

Enable this option if you want to interrupt (or stop) tasks that take too long to execute.

By default, this option is disabled. The default task execution time is 120 minutes.

- Notification settings:
 - **Store task history** block
 - **Store in the Administration Server database for (days)**

Application events related to execution of the task on all client devices from the task scope are stored on the Administration Server during the specified number of days. When this period elapses, the information is deleted from the Administration Server.

By default, this option is enabled.

- **Store in the OS event log on device**

Application events related to execution of the task are stored locally in Windows Event Log of each client device.

By default, this option is disabled.

- **Store in the OS event log on Administration Server**

Application events related to execution of the task on all client devices from the task scope are stored centrally in Windows Event Log of the Administration Server operating system (OS).

By default, this option is disabled.

- **Save all events**

If this option is selected, all events related to the task are saved to the event logs.

- **Save events related to task progress**

If this option is selected, only events related to the task execution are saved to the event logs.

- **Save only task execution results**

If this option is selected, only events related to the task results are saved to the event logs.

- **Notify administrator of task execution results**

You can select the methods by which administrators receive notifications about task execution results: by email, by SMS, and by running an executable file. To configure notification, click the **Settings** link.

By default, all notification methods are disabled.

- **Notify of errors only**

If this option is enabled, administrators are only notified when a task execution completes with an error.

If this option is disabled, administrators are notified after every task execution completion.

By default, this option is enabled.

- Security settings
- Task scope settings

Depending on how the task scope is determined, the following settings are present:

- **Devices**

If the scope of a task is determined by an administration group, you can view this group. No changes are available here. However, you can set **Exclusions from task scope**.

If the scope of a task is determined by a list of devices, you can modify this list by adding and removing devices.

- **Device selection**

You can change the device selection to which the task is applied.

- **Exclusions from task scope**

You can specify groups of devices to which the task is not applied. Groups to be excluded can only be subgroups of the administration group to which the task is applied.

- **Revision history**

See also:

Scenario: Kaspersky applications deployment through Kaspersky Security Center 13 Web Console[1023](#)

Starting the wizard for changing tasks password

For a non-local task, you can specify an account under which the task must be run. You can specify the account during task creation or in the properties of an existing task. If the specified account is used in accordance with security instructions of the organization, these instructions might require changing the account password from time to time. When the account password expires and you set a new one, the tasks will not start until you specify the new valid password in the task properties.

The wizard for changing the tasks password enables you to replace the old password with the new one in all tasks in which the account is specified. Alternatively, you can change this password manually in the properties of each task.

► *To start the wizard for changing the tasks password:*

1. On the **DEVICES** tab, select **TASKS**.
2. Click **Manage credentials of accounts for starting tasks**.

Follow the instructions of the wizard.

See also:

About tasks	1078
About task scope	1079
Viewing the task list	1081 In this section
Step 1. Specifying credentials	1088
Step 2. Selecting an action to take	1088
Step 3. Viewing the results	1089

Step 1. Specifying credentials

Specify new credentials that are currently valid in your system (for example, in Active Directory). When you switch to the next step of the wizard, Kaspersky Security Center checks if the specified account name matches the account name in the properties of each non-local task. If the account names match, the password in the task properties will be automatically replaced with the new one.

To specify the new account, select an option:

- **Use current account**

The wizard uses the name of the account under which you are currently signed in to Kaspersky Security Center 13 Web Console. Then manually specify the account password in the **Current password to use in tasks** field.

- **Specify a different account**

Specify the name of the account under which the tasks must be started. Then specify the account password in the **Current password to use in tasks** field.

If you fill in the **Previous password (optional; if you want to replace it with the current one)** field, Kaspersky Security Center replaces the password only for those tasks in which both the account name and the old password are found. The replacement is performed automatically. In all other cases you have to choose an action to take in the next step of the wizard.

See also:

Starting the wizard for changing tasks password	1087
Step 2. Selecting an action to take	1088
Step 3. Viewing the results	1089

Step 2. Selecting an action to take

If you did not specify the previous password in the first step of the wizard or if the specified old password has not matched the passwords in the task properties, you must choose an action to take for the tasks found.

► *To choose an action for a task:*

1. Select the check box next to the task for which you want to choose an action.
2. Perform one of the following:
 - To remove the password in the task properties, click **Delete credentials**.
The task is switched to run under the default account.
 - To replace the password with a new one, click **Enforce the password change even if the old password is wrong or not provided**.
 - To cancel the password change, click **No action is selected**.

The chosen actions are applied after you move to the next step of the wizard.

See also:

Starting the wizard for changing tasks password.....	1087
Step 1. Specifying credentials.....	1088
Step 3. Viewing the results.....	1089

Step 3. Viewing the results

On the last step of the wizard, view the results for each of the tasks found. To complete the wizard, click the **Finish** button.

See also:

Starting the wizard for changing tasks password	1087
Step 1. Specifying credentials	1088
Step 2. Selecting an action to take	1088

Managing client devices

This section describes how to manage devices in the administration groups.

In this chapter

Settings of a managed device	1090
Creating device moving rules	1094
Copying device moving rules.....	1095
Adding devices to an administration group manually	1096
Moving devices to an administration group manually.....	1097
Viewing and configuring the actions when devices show inactivity.....	1098
About device statuses.....	1099
Configuring the switching of device statuses	1104
Remotely connecting to the desktop of a client device	1105
Connecting to devices through Windows Desktop Sharing.....	1107

Settings of a managed device

► *To view the settings of a managed device:*

1. Select **DEVICES** → **MANAGED DEVICES**.

The list of managed devices is displayed.

2. In the list of managed devices, click the link with the name of the required device.

The properties window of the selected device is displayed.

General

The **General** section displays general information about the client device. Information is provided on the basis of data received during the last synchronization of the client device with the Administration Server:

- **Name**

In this field, you can view and modify the client device name in the administration group.

- **Description**

In this field, you can enter an additional description for the client device.

- **Group**

Administration group, which includes the client device.

- **Last updated**

Date the databases or applications were last updated on the device.

- **Last visible**

Date and time the device was last visible on the network.

- **Connected to Administration Server**

Date and time Network Agent installed on the client device last connected to the Administration Server.

- **Do not disconnect from the Administration Server**

If this check box is selected, an uninterrupted connection is maintained between the Administration Server and the client device.

If this check box is cleared, the client device will only connect to the Administration Server to synchronize data or to transmit information.

This check box is selected by default if Administration Server is installed on the device.

If only Network Agent is installed on the device, this check box is cleared by default.

Network

The **Network** section displays the following information about the network properties of the client device:

- **IP address**

Device IP address

- **Windows domain**

Windows domain or workgroup, which contains the device.

- **DNS name**

Name of the DNS domain of the client device.

- **NetBIOS name**

Windows network name of the client device.

System

The **System** section provides information about the operating system installed on the client device.

Protection

The **Protection** section provides information about the current status of anti-virus protection on the client device:

- **Device status**

Status of the client device assigned on the basis of the criteria defined by the administrator for the status of anti-virus protection on the device and the activity of the device on the network.

- **All problems**

This table contains a complete list of problems detected by the managed applications installed on the client device. Each problem is accompanied by a status, which the application suggests you assign to the device for this problem.

- **Real-time protection**

This field shows the current status of real-time protection (see section "List of managed devices. Description of columns" on page [905](#)) on the client device.

When the status changes on the device, the new status is displayed in the device properties window only after the client device is synchronized with the Administration Server.

- **Last on-demand scan**

Date and time the last virus scan was performed on the client device.

- **Total number of threats detected**

Total number of threats detected on the client device since installation of the anti-virus application (first scan), or since the last reset of the threat counter.

- **Active threats**

Number of unprocessed files on the client device.

This field ignores the number of unprocessed files on mobile devices.

- **Disk encryption status**

The current status of file encryption on the local drives of the device.

Device status defined by application

The **Device status defined by application** section provides information about the device status that is defined by the managed application installed on the device. This device status can differ from the one defined by Kaspersky Security Center.

Applications

The **Applications** section lists all Kaspersky applications installed on the client device. You can click the application name to view general information about the application, a list of events that have occurred on the device, and the application settings.

Active policies and policy profiles

The **Active policies and policy profiles** section lists the policies and policy profiles which are currently active on the managed device.

Tasks

In the **Tasks** section, you can manage client device tasks: view the list of existing tasks, create new ones, remove, start, and stop tasks, modify their settings, and view execution results. The list of tasks is provided based on data received during the last session of client synchronization with the Administration Server. The Administration Server requests the task status details from the client device. If connection is not established, the status is not displayed.

Events

The **Events** section displays events logged on the Administration Server for the selected client device.

Incidents

In the **Incidents** section, you can view, edit, and create incidents for the client device. Incidents can be created either automatically, through managed Kaspersky applications installed on the client device, or manually by the administrator. For example, if some users regularly move malware from their removable drives to devices, the administrator can create an incident. The administrator can provide a brief description of the case and recommended actions (such as disciplinary actions to be taken against a user) in the text of the incident, and can add a link to the user or users.

An incident for which all of the required actions have been taken is called *processed*. The presence of unprocessed incidents can be chosen as the condition for a change of the device status to *Critical* or *Warning*.

This section contains a list of incidents that have been created for the device. Incidents are classified by severity level and type. The type of an incident is defined by the Kaspersky application, which creates the incident. You can highlight processed incidents in the list by selecting the check box in the **Processed** column.

Tags

In the **Tags** section, you can manage the list of keywords that are used for finding client devices: view the list of existing tags, assign tags from the list, configure auto-tagging rules, add new tags and rename old tags, and remove tags.

Applications registry

This feature is only available in MMC-based Administration Console, and Kaspersky Security Center 12.2 Web Console or later versions.

In the **Applications registry** section, you can view the registry of applications installed on the client device and their updates; you can also set up the display of the applications registry.

Information about installed applications is provided if Network Agent installed on the client device sends required information to the Administration Server. You can configure sending of information to the Administration Server in the properties window of Network Agent or its policy, in the **Repositories** section. Information about installed applications is provided only for devices running Windows.

Network Agent provides information about the applications based on data received from the system registry.

Clicking an application name opens a window that contains the application details and a list of the update packages installed for the application.

Executable files

The **Executable files** section displays executable files found on the client device.

Distribution points

This section provides a list of distribution points with which the device interacts.

- **Export to file**

Click the **Export to file** button to save to a file a list of distribution points with which the device interacts. By default, the application exports the list of devices to a CSV file.

- **Properties**

Click the **Properties** button to view and configure the distribution point with which the device interacts.

Hardware registry

In the **Hardware registry** section, you can view information about hardware installed on the client device. You can view this information for Windows devices and Linux devices.

Available updates

This section displays a list of software updates found on this device but not installed yet.

- **Show installed updates**

If this check box is selected, the list displays both updates that have not been installed

and those already installed on the client device.

By default, this check box is cleared.

Software vulnerabilities



The **Software vulnerabilities** section provides information about vulnerabilities in third-party applications installed on client devices.

To save the vulnerabilities to a file, select the check boxes next to the vulnerabilities that you want to save, and then click the **Export rows to CSV file** button or **Export rows to TXT file** button.

The **Software vulnerabilities** section contains the following settings:

- **Show only vulnerabilities that can be fixed**

If this check box is selected, the section displays vulnerabilities that can be fixed by using a patch.

If this check box is cleared, the section displays both vulnerabilities that can be fixed by using a patch, and vulnerabilities for which no patch has been released.

By default, this check box is selected.

- **Vulnerability properties**

See also:

Adjusting the general settings of Administration Server [609](#)

Creating device moving rules

You can set up device moving rules, which automatically allocate devices to administration groups.

To create a moving rule:

1. Go to **DEVICES** → **MOVING RULES** tab.
2. Click **Add**.
3. In the window that opens, specify the following information on the **General** tab:

- **Rule name**

Enter a name for the new rule.

If you are copying a rule, the new rule gets the same name as the source rule, but an index in () format is added to the name, for example: (1).

- **Administration group**

Select the administration group into which the devices are to be moved automatically.

- **Apply rule**

You can select one of the following options:

- Run once for each device.
The rule is applied once for each device that matches your criteria.
- Run once for each device, then at every Network Agent reinstallation.
The rule is applied once for each device that matches your criteria, then only when Network Agent is reinstalled on these devices.
- Rule applied continuously.
The rule is applied according to the schedule which the Administration Server sets up automatically (usually every several hours).

- **Move only devices that do not belong to an administration group**

If this option is enabled, only unassigned devices will be moved to the selected group.

If this option is disabled, devices that already belong to other administration groups, as well as unassigned devices, will be moved to the selected group.

- **Enable rule**

If this option is enabled, the rule is enabled and starts working after it is saved.

If this option is disabled, the rule is created, but not enabled. It will not work until you enable this option.

1. If you want, on the **Rule conditions** tab, specify the criteria for the devices that you want to be moved automatically.
2. Click **Save**.

The moving rule is created. It is displayed in the list of moving rules.

See also:

| Adding devices to an administration group manually [1096](#)

Copying device moving rules

You can copy moving rules, for example, if you want to have several identical rules for different target administration groups.

To copy an existing a moving rule:

1. Go to **DEVICES** → **MOVING RULES** tab.

You can also select **DISCOVERY & DEPLOYMENT** → **DEPLOYMENT & ASSIGNMENT**, and on the menu, select **MOVING RULES**.

The list of moving rules is displayed.

2. Select the check box next to the rule you want to copy.
3. Click **Copy**.
4. In the window that opens, change the following information on the **General** tab—or make no changes if you only want to copy the rule without changing its settings:

- **Rule name**

Enter a name for the new rule.

If you are copying a rule, the new rule gets the same name as the source rule, but an index in () format is added to the name, for example: (1).

- **Administration group**

Select the administration group into which the devices are to be moved automatically.

- **Apply rule**

You can select one of the following options:

- Run once for each device.

The rule is applied once for each device that matches your criteria.

- Run once for each device, then at every Network Agent reinstallation.

The rule is applied once for each device that matches your criteria, then only when Network Agent is reinstalled on these devices.

- Rule applied continuously.

The rule is applied according to the schedule which the Administration Server sets up automatically (usually every several hours).

- **Move only devices that do not belong to an administration group**

If this option is enabled, only unassigned devices will be moved to the selected group.

If this option is disabled, devices that already belong to other administration groups, as well as unassigned devices, will be moved to the selected group.

- **Enable rule**

If this option is enabled, the rule is enabled and starts working after it is saved.

If this option is disabled, the rule is created, but not enabled. It will not work until you enable this option.

1. If you want, on the **Rule conditions** tab, specify the criteria for the devices that you want to be moved automatically.
2. Click **Save**.

The new moving rule is created. It is displayed in the list of moving rules.

Adding devices to an administration group manually

This section describes features applicable only to Kaspersky Security Center 12.1 or a later version.

You can move devices to administration groups automatically by creating device moving rules or manually by moving devices from one administration group to another or by adding devices to a selected administration group. This section describes how to manually add devices to an administration group.

► *To add manually one or more devices to a selected administration group:*

1. Go to **DEVICES** → **MANAGED DEVICES**.
2. Click the **Groups** button, and then select the administration group to which you want to add the devices.
3. Click the **Add devices** button.

The Move Devices Wizard starts.

4. Make a list of the devices that you want to add to the administration group.

You can add only devices for which information has already been added to the Administration Server database either upon connection of the device or after device discovery.

Select how you want to add devices to the list:

- Click the **Add devices** button, and then specify the devices in one of the following ways:
 - Select devices from the list of devices detected by the Administration Server.
 - Specify a device IP address or an IP range.
 - Specify the NetBIOS name or DNS name of a device.

The device name field must not contain space characters, backspace characters, or the following prohibited characters: , \ / * ; : & ` ~ ! @ # \$ ^ & () = + [] { } | < > %

- Click the **Import devices from file** button to import a list of devices from a .txt file. Each device address or name must be specified on a separate line.

The file must not contain space characters, backspace characters, or the following prohibited characters: , \ / * ; : & ` ~ ! @ # \$ ^ & () = + [] { } | , < > %

5. View the list of devices to be added to the administration group. You can edit the list by adding or removing devices.
6. After making sure that the list is correct, click the **Next** button.

The Wizard processes the device list and displays the result. The successfully processed devices are added to the administration group and are displayed in the list of devices under names generated by Administration Server.

See also:

Creating device moving rules.....	1094
Moving devices to an administration group manually	1097

Moving devices to an administration group manually

You can move devices from one administration group to another, or from the group of unassigned devices to an administration group.

► *To move one or several devices to a selected administration group:*

1. Open the administration group from which you want to move the devices. To do this, perform one of the following:

- To open an administration group, go to **DEVICES** → **Groups** → **<group name>** → **MANAGED DEVICES**.
 - To open the **UNASSIGNED DEVICES** group, go to **DISCOVERY & DEPLOYMENT** → **UNASSIGNED DEVICES**.
2. Select the check boxes next to the devices that you want to move to a different group.
 3. Click the **Move to group** button.
 4. In the hierarchy of administration groups, select the check box next to the administration group to which you want to move the selected devices.
 5. Click the **Move** button.
- The selected devices are moved to the selected administration group.

Viewing and configuring the actions when devices show inactivity

If client devices within a group are inactive, you can get notifications about it. You can also automatically delete such devices.

► *To view or configure the actions when the devices in the group show inactivity:*

1. Go to **DEVICES** → **HIERARCHY OF GROUPS**.
2. Click the name of the required administration group.
This opens the administration group properties window.
3. In the properties window, go to the **Settings** tab.
4. In the **Inheritance** section, enable or disable the following options:
 - **Inherit from parent group**
The settings in this section will be inherited from the parent group in which the client device is included. If this option is enabled, the settings under **Device activity on the network** are locked from any changes.
This option is available only if the administration group has a parent group.
By default, this option is enabled.
 - **Force inheritance of settings in child groups**
The setting values will be distributed to child groups but in the properties of the child groups these settings are locked.
By default, this option is disabled.
5. In the **Device activity** section, enable or disable the following options:
 - **Notify the administrator if the device has been inactive for longer than (days)**
If this option is enabled, the administrator receives notifications about inactive devices. You can specify the time interval after which the **Device has remained inactive on the network in a long time** event is created. The default time interval is 7 days.

By default, this option is enabled.

- **Remove the device from the group if it has been inactive for longer than (days)**

If this option is enabled, you can specify the time interval after which the device is automatically removed from the group. The default time interval is 60 days.

By default, this option is enabled.

1. Click **Save**.

Your changes are saved and applied.

About device statuses

Kaspersky Security Center assigns a status to each managed device. The particular status depends on whether the conditions defined by the user are met. In some cases, when assigning a status to a device, Kaspersky Security Center takes into consideration the device's visibility flag on the network (see the table below). If Kaspersky Security Center does not find a device on the network within two hours, the visibility flag of the device is set to *Not Visible*.

The statuses are the following:

- *Critical* or *Critical / Visible*
- *Warning* or *Warning / Visible*
- *OK* or *OK / Visible*

The table below lists the default conditions that must be met to assign the *Critical* or *Warning* status to a device, with all possible values.

Table 80. Conditions for assigning a status to a device

Condition	Condition description	Available values
Security application is not installed	Network Agent is installed on the device, but a security application is not installed.	<ul style="list-style-type: none"> • Toggle button is on. • Toggle button is off.
Too many viruses detected	Some viruses have been found on the device by a task for virus detection, for example, the Virus scan task, and the number of viruses found exceeds the specified value.	More than 0.
Real-time protection level differs from the level set by the Administrator	The device is visible on the network, but the real-time protection level differs from the level set (in the condition) by the administrator for the device status.	<ul style="list-style-type: none"> • Stopped. • Paused. • Running.
Virus scan has not been performed in a long time	The device is visible on the network and a security application is installed on the device, but the Virus scan task has not been run within the specified time interval. The condition is applicable only to devices that were added to the Administration Server database 7 days ago or earlier.	More than 1 day.
Databases are outdated	The device is visible on the network and a security application is installed on the device, but the anti-virus databases have not been updated on this device within the specified time interval. The condition is applicable only to devices that were added to the Administration Server database 1 day ago or earlier.	More than 1 day.
Not connected in a long time	Network Agent is installed on the device, but the device has not connected to an Administration Server within the specified time interval, because the device was turned off.	More than 1 day.
Active threats are detected	The number of unprocessed objects in the ACTIVE THREATS folder exceeds the specified value.	More than 0 items.

Condition	Condition description	Available values
Restart is required	The device is visible on the network, but an application requires the device restart longer than the specified time interval and for one of the selected reasons.	More than 0 minutes.
Incompatible applications are installed	The device is visible on the network, but software inventory performed through Network Agent has detected incompatible applications installed on the device.	<ul style="list-style-type: none"> • Toggle button is off. • Toggle button is on.
Software vulnerabilities have been detected	The device is visible on the network and Network Agent is installed on the device, but the <i>Find vulnerabilities and required updates</i> task has detected vulnerabilities with the specified severity level in applications installed on the device.	<ul style="list-style-type: none"> • Critical. • High. • Medium. • Ignore if the vulnerability cannot be fixed. • Ignore if an update is assigned for installation.
License expired	The device is visible on the network, but the license has expired.	<ul style="list-style-type: none"> • Toggle button is off. • Toggle button is on.
License expires soon	The device is visible on the network, but the license will expire on the device in less than the specified number of days.	More than 0 days.

Condition	Condition description	Available values
Check for Windows Update updates has not been performed in a long time	The device is visible on the network, but the Perform Windows Update synchronization task has not been run within the specified time interval.	More than 1 day.
Invalid encryption status	Network Agent is installed on the device, but the device encryption result is equal to the specified value.	<ul style="list-style-type: none"> Does not comply with the policy due to the user's refusal (for external devices only). Does not comply with the policy due to an error. Restart is required when applying the policy. No encryption policy is specified. Not supported. When applying the policy.
Mobile device settings do not comply with the policy	The mobile device settings are other than the settings that were specified in the Kaspersky Endpoint Security for Android policy during the check of compliance rules.	<ul style="list-style-type: none"> Toggle button is off. Toggle button is on.
Unprocessed incidents detected	Some unprocessed incidents have been found on the device. Incidents can be created either automatically, through managed Kaspersky applications installed on the client device, or manually by the administrator.	<ul style="list-style-type: none"> Toggle button is off. Toggle button is on.
Device status defined by application	The status of the device is defined by the managed application.	<ul style="list-style-type: none"> Toggle button is off. Toggle button is on.
Device is out of disk space	Free disk space on the device is less than the specified value or the device could not be synchronized with the Administration Server. The <i>Critical</i> or <i>Warning</i> status is changed to the <i>OK</i> status when the device is successfully synchronized with the Administration Server and free space on the device is greater than or equal to the specified value.	More than 0 MB

Condition	Condition description	Available values
Device has become unmanaged	During device discovery, the device was recognized as visible on the network, but more than three attempts to synchronize with the Administration Server failed.	<ul style="list-style-type: none"> Toggle button is off. Toggle button is on.
Protection is disabled	The device is visible on the network, but the security application on the device has been disabled for longer than the specified time interval.	More than 0 minutes.
Security application is not running	The device is visible on the network and a security application is installed on the device but is not running.	<ul style="list-style-type: none"> Toggle button is off. Toggle button is on.

Kaspersky Security Center allows you to set up automatic switching of the status of a device in an administration group when specified conditions are met. When specified conditions are met, the client device is assigned one of the following statuses: *Critical* or *Warning*. When specified conditions are not met, the client device is assigned the *OK* status.

Different statuses may correspond to different values of one condition. For example, by default, if the **Databases are outdated** condition has the **More than 3 days** value, the client device is assigned the *Warning* status; if the value is **More than 7 days**, the *Critical* status is assigned.

If you upgrade the Kaspersky Security Center from the previous version, the values of the **Databases are outdated** condition for assigning the status to *Critical* or *Warning* do not change.

When Kaspersky Security Center assigns a status to a device, for some conditions (see the Condition description column) the visibility flag is taken into consideration. For example, if a managed device was assigned the *Critical* status because the Databases are outdated condition was met, and later the visibility flag was set for the device, then the device is assigned the *OK* status.

See also:

Configuring the switching of device statuses[1301](#)

Configuring the switching of device statuses

You can change conditions to assign the *Critical* or *Warning* status to a device.

► *To enable changing the device status to Critical:*

1. Open the properties window in one of the following ways:

- In the **Policies** folder, in the context menu of an Administration Server policy, select **Properties**.
 - Select **Properties** in the context menu of an administration group.
2. In the properties window that opens, in the **Sections** pane, select **Device status**.
 3. In the right pane, in the **Set to Critical if these are specified** section, select the check box next to a condition in the list.

You can change only settings that are not locked in the parent policy (see section "Hierarchy of policies" on page [385](#)).

4. Set the required value for the selected condition.
You can set values for some, but not all, conditions.
5. Click **OK**.

When specified conditions are met, the managed device is assigned the *Critical* status.

► *To enable changing the device status to Warning:*

1. Open the properties window in one of the following ways:
 - In the **Policies** folder, in the context menu of the Administration Server policy, select **Properties**.
 - Select **Properties** in the context menu of the administration group.
2. In the properties window that opens, in the **Sections** pane select **Device status**.
3. In the right pane, in the **Set to Warning if these are specified** section select the check box next to a condition in the list.

You can change only settings that are not locked in the parent policy (see section "Hierarchy of policies" on page [385](#)).

4. Set the required value for the selected condition.
You can set values for some, but not all, conditions.
5. Click **OK**.

When specified conditions are met, the managed device is assigned the *Warning* status.



See also:

| Adjusting the general settings of Administration Server [609](#)

Remotely connecting to the desktop of a client device

The administrator can obtain remote access to the desktop of a client device through a Network Agent installed on the device. Remote connection to a device through the Network Agent is possible even if the TCP and UDP ports of the client device are closed.

Upon establishing the connection with the device, the administrator gains full access to information stored on this device and can manage applications installed on it.

Remote connection must be allowed in the operating system settings of the target managed device. For example, in Windows 10, this option is called **Allow Remote Assistance connections to this computer** (you can find this option at **Control Panel** → **System and Security** → **System** → **Remote settings**). If you have a license for the Vulnerability and Patch Management feature, you can enable this option forcibly when you establish connection to a managed device. If you do not have the license, enable this option locally on the target managed device. If this option is disabled, remote connection is not possible.

To establish remote connection to a device, you must have two utilities:

- Kaspersky utility named `klstunnel`. This utility must be stored on the administrator's workstation. You use this utility for tunneling the connection between a client device and the Administration Server.

Kaspersky Security Center allows tunneling TCP connections from Administration Console via the Administration Server and then via Network Agent to a specified port on a managed device. Tunneling is designed for connecting a client application on a device with Administration Console installed to a TCP port on a managed device—if no direct connection is possible between Administration Console and the target device.

Connection tunneling between a remote client device and Administration Server is required if the port used for connection to Administration Server is not available on the device. The port on the device may be unavailable in the following cases:

- The remote device is connected to a local network that uses the NAT mechanism.
- The remote device is part of the local network of Administration Server, but its port is closed by a firewall.
- Standard Microsoft Windows component named Remote Desktop Connection. Connection to a remote desktop is established through the standard Windows utility `mstsc.exe` in accordance with the utility's settings.

Connection to the current remote desktop session of the user is established without the user's knowledge. Once the administrator connects to the session, the device user is disconnected from the session without an advance notification.

► *To connect to the desktop of a client device:*

1. In MMC-based Administration Console, in the context menu of the Administration Server, select **Properties**.
2. In the Administration Server properties window that opens, go to **Administration Server connection settings** → **Connection ports**.
3. Make sure that the **Open RDP port for Kaspersky Security Center 13 Web Console** option is enabled.
4. In Kaspersky Security Center 13 Web Console, go to **DEVICES** → **MANAGED DEVICES** → **Groups**, and then select the administration group that contains the device to which you want to obtain access.
5. Select the check box next to the name of the device to which you want to obtain access.
6. Click the **Connect to Remote Desktop** button.

The Remote Desktop (Windows only) window opens.

7. Enable the **Allow remote desktop connection on managed device** option. In this case, the connection will be established even if remote connections are currently prohibited in the operating system settings on the managed device.

This option is applicable only to Kaspersky Security Center 12.1 or a later version.
This option is only available if you have a license for the Vulnerability and Patch Management feature.

8. Click the **Download** button to download the klsctunnel utility.
9. Click the **Copy to clipboard** button to copy the text from the text field. This text is a Binary Large Object (BLOB) that contains settings required to establish connection between the Administration Server and the managed device.

A BLOB is valid for 3 minutes. If it has expired, reopen the Remote Desktop (Windows only) window to generate a new BLOB.

10. Run the klsctunnel utility.
The utility window opens.
11. Paste the copied text into the text field.
12. If you use a proxy server, select the **Use proxy server** check box, and then specify the proxy server connection settings.
13. Click the **Open port** button.
The Remote Desktop Connection login window opens.
14. Specify the credentials of the account under which you are currently logged in to Kaspersky Security Center 13 Web Console.
15. Click the **Connect** button.

When connection to the device is established, the desktop is available in the Remote Desktop Connection window of Microsoft Windows.

Connecting to devices through Windows Desktop Sharing

This section describes features applicable only to Kaspersky Security Center 12.1 or a later version.

The administrator can obtain remote access to the desktop of a client device through a Network Agent installed on the device. Remote connection to a device through the Network Agent is possible even if the TCP and UDP ports of the client device are closed.

The administrator can connect to an existing session on a client device without disconnecting the user in this session. In this case, the administrator and the session user on the device share access to the desktop.

To establish remote connection to a device, you must have two utilities:

- Kaspersky utility named klsctunnel. This utility must be stored on the administrator's workstation. You use this utility for tunneling the connection between a client device and the Administration Server.

Kaspersky Security Center allows tunneling TCP connections from Administration Console via the Administration Server and then via Network Agent to a specified port on a managed device. Tunneling is designed for connecting a client application on a device with Administration Console installed to a TCP port on a managed device—if no direct connection is possible between Administration Console and the target device.

Connection tunneling between a remote client device and Administration Server is required if the port used for connection to Administration Server is not available on the device. The port on the device may be unavailable in the following cases:

- The remote device is connected to a local network that uses the NAT mechanism.
- The remote device is part of the local network of Administration Server, but its port is closed by a firewall.
- Windows Desktop Sharing. When connecting to an existing session of the remote desktop, the session user on the device receives a connection request from the administrator. No information about remote activity on the device and its results will be saved in reports created by Kaspersky Security Center.

The administrator can configure an audit of user activity on a remote client device. During the audit, the application saves information about files on the client device that have been opened and/or modified by the administrator (see section "Auditing actions on a remote client device" on page [641](#)).

To connect to the desktop of a client device through Windows Desktop Sharing, the following conditions must be met:

- Microsoft Windows Vista or later is installed on the administrator's workstation.
To check whether the Windows Desktop Sharing feature is included in your Windows edition, make sure that CLSID {32BE5ED2-5C86-480F-A914-0FF8885A1B3F} is included in the 32-bit registry.
- Microsoft Windows Vista or later is installed on the client device.
- Kaspersky Security Center uses a license for Vulnerability and Patch Management.

► *To connect to the desktop of a client device through Windows Desktop Sharing:*

1. In MMC-based Administration Console, in the context menu of the Administration Server, select **Properties**.
2. In the Administration Server properties window that opens, go to **Administration Server connection settings** → **Connection ports**.
3. Make sure that the **Open RDP port for Kaspersky Security Center 13 Web Console** option is enabled.
4. In Kaspersky Security Center 13 Web Console, go to **DEVICES** → **MANAGED DEVICES** → **Groups**, and then select the administration group that contains the device to which you want to obtain access.
5. Select the check box next to the name of the device to which you want to obtain access.

6. Click the **Windows Desktop Sharing** button.

The Windows Desktop Sharing Wizard opens.

7. Click the **Download** button to download the klstunnel utility, and wait for the download process to complete.

If you already have the klstunnel utility, skip this step.

8. Click the **Next** button.
9. Select the session on the device to which you want to connect, and then click the **Next** button.

10. On the target device, in the dialog box that opens, the user must allow a desktop sharing session. Otherwise, the session is not possible.

After the device user confirms the desktop sharing session, the next page of the Wizard opens.

11. Click the **Copy to clipboard** button to copy the text from the text field. This text is a Binary Large Object (BLOB) that contains settings required to establish connection between the Administration Server and the managed device.

A BLOB is valid for 3 minutes. If it has expired, generate a new BLOB.


12. Run the klstunnel utility.

The utility window opens.

13. Paste the copied text into the text field.

14. If you use a proxy server, select the **Use proxy server** check box, and then specify the proxy server connection settings.

15. Click the **Open port** button.

Desktop sharing starts in a new window. If you want to interact with the device, click the **Menu** icon () in the upper-left corner of the window, and then select **Interactive mode**.

See also:

Kaspersky Security Center licensing options.....	320
Ports used by Kaspersky Security Center	65

Policies and policy profiles

In Kaspersky Security Center 13 Web Console, you can create policies for Kaspersky applications (see section "List of Kaspersky applications supported by Kaspersky Security Center 13 Web Console" on page [957](#)). This section describes policies and policy profiles, and provides instructions for creating and modifying them.

In this chapter

About policies and policy profiles	1110
About lock and locked settings	1111
Inheritance of policies and policy profiles	1112
Managing policies	1118
Managing policy profiles	1127

About policies and policy profiles

A *policy* is a set of Kaspersky application settings that are applied to an administration group (see section "Administration groups" on page [49](#)) and its subgroups. You can install several Kaspersky applications (see section "List of Kaspersky applications supported by Kaspersky Security Center 13 Web Console" on page [957](#)) on the devices of an administration group. Kaspersky Security Center provides a single policy for each Kaspersky application in an administration group. A policy has one of the following statuses:

Table 81. The status of the policy

Status	Description
Active	The current policy that is applied to the device. Only one policy may be active for a Kaspersky application in each administration group. Devices apply the settings values of an active policy for a Kaspersky application.
Inactive	A policy that is not currently applied to a device.
Out-of-office	If this option is selected, the policy becomes active when the device leaves the corporate network.

Policies function according to the following rules:

- Multiple policies with different values can be configured for a single application.
- Only one policy can be active for the current application.
- You can activate an inactive policy when a specific event occurs. For example, you can enforce stricter anti-virus protection settings during virus outbreaks.
- A policy can have child policies.

Generally, you can use policies as preparations for emergency situations, such as a virus attack. For example, if there is an attack via flash drives, you can activate a policy that blocks access to flash drives. In this case, the current active policy automatically becomes inactive.

In order to prevent maintaining multiple policies, for example, when different occasions assume changing of several settings only, you may use policy profiles.

A *policy profile* is a named subset of policy settings values that replaces the settings values of a policy. A policy profile affects the effective settings formation on a managed device. *Effective settings* are a set of policy settings, policy profile settings, and local application settings that are currently applied for the device.

Policy profiles function according to the following rules:

- A policy profile takes an effect when a specific activation condition occurs.
- Policy profiles contain values of settings that differ from the policy settings.
- Activation of a policy profile changes the effective settings of the managed device.
- A policy can include a maximum of 100 policy profiles.



See also:

Inheritance of policies and policy profiles[1112](#)

About lock and locked settings

Each policy setting has a lock button icon (🔒). The table below shows lock button statuses:

Table 82. Lock button statuses

Status	Description
🔓 Undefined 	If an open lock is displayed next to a setting and the toggle button is disabled, the setting is not specified in the policy. A user can change these settings in the managed application interface. These type of settings are called <i>unlocked</i> .
🔒 Enforce 	If a closed lock is displayed next to a setting and the toggle button is enabled, the setting is applied to the devices where the policy is enforced. A user cannot modify the values of these settings in the managed application interface. These type of settings are called <i>locked</i> .

You can use a lock button for performing the following actions:

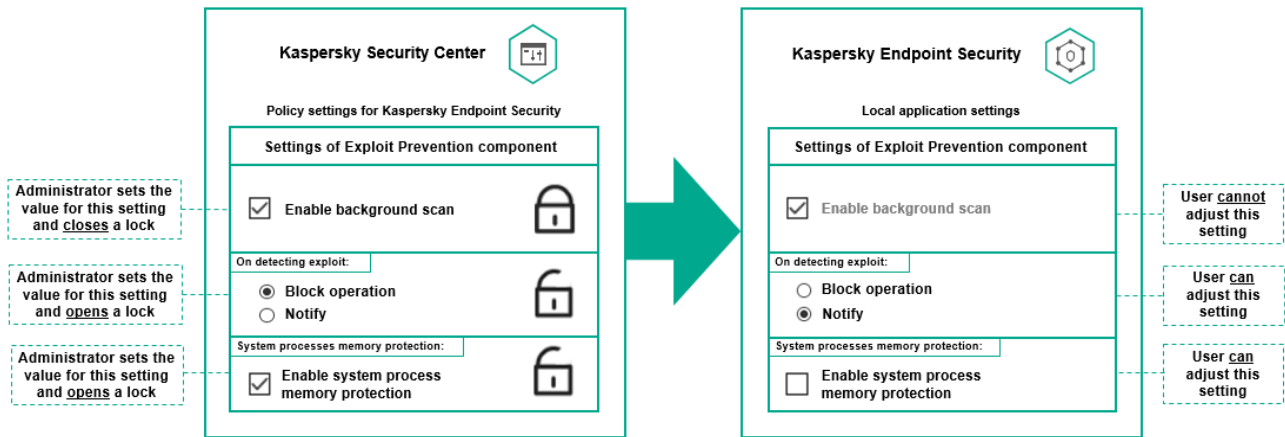
- Locking settings for an administration subgroup policy.
- Locking settings of a Kaspersky application on a managed device.

Thus, a locked setting is used for implementing effective settings on a managed device.

A process of effective settings implementation includes the following actions:

- Managed device applies unlocked settings values of a policy.
- Managed device applies settings values of Kaspersky application.
- Managed device applies locked settings values of a policy.

A policy and local Kaspersky application contain the same set of settings. When you configure policy settings, the Kaspersky application settings change values on a managed device. You cannot adjust locked settings on a managed device (see the figure below).



See also:

Policy profiles in a hierarchy of policies	1113
Hierarchy of policies	1112

Inheritance of policies and policy profiles

This section provides information about the hierarchy and inheritance of policies and policy profiles.

In this section

Hierarchy of policies	1112
Policy profiles in a hierarchy of policies	1113
How settings are implemented on a managed device.....	1116

Hierarchy of policies

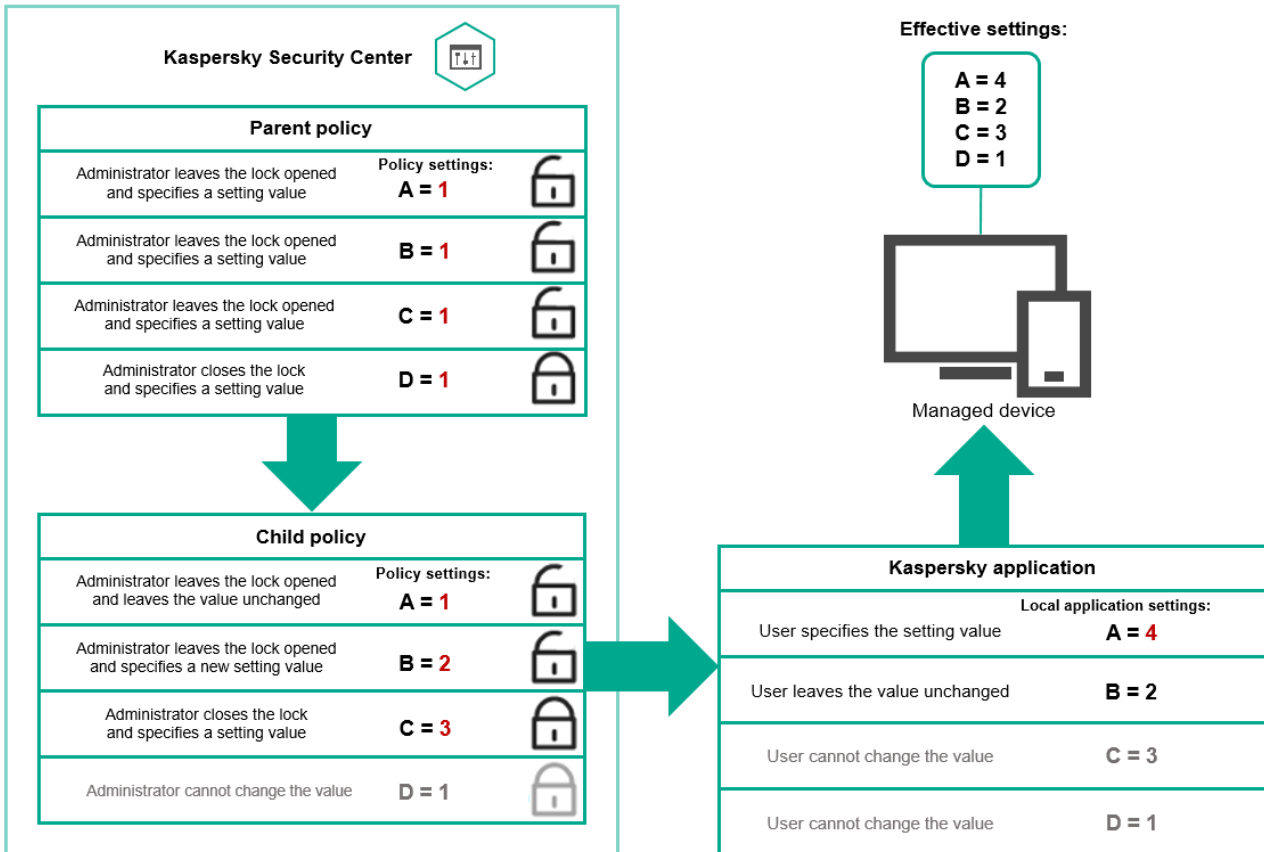
If different devices need different settings, you can organize devices into administration groups.

You can specify a policy for a single administration group (see section "Administration groups" on page 49). Policy settings can be *inherited*. Inheritance means receiving policy settings values in subgroups (child groups) from a policy of a higher-level (parent) administration group.

Hereinafter, a policy for a parent group is also referred to as a *parent policy*. A policy for a subgroup (child group) is also referred to as a *child policy*.

By default, at least one managed devices group exists on Administration Server. If you want to create custom groups, they are created as subgroups (child groups) within the managed devices group.

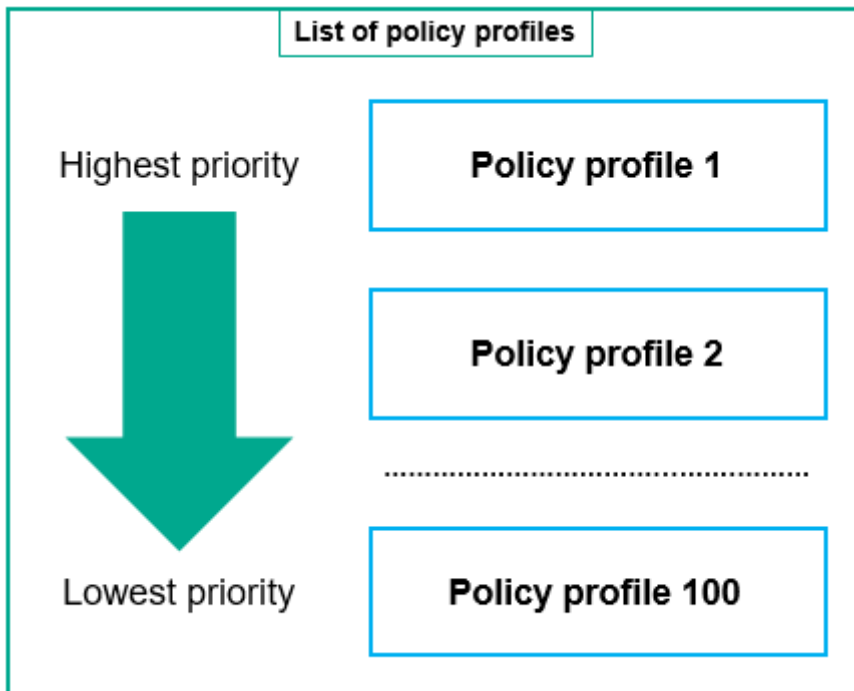
Policies of the same application act on each other, according to a hierarchy of administration groups. Locked settings from a policy of a higher-level (parent) administration group will reassign policy settings values of a subgroup (see the figure below).



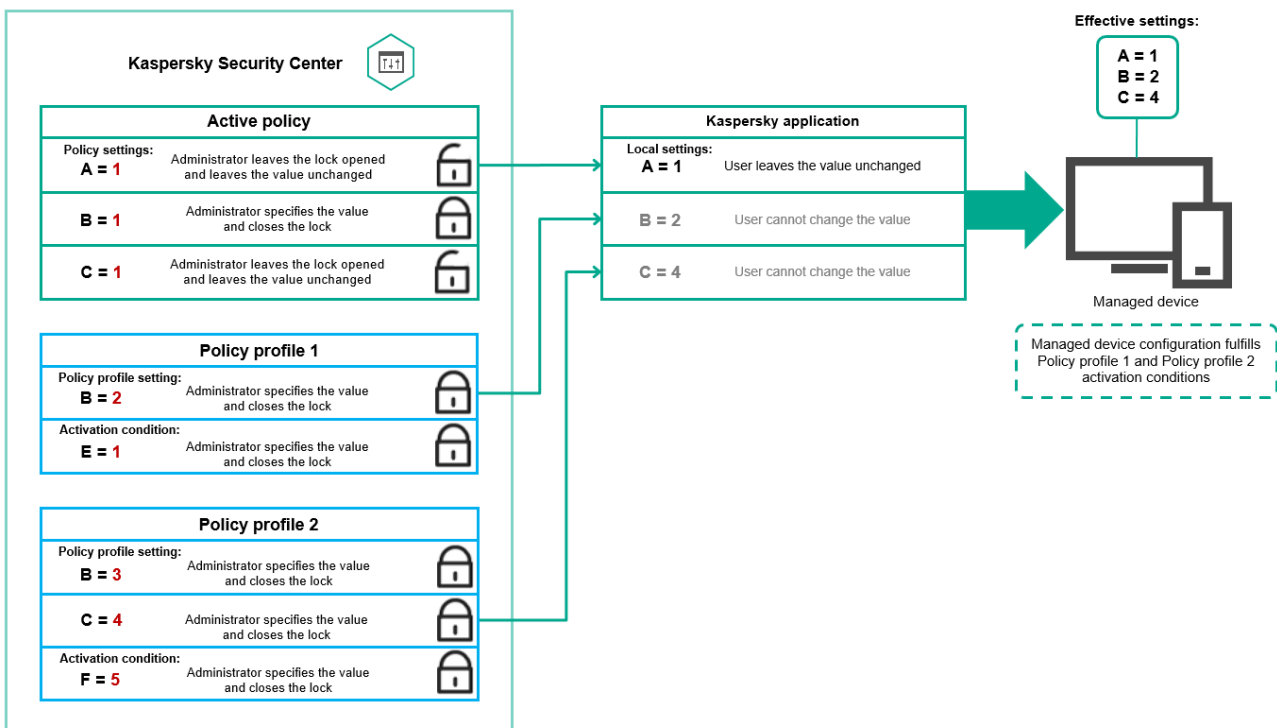
Policy profiles in a hierarchy of policies

Policy profiles have the following priority assignment conditions:

- A profile's position in a policy profile list indicates its priority. You can change a policy profile priority. The highest position in a list indicates the highest priority (see the figure below).



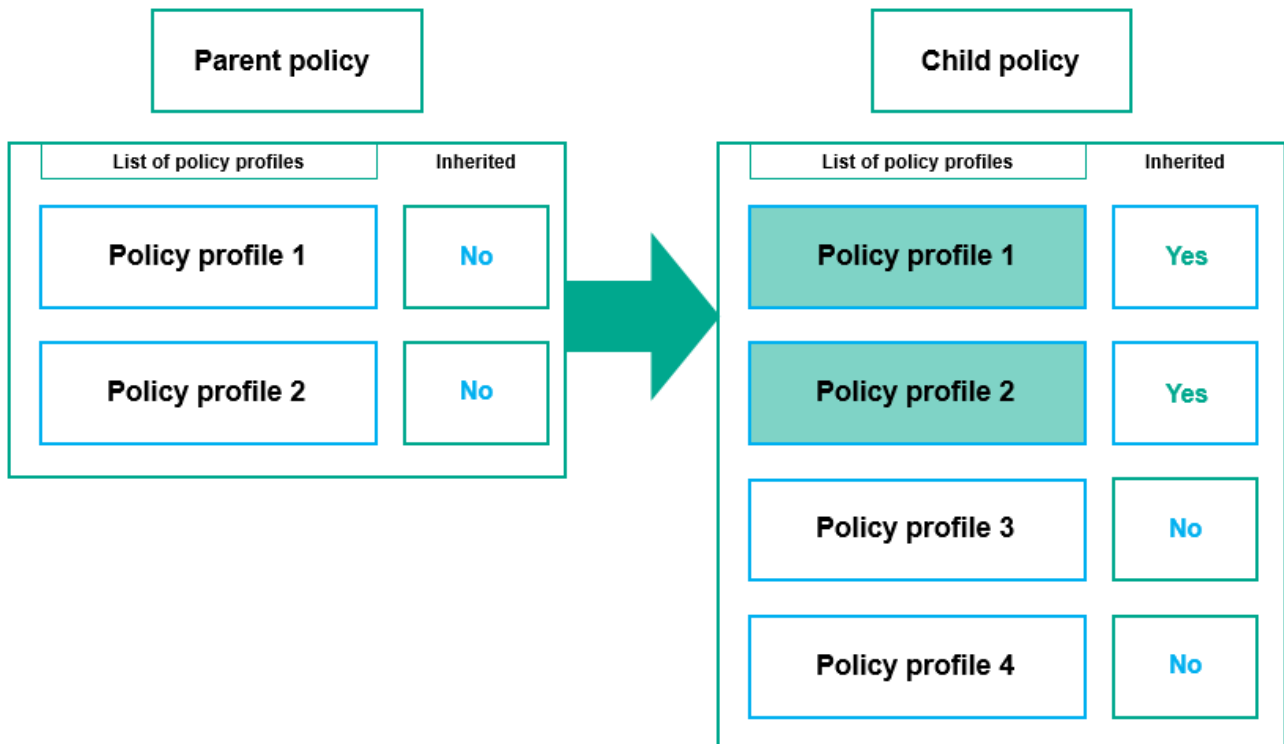
- Activation conditions of policy profiles do not depend on each other. Several policy profiles can be activated simultaneously. If several policy profiles affect the same setting, the device takes the setting value from the policy profile with the highest priority (see the figure below).



Policy profiles in a hierarchy of inheritance

Policy profiles from different hierarchy level policies comply with the following conditions:

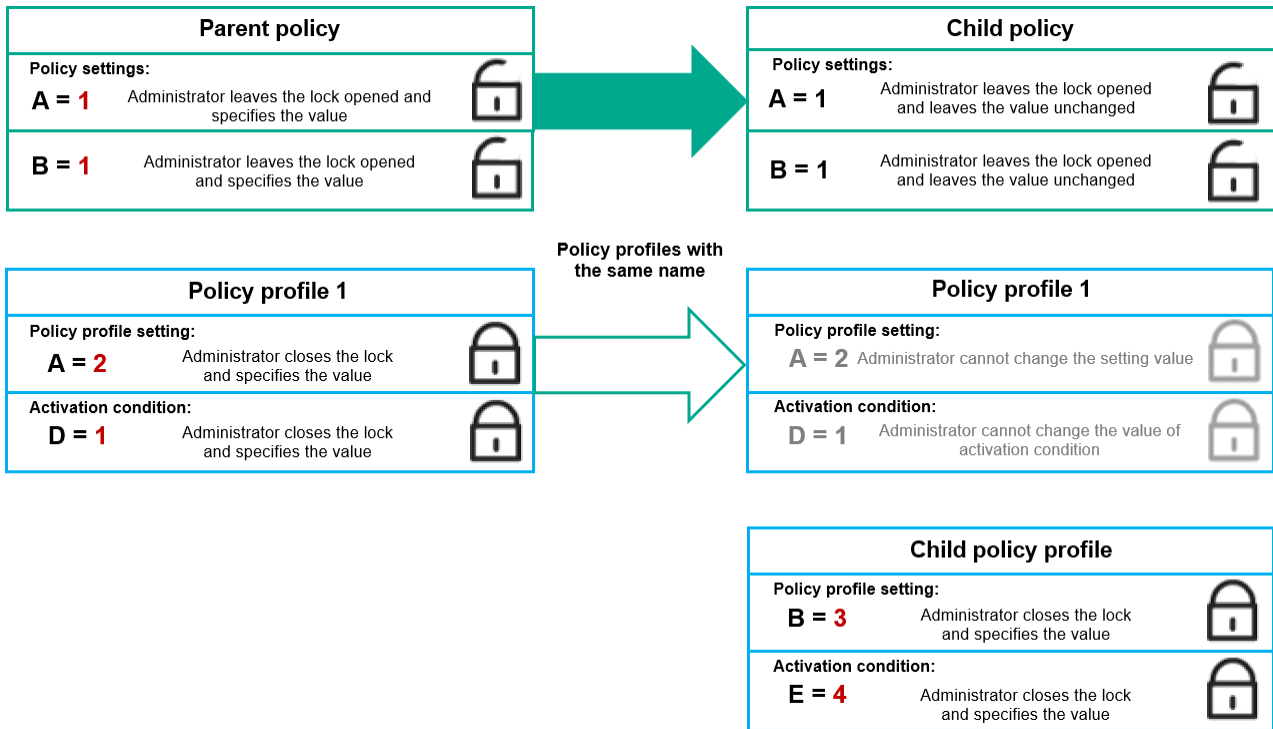
- A lower-level policy inherits policy profiles from a higher-level policy. A policy profile inherited from a higher-level policy obtains higher priority than the original policy profile's level.
- You cannot change a priority of an inherited policy profile (see the figure below).



Policy profiles with the same name

If there are two policies with the same names in different hierarchy levels, these policies function according to the following rules:

- Locked settings and the profile activation condition of a higher-level policy profile changes the settings and profile activation condition of a lower-level policy profile (see the figure below).



- Unlocked settings and the profile activation condition of a higher-level policy profile do not change the settings and profile activation condition of a lower-level policy profile.

How settings are implemented on a managed device

Implementation of an effective policy on a managed device can be described as follows:

- The settings are taken from the basic policy (the policy of an administration group for a managed device).
- Then they are overwritten by the settings (with the closed locks) that are taken from the active policy profile that is the lowest in the list of profiles of this policy.
- Then according to the priority, the settings of each profile that is higher in the list overwrite the settings of the profile that are lower in the list.

Implementation of effective settings on a managed device can be described as follows:

- The values of all settings that have not been locked are taken from the effective policy.
- Then they are overwritten with the values of managed application settings.
- And then the locked settings values from the effective policy are applied. Locked settings values change the values of unlocked effective settings.

See also:

About policies and policy profiles	1110
About lock and locked settings	1111
Hierarchy of policies	1112
Policy profiles in a hierarchy of policies.....	1113

Managing policies

This section describes managing policies and provides information about viewing the list of policies, creating a policy, modifying a policy, copying a policy, moving a policy, forced synchronization, viewing the policy distribution status chart, and deleting a policy.

In this chapter

Viewing the list of policies.....	1118
Creating a policy.....	1118
Modifying a policy.....	1119
General policy settings.....	1120
Enabling and disabling a policy inheritance option.....	1121
Copying a policy.....	1122
Moving a policy.....	1122
Forced synchronization.....	1123
Viewing the policy distribution status chart.....	1124
Activating a policy automatically at the Virus outbreak event.....	1125
Deleting a policy.....	1125

Viewing the list of policies

You can view lists of policies created for the Administration Server or for any administration group.

► To view a list of policies:

1. Go to **DEVICES** → **HIERARCHY OF GROUPS**.
2. In the administration group structure, select the administration group for which you want to view the list of policies.

The list of policies appears in tabular format. If there are no policies, the table is empty. You can show or hide the columns of the table, change their order, view only lines that contain a value that you specify, or use search.

Creating a policy

You can create policies; you can also modify and delete existing policies.

► To create a policy:

1. Go to **DEVICES** → **POLICIES & PROFILES**.
2. Click **Add**.
The **Select application** window opens.
3. Select the application for which you want to create a policy.

4. Click **Next**.

The new policy settings window opens with the **General** tab selected.

5. If you want, change the default name, default status, and default inheritance settings of the policy.

6. Select the **Application settings** tab.

Or, you can click **Save** and exit. The policy will appear in the list of policies, and you can edit its settings later.

7. On the **Application settings** tab, in the left pane select the category that you want and in the results pane on the right, edit the settings of the policy. You can edit policy settings in each category (section).

The set of settings depends on the application for which you create a policy. For details, refer to the following:

- Administration Server configuration (see section "Configuring Administration Server" on page [1007](#))
- Network Agent policy settings (on page [665](#))
- Kaspersky Endpoint Security for Windows documentation
<https://help.kaspersky.com/KESWin/11.6.0/en-US/>

For details about settings of other security applications, refer to the documentation for the corresponding application.

When editing the settings, you can click **Cancel** to cancel the last operation.

8. Click **Save** to save the policy.

The policy will appear in the list of policies.

See also:

Scenario: Kaspersky applications deployment through Kaspersky Security Center 13 Web Console ... [1023](#)

Modifying a policy

► *To modify a policy:*

1. Go to **DEVICES** → **POLICIES & PROFILES**.

2. Click the policy that you want to modify.

The policy settings window opens.

3. Specify the general settings (see section "General policy settings" on page [1120](#)) and the application settings.

The set of application settings depends on the application for which you create a policy. For details, refer to the following:

- Administration Server configuration (see section "Configuring Administration Server" on page [1007](#))
- Network Agent policy settings (on page [665](#))
- Kaspersky Endpoint Security for Windows documentation
<https://help.kaspersky.com/KESWin/11.6.0/en-US/>

For details about settings of other security applications, refer to the documentation for that application.

4. Click **Save**.

The changes made to the policy will be saved in the policy properties, and will appear in the **Revision history** section.

General policy settings

General

In the **General** tab, you can modify the policy status and specify the inheritance of policy settings:

- In the **Policy status** block, you can select one of the policy modes:
 - **Active**

If this option is selected, the policy becomes active.

By default, this option is selected.
 - **Out-of-office**

If this option is selected, the policy becomes active when the device leaves the corporate network. Out-of-office policy is available only for Kaspersky Anti-Virus 6.0 for Windows Workstations MP3 or later.
 - **Inactive**

If this option is selected, the policy becomes inactive, but it is still stored in the **Policies** folder. If required, the policy can be activated.
- In the **Settings inheritance** settings group, you can configure the policy inheritance:
 - **Inherit settings from parent policy**

If this option is enabled, the policy setting values are inherited from the upper-level group policy and, therefore, are locked.

By default, this option is enabled.
 - **Force inheritance of settings in child policies**

If this option is enabled, after policy changes are applied, the following actions will be performed:

 - The values of the policy settings will be propagated to the policies of nested administration groups, that is, to the child policies.
 - In the **Settings inheritance** block of the **General** section in the properties window of each child policy, the **Inherit settings from parent policy** option will be automatically enabled.

If this option is enabled, the child policies settings are locked.

By default, this option is disabled.

Event configuration

The **Event configuration** tab allows you to configure event logging and event notification. Events are distributed by importance level on the following tabs:

- **Critical**

The **Critical** section is not displayed in the Network Agent policy properties.
- **Functional failure**

- **Warning**
- **Info**

In each section, the list shows the types of events and the default event storage term on the Administration Server (in days). Clicking an event type lets you specify the following settings:

- **Event registration**

You can specify how many days to store the event and select where to store the event:

- **Export to SIEM system using Syslog**
- **Store in the OS event log on device**
- **Store in the OS event log on Administration Server**

- **Event notifications**

You can select if you want to be notified about the event in one of the following ways:

- **Notify by email**
- **Notify by SMS**
- **Notify by running an executable file or script**
- **Notify by SNMP**

By default, the notification settings specified on the Administration Server properties tab (such as recipient address) are used. If you want, you can change these settings in the **Email**, **SMS**, and **Executable file to be run** tabs.

Revision history

The **Revision history** tab allows you to view the list of the policy revisions and roll back changes (see section "Rolling back an object to a previous revision" on page [1076](#)) made to the policy, if necessary.

Enabling and disabling a policy inheritance option

► *To enable or disable the inheritance option in a policy:*

1. Open the required policy.
2. Open the **General** tab.
3. Enable or disable policy inheritance:
 - If you enable **Inherit settings from parent policy** in a child policy and an administrator locks some settings in the parent policy, then you cannot change these settings in the child policy.
 - If you disable **Inherit settings from parent policy** in a child policy, then you can change all of the settings in the child policy, even if some settings are locked in the parent policy.
 - If you enable **Force inheritance of settings in child policies** in the parent group, this enables the **Inherit settings from parent policy** option for each child policy. In this case, you cannot disable this option for any child policy. All of the settings that are locked in the parent policy are forcibly inherited in the child groups, and you cannot change these settings in the child groups.
4. Click the **Save** button to save changes or click the **Cancel** button to reject changes.

By default, the **Inherit settings from parent policy** option is enabled for a new policy.

If a policy has profiles, all of the child policies inherit these profiles.

See also:

General policy settings[663](#)

Copying a policy

You can copy policies from one administration group to another.

► *To copy a policy to another administration group:*

1. Go to **DEVICES** → **POLICIES & PROFILES**.
2. Select the check box next to the policy (or policies) that you want to copy.
3. Click the **Copy** button.
On the right side of the screen, the tree of the administration groups appears.
4. In the tree, select the target group, that is, the group to which you want to copy the policy (or policies).
5. Click the **Copy** button at the bottom of the screen.
6. Click **OK** to confirm the operation.

The policy (policies) will be copied to the target group with all its profiles. The status of each copied policy in the target group will be **Inactive**. You can change the status to **Active** at any time.

If a policy with the name identical to that of the newly moved policy already exists in the target group, the name of the newly moved policy is expanded with the (<next sequence number>) index, for example: (1).

Moving a policy

You can move policies from one administration group to another. For example, you want to delete a group, but you want to use its policies for another group. In this case, you may want move the policy from the old group to the new one before deleting the old group.

► *To move a policy to another administration group:*

1. Go to **DEVICES** → **POLICIES & PROFILES**.
2. Select the check box next to the policy (or policies) that you want to move.
3. Click the **Move** button.
On the right side of the screen, the tree of the administration groups appears.
4. In the tree, select the target group, that is, the group to which you want to move the policy (or policies).
5. Click the **Move** button at the bottom of the screen.
6. Click **OK** to confirm the operation.

If a policy is not inherited in the source group, it is moved to the target group with all its profiles. The status of the policy in the target group is **Inactive**. You can change the status to **Active** at any time.

If a policy is inherited in the source group, it remains in the source group. It is copied to the target group with all its profiles. The status of the policy in the target group is **Inactive**. You can change the status to **Active** at any time.

If a policy with the name identical to that of the newly moved policy already exists in the target group, the name of the newly moved policy is expanded with the (<next sequence number>) index, for example: (1).

Forced synchronization

Although Kaspersky Security Center automatically synchronizes the status, settings, tasks, and policies for managed devices, in some cases the administrator must know for certain, at a given moment, whether synchronization has already been performed for a specified device.

Synchronizing a single device

► *To force synchronization between the Administration Server and a managed device:*

1. Go to **DEVICES** → **MANAGED DEVICES**.
2. Click the name of the device that you want to synchronize with the Administration Server.
A property window opens with the **General** section selected.
3. Click the **Force synchronization** button.

The application synchronizes the selected device with the Administration Server.

Synchronizing multiple devices

This feature is applicable only to Kaspersky Security Center 12.1 or a later version.

► *To force synchronization between the Administration Server and multiple managed devices:*

1. Open the device list of an administration group or a device selection:
 - Go to **DEVICES** → **MANAGED DEVICES** → **Groups**, and then select the administration group that contains devices to synchronize.
 - Run a device selection (see section "Device selections" on page [1037](#)) to view the device list.
2. Select the check boxes next to the devices that you want to synchronize with the Administration Server.
3. Click the **Force synchronization** button.
The application synchronizes the selected devices with the Administration Server.
4. In the device list, check that the time of last connection to the Administration Server has changed, for the selected devices, to the current time. If the time has not changed, update the page content by clicking the **Refresh** button.

The selected devices are synchronized with the Administration Server.

Viewing the time of a policy delivery

After changing a policy for a Kaspersky application on the Administration Server, the administrator can check whether the changed policy has been delivered to a specific managed device. A policy can be delivered during a regular synchronization or a forced synchronization.

► *To view the date and time that an application policy was delivered to a managed device:*

1. Go to **DEVICES** → **MANAGED DEVICES**.
2. Click the name of the device that you want to synchronize with the Administration Server.
A property window opens with the **General** section selected.
3. Click the **Applications** tab.
4. Select the application for which you want to view the policy synchronization date.
The application policy window opens with the **General** section selected and the policy delivery date and time displayed.

Viewing the policy distribution status chart

This feature is only available in Kaspersky Security Center 12.2 Web Console or later versions.

In Kaspersky Security Center, you can view the status of policy application on each device in a policy distribution status chart.

► *To view the policy distribution status on each device:*

1. Go to **DEVICES** → **POLICIES & PROFILES**.
2. Select check box next to the name of the policy for which you want to view the distribution status on devices.
3. In the menu that appears, select the **Distribution** link.
The **<Policy name> distribution results** window opens.
4. In the **<Policy name> distribution results** window that opens, the **Status description** of the policy is displayed.



You can change number of results displayed in the list with policy distribution. The maximum number of devices is 100000.

► *To change the number of devices displayed in the list with policy distribution results:*

1. Go to the **Interface options** section in the toolbar.
2. In the **Limit of devices displayed in policy distribution results**, enter the number of devices (up to 100000).
By default, the number is 5000.
3. Click **Save**.
The settings are saved and applied.

Activating a policy automatically at the Virus outbreak event

► *To make a policy perform automatic activation at a Virus outbreak event:*

1. At the top of the screen, click the **Settings** icon () next to the name of the required Administration Server.
The Administration Server properties window opens, with the **General** tab selected.
2. Select the **Virus outbreak** section.
3. In the right pane, click the **Configure policies to activate when a Virus outbreak event occurs** link.
The **Policy activation** window opens.
4. In the section relating to the component that detects a virus outbreak—Anti-Virus for workstations and file servers, Anti-Virus for mail servers, or Anti-Virus for perimeter defense—select the option button next to the entry you want, and then click **Add**.
A window opens with the **Managed devices** administration group.
5. Click the chevron () next to **Managed devices**.
A hierarchy of administration groups and their policies is displayed.
6. In the hierarchy of administration groups and their policies, click the name of a policy or policies that are activated when a virus outbreak is detected.
To select all policies in the list or in a group, select the check box next to the required name.
7. Click the **Save** button.
The window with the hierarchy of administration groups and their policies is closed.

The selected policies are added to the list of policies that are activated when a virus outbreak is detected. The selected policies are activated at the virus outbreak, independent whether they are active or inactive.

If a policy has been activated on the Virus outbreak event, you can return to the previous policy only by using the manual mode.

See also:

| Scenario: Monitoring and reporting[1279](#)

Deleting a policy

You can delete a policy if you do not need it anymore. You can delete only a policy that is not inherited in the specified administration group. If a policy is inherited, you can only delete it in the upper-level group for which it was created.

► *To delete a policy:*

1. Go to **DEVICES** → **POLICIES & PROFILES**.
2. Select the check box next to the policy that you want to delete, and click **Delete**.

The **Delete** button becomes unavailable (dimmed) if you select an inherited policy.

3. Click **OK** to confirm the operation.

The policy is deleted together with all its profiles.

Managing policy profiles

This section describes managing policy profiles and provides information about viewing the profiles of a policy, changing a policy profile priority, creating a policy profile, modifying a policy profile, copying a policy profile, creating a policy profile activation rule, and deleting a policy profile.

In this chapter

Viewing the profiles of a policy	1127
Changing a policy profile priority	1127
Creating a policy profile	1128
Modifying a policy profile	1128
Copying a policy profile.....	1129
Creating a policy profile activation rule.....	1129
Deleting a policy profile.....	1133

Viewing the profiles of a policy

► *To view profiles of a policy:*

1. Go to **DEVICES** → **POLICIES & PROFILES**.
2. Click the name of the policy whose profiles you want to view.
The policy properties window opens with the **General** tab selected.
3. Open the **Policy profiles** tab.

The list of policy profiles appears in tabular format. If the policy does not have profiles, the table is empty.

Changing a policy profile priority

► *To change a policy profile priority:*

1. Proceed to the list of profiles of a policy that you want (see section "Viewing the profiles of a policy" on page [1127](#)).
The list of policy profiles appears.
2. On the **Policy profiles** tab, select the check box next to the policy profile for which you want to change priority.
3. Set a new position of the policy profile in the list by clicking **Prioritize** or **Deprioritize**.

The higher a policy profile is located in the list, the higher its priority.

4. Click the **Save** button.

Priority of the selected policy profile is changed and applied.

See also:

Policy profiles in a hierarchy of policies	1113
Inheritance of policies and policy profiles	1112

Creating a policy profile

You can create policy profiles for a policy.

► *To create a policy profile:*

1. Proceed to the list of profiles for the policy that you want (see section "Viewing the profiles of a policy" on page [1127](#)).
The list of policy profiles appears. If the policy does not have profiles, an empty table appears.
2. Click **Add**.
3. If you want, change the default name and default inheritance settings of the profile.
4. Click the **Application settings** tab.
Or, you can click **Save** and exit. The profile that you have created will appear in the list of policy profiles, and you can edit its settings later.
5. On the **Application settings** tab, in the left pane select the category that you want and in the results pane on the right, edit the settings for the profile. You can edit policy profile settings in each category (section).
When editing the settings, you can click **Cancel** to cancel the last operation.
6. Click **Save** to save the profile.
The profile will appear in the list of policy profiles.

Modifying a policy profile

The capability to edit a policy profile is only available for policies of Kaspersky Endpoint Security for Windows.

► *To modify a policy profile:*

1. Proceed to the list of profiles of a policy that you want (see section "Viewing the profiles of a policy" on page [1127](#)).
The list of policy profiles appears.
2. On the **Policy profiles** tab, click the policy profile that you want to modify.
The policy profile properties window opens.
3. Configure the profile in the properties window:
 - If necessary, on the **General** tab, change the profile name and enable or disable the profile.
 - Edit the profile activation rules (see section "Creating a policy profile activation rule" on page [1129](#)).
 - Edit the application settings.

For details about settings of security applications, please see the documentation of the corresponding application.

4. Click **Save**.

The modified settings will take effect either after the device is synchronized with the Administration Server (if the policy profile is active), or after an activation rule is triggered (if the policy profile is inactive).

Copying a policy profile

You can copy a policy profile to the current policy or to another, for example, if you want to have identical profiles for different policies. You can also use copying if you want to have two or more profiles that differ in only a small number of settings.

► *To copy a policy profile:*

1. Proceed to the list of the profiles of a policy that you want (see section "Viewing the profiles of a policy" on page [1127](#)).

The list of policy profiles appears. If the policy does not have profiles, an empty table appears.

2. On the **Policy profiles** tab, select the policy profile that you want to copy.
3. Click **Copy**.
4. In the window that opens, select the policy to which you want to copy the profile.

You can copy a policy profile to the same policy or to a policy that you specify.

5. Click **Copy**.

The policy profile is copied to the policy that you selected. The newly copied profile gets the lowest priority. If you copy the profile to the same policy, the name of the newly copied profile will be expanded with the () index, for example: (1), (2).

Later, you can change the settings of the profile, including its name and its priority; the original policy profile will not be changed in this case.

Creating a policy profile activation rule

► *To create a policy profile activation rule:*

1. Proceed to the list of profiles of a policy that you want (see section "Viewing the profiles of a policy" on page [1127](#)).

The list of policy profiles appears.

2. On the **Policy profiles** tab, click the policy profile for which you need to create an activation rule.

If the list of policy profiles is empty, you can create a policy profile (see section "Creating a policy profile" on page [1128](#)).

3. On the **Activation rules** tab, click the **Add** button.

The window with policy profile activation rules opens.

4. Specify a name for the rule.
5. Select the check boxes next to the conditions that must affect activation of the policy profile that you are creating:

- **General rules for policy profile activation**

Select this check box to set up policy profile activation rules on the device depending on the status of the device offline mode, rule for connection to Administration Server, and tags assigned to the device.

For this option, specify at the next step:

- **Device status**

Defines the condition for device presence on the network:

- **Online**—The device is on the network, and so the Administration Server is available.
- **Offline**—The device is on an external network, which means that the Administration Server is not available.
- **N/A**—The criterion will not be applied.

- **Rule for Administration Server connection is active on this device**

Choose the condition of policy profile activation (whether the rule is executed or not) and select the rule name.

The rule defines the network location of the device for connection to the Administration Server, whose conditions must be met (or must not be met) for activation of the policy profile.

A network location description of devices for connection to an Administration Server can be created or configured in a Network Agent switching rule.

- **Rules for specific device owner**

For this option, specify at the next step:

- **Device owner**

Select this check box to configure and enable the rule for profile activation on the device according to its owner. In the drop-down list under this check box, you can select a criterion for the profile activation:

- The device belongs to the specified owner ("=" sign).
- The device does not belong to the specified owner ("#" sign).

If this check box is selected, the profile is activated on the device in accordance with the criterion configured. You can specify the device owner when the check box is selected. If this check box is cleared, the profile activation criterion is not applied. By default, this check box is cleared.

- **Device owner is included in an internal security group**

Select this check box to configure and enable the rule of profile activation on the device by the owner's membership in an internal security group of Kaspersky Security Center. In the drop-down list under this check box, you can select a criterion for the profile activation:

- The device owner is a member of the specified security group ("=" sign).
- The device owner is not a member of the specified security group ("#" sign).

If this check box is selected, the profile is activated on the device in accordance with the criterion configured. You can specify a security group of Kaspersky Security Center when this check box is selected. If this check box is cleared, the profile activation criterion is not applied. By default, this check box is cleared.

- **Rules for hardware specifications**

Select this check box to set up rules for policy profile activation on the device depending on the memory volume and the number of logical processors.

For this option, specify at the next step:

- **RAM size, in MB**

Select this check box to configure and enable the rule of profile activation on the device by the RAM volume available on that device. In the drop-down list under this check box, you can select a criterion for the profile activation:

- The device RAM size is less than the specified value (" $<$ " sign).
- The device RAM size is greater than the specified value (" $>$ " sign).

If this check box is selected, the profile is activated on the device in accordance with the criterion configured. When this check box is selected, you can specify the RAM volume on the device. If this check box is cleared, the profile activation criterion is not applied. By default, this check box is cleared.

- **Number of logical processors**

Select this check box to configure and enable the rule of profile activation on the device by the number of logical processors on that device. In the drop-down list under this check box, you can select a criterion for the profile activation:

- The number of logical processors on the device is less than or equal to the specified value (" $<$ " sign).
- The number of logical processors on the device is greater than or equal to the specified value (" $>$ " sign).

If this check box is selected, the profile is activated on the device in accordance with the criterion configured. When this check box is selected, you can specify the number of logical processors on the device. If this check box is cleared, the profile activation criterion is not applied. By default, this check box is cleared.

- **Rules for role assignment**

For this option, specify at the next step:

- **Activate policy profile by specific role of device owner**

Select this option to configure and enable the rule of profile activation on the device depending on the owner's role (see section "Configuring access rights to application features. Role-based access control" on page [683](#)). Add the role manually from the list of existing roles.

If this option is enabled, the profile is activated on the device in accordance with the criterion configured.

- **Rules for tag usage**

Select this check box to set up rules for policy profile activation on the device depending on the tags assigned to the device. You can activate the policy profile to the devices that either have the selected tags or do not have them.

For this option, specify at the next step:

- **Tag list**

In the list of tags, specify the rule for device inclusion in the policy profile by selecting the check boxes next to the relevant tags.

You can add new tags to the list by entering them in the field over the list and clicking the **Add** button.

The policy profile includes devices with descriptions containing all the selected tags. If check boxes are cleared, the criterion is not applied. By default, these check boxes are cleared.

- **Apply to devices without the specified tags**

Select this check box if you have to invert your selection of tags.

If this check box is selected, the policy profile includes devices with descriptions that contain none of the selected tags. If this check box is cleared, the criterion is not applied. By default, this check box is cleared.

- **Rules for Active Directory usage**

Select this check box to set up rules for policy profile activation on the device depending on the presence of the device in an Active Directory organizational unit (OU), or on membership of the device (or its owner) in an Active Directory security group.

For this option, specify at the next step:

- **Device owner's membership in Active Directory security group**

If this check box is selected, the policy profile is activated on the device whose owner is a member of the specified security group. If this check box is cleared, the profile activation criterion is not applied. By default, this check box is cleared.

- **Device membership in Active Directory security group**

If this check box is selected, the policy profile is activated on the device. If this check box is cleared, the profile activation criterion is not applied. By default, this check box is cleared.

- **Device allocation in Active Directory organizational unit**

If this check box is selected, the policy profile is activated on the device, which is included in the specified Active Directory OU. If this check box is cleared, the profile activation criterion is not applied. By default, this check box is cleared.

The number of additional pages of the Wizard depends on the settings that you select at the first step. You can modify policy profile activation rules later.

1. Check the list of the configured parameters. If the list is correct, click **Create**.

The profile will be saved. The profile will be activated on the device when activation rules are triggered.

Policy profile activation rules created for the profile are displayed in the policy profile properties on the **Activation rules** tab. You can modify or remove any policy profile activation rule.

Multiple activation rules can be triggered simultaneously.

Deleting a policy profile

► *To delete a policy profile:*

1. Proceed to the list of profiles of a policy that you want (see section "Viewing the profiles of a policy" on page [1127](#)).

The list of policy profiles appears.

2. On the **Policy profiles** tab, select the check box next to the policy profile that you want to delete, and click **Delete**.

3. In the confirmation window that opens, click **Delete** again.

The policy profile will be deleted. If the policy is inherited by a lower-level group, the profile remains in that group, but becomes the profile of the policy of that group. This is done to eliminate significant change in settings of the managed applications installed on the devices of lower-level groups.

Data encryption and protection

Data encryption reduces the risk of unintentional leakage in case your notebook or hard drive is stolen or lost, or upon access by unauthorized users and applications.

The following Kaspersky applications support encryption:

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Mac

You can show or hide some of the interface elements related to the encryption management feature by using the user interface settings <https://support.kaspersky.com/KSC/CloudConsole/en-US/195133.htm>.

Encryption of data in Kaspersky Endpoint Security for Windows

You can manage BitLocker encryption on devices managed through Kaspersky Endpoint Security for Windows: enable or disable encryption, view the list of encrypted drives, generate and view reports about encryption.

You configure encryption by defining policies of Kaspersky Endpoint Security for Windows in Kaspersky Security Center Cloud Console. Kaspersky Endpoint Security for Windows performs encryption and decryption according to the active policy. For detailed instructions on how to configure rules and a description of encryption features, refer to the Kaspersky Endpoint Security for Windows Online Help <https://support.kaspersky.com/KESWin/11.6.0/en-US/196002.htm>.

Encryption of data in Kaspersky Endpoint Security for Mac

You can use FileVault encryption on devices running macOS. While working with Kaspersky Endpoint Security for Mac, you can enable or disable this encryption.

You configure encryption by defining policies of Kaspersky Endpoint Security for Mac in Kaspersky Security Center Cloud Console. Kaspersky Endpoint Security for Mac performs encryption and decryption according to the active policy. For a detailed description of encryption features, refer to the Kaspersky Endpoint Security for Mac Online Help https://support.kaspersky.com/KESMac/11.1_patchA_adminguide/en-US/159877.htm.

See also

List of supported Kaspersky applications	41 In this section
Viewing the list of encrypted drives	1134
Viewing the list of encryption events	1134
Creating and viewing encryption reports	1135
Granting access to an encrypted drive in offline mode	1136

Viewing the list of encrypted drives

Interface elements related to the encryption management feature are displayed or hidden depending on the user interface settings (see section "Configuring the interface" on page [1014](#)).

► *To view the list of encrypted drives,*

Select **OPERATIONS** → **DATA ENCRYPTION AND PROTECTION**, and in the drop-down list select **ENCRYPTED DRIVES**.

A list of encrypted drives appears.

The window displays information about encrypted drives, and about devices encrypted at the drive level. After the information on a drive is decrypted, the drive is automatically removed from the list.

You can export the list of encrypted drives to a CSV file or TXT file.

Viewing the list of encryption events

When running data encryption or decryption tasks on devices, Kaspersky Endpoint Security for Windows sends Kaspersky Security Center information about events of the following types:

- Cannot encrypt or decrypt a file, or create an encrypted archive due to a lack of free disk space.
- Cannot encrypt or decrypt a file, or create an encrypted archive due to license issues.
- Cannot encrypt or decrypt a file, or create an encrypted archive due to missing access rights.
- The application has been prohibited from accessing an encrypted file.
- Unknown errors.

Interface elements related to the encryption management feature are displayed or hidden depending on the user interface settings (see section "Configuring the interface" on page [1014](#)).

► *To view a list of events that have occurred during data encryption on devices,*

Select **OPERATIONS** → **DATA ENCRYPTION AND PROTECTION**, and in the drop-down list select **ENCRYPTION EVENTS**.

A list of encryption events appears.

The window displays information about problems that have occurred during data encryption on devices.

You can export the list of encrypted devices to a CSV file or TXT file.

Creating and viewing encryption reports

You can generate the following reports:

- Report on encryption status of mass storage devices. This report contains information about the device encryption status for all groups of devices.
- Report on rights of access to encrypted drives. This report contains information about the status of user accounts that have been granted access to encrypted drives.
- Report on file encryption errors. This report contains information about errors that occurred when data encryption or decryption tasks were run on devices.
- Report on blockage of access to encrypted files. This report contains information about blocking application access to encrypted files.

You can generate any report (see section "Generating and viewing a report" on page [1287](#)) in the **REPORTS** section (**MONITORING & REPORTING** → **REPORTS**). Alternatively, you can generate some of the encryption reports in the **ENCRYPTED DRIVES** section and the **ENCRYPTION EVENTS** section.

► *To generate encryption reports in the ENCRYPTED DRIVES section:*

1. Make sure that you enabled the **Show Data encryption and protection** option in the Interface options (see section "Configuring the interface" on page [1014](#)).
2. Select **OPERATIONS** → **DATA ENCRYPTION AND PROTECTION**, and in the drop-down list select **ENCRYPTED DRIVES**.
3. To generate an encryption report, click the name of the report that you want to generate:
 - **Report on encryption status of mass storage devices**
 - **Report on rights to access encrypted drives**

The report generation starts.

► *To generate Report on file encryption errors in the ENCRYPTION EVENTS section:*

1. Make sure that you enabled the **Show Data encryption and protection** option in the Interface options (see section "Configuring the interface" on page [1014](#)).
2. Select **OPERATIONS** → **DATA ENCRYPTION AND PROTECTION**, and in the drop-down list select **ENCRYPTION EVENTS**.
3. To generate the encryption report, click the **Report on file encryption errors** link.

The report generation starts.

Granting access to an encrypted drive in offline mode

A user can request access to an encrypted device, for example, when Kaspersky Endpoint Security for Windows is not installed on the managed device. After you receive the request, you can create an access key file and send it to the user. All of the use cases and detailed instructions are provided in the Kaspersky Endpoint Security for Windows documentation.

► *To grant access to an encrypted drive in offline mode:*

1. Select **OPERATIONS** → **DATA ENCRYPTION AND PROTECTION**, and in the drop-down list select **ENCRYPTED DRIVES**.

A list of encrypted drives appears.

2. Select the drive to which the user requested access.
3. Click the **Grant access to the device in offline mode** button.
4. In the window that opens, select the plug-in corresponding to the Kaspersky application that was used to encrypt the selected drive.

If a drive is encrypted with a Kaspersky application that is not supported by Kaspersky Security Center 13 Web Console, use Microsoft Management Console-based Administration Console to grant the offline access.

5. Follow the instructions provided in the Kaspersky Endpoint Security for Windows documentation.

The user can use the received file to access the encrypted drive and read data stored on the drive.

See also:

- List of Kaspersky applications supported by Kaspersky Security Center 13 Web Console [957](#)

Users and user roles

This section describes users and user roles, and provides instructions for creating and modifying them, for assigning roles and groups to users, and for associating policy profiles with roles.

In this chapter

About user roles.....	1137
Configuring access rights to application features. Role-based access control	1139
Adding an account of an internal user	1161
Creating a user group	1162
Editing an account of an internal user	1162
Editing a user group.....	1163
Adding user accounts to an internal group	1164
Assigning a user as a device owner	1164
Deleting a user or a security group.....	1164
Creating a user role	1165
Editing a user role.....	1165
Editing the scope of a user role	1165
Deleting a user role.....	1166
Associating policy profiles with roles	1167

About user roles

A *user role* (also referred to as a *role*) is an object containing a set of rights and privileges. A role can be associated with settings of Kaspersky applications installed on a user device. You can assign a role to a set of users or to a set of security groups at any level in the hierarchy of administration groups.

You can associate user roles with policy profiles. If a user is assigned a role, this user gets security settings necessary to perform job functions.

A user role can be associated with users of devices in a specific administration group.

User role scope

A *user role scope* is a combination of users and administration groups. Settings associated with a user role apply only to devices that belong to users who have this role, and only if these devices belong to groups associated with this role, including child groups.

Advantage of using roles

An advantage of using roles is that you do not have to specify security settings for each of the managed devices or for each of the users separately. The number of users and devices in a company may be quite large, but the number of different job functions that require different security settings is considerably smaller.

Differences from using policy profiles

Policy profiles are properties of a policy that is created for each Kaspersky application separately. A role is associated with many policy profiles created for different applications. Therefore, a role is a method of uniting settings for a certain user type in one place.

Configuring access rights to application features. Role-based access control

Kaspersky Security Center provides facilities for role-based access to the features of Kaspersky Security Center and of managed Kaspersky applications.

You can configure access rights to application features (on page [1139](#)) for Kaspersky Security Center users in one of the following ways:

- By configuring the rights for each user or group of users individually.
- By creating standard user roles (see section "About user roles" on page [1137](#)) with a predefined set of rights and assigning those roles to users depending on their scope of duties.

Application of user roles is intended to simplify and shorten routine procedures of configuring users' access rights to application features. Access rights within a role are configured in accordance with the standard tasks and the users' scope of duties.

User roles can be assigned names that correspond to their respective purposes. You can create an unlimited number of roles in the application.

You can use the predefined user roles (on page [1155](#)) with already configured set of rights, or create new roles (see section "Creating a user role" on page [1165](#)) and configure the required rights yourself.

In this chapter

Access rights to application features	1139
Predefined user roles.....	1155

Access rights to application features

The table below shows the Kaspersky Security Center features with the access rights to manage the associated tasks, reports, settings, and perform the associated user actions.

To perform the user actions listed in the table, a user has to have the right specified next to the action.

Read, **Modify**, and **Execute** rights are applicable to any task, report, or setting. In addition to these rights, a user has to have the **Perform operations on device selections** right to manage tasks, reports, or settings on device selections.

All tasks, reports, settings, and installation packages that are missing in the table belong to the **General features: Basic functionality** functional area.

Table 83. Access rights to application features

Functional area	Right	User action: right required to perform the action	Task	Report	Other
General features: Management of administration groups	Modify	<ul style="list-style-type: none"> • Add device to an administration group: Modify • Delete device from an administration group: Modify • Add an administration group to another administration group: Modify • Delete an administration group from another administration group: Modify 	None	None	None
General features: Access objects regardless of their ACLs	Read	Get read access to all objects: Read	None	None	None

<p>General features: Basic functionality</p>	<ul style="list-style-type: none"> • Read • Modify • Execute • Perform operations on device selections 	<ul style="list-style-type: none"> • Device moving rules (create, modify, or delete) for the virtual Server: Modify, Perform operations on device selections • Get Mobile (LWNGT) protocol custom certificate: Read • Set Mobile (LWNGT) protocol custom certificate: Write • Get NLA-defined network list: Read • Add, modify, or delete NLA-defined network list: Modify • View Access Control List of groups: Read • View the Kaspersky Event Log: Read 	<ul style="list-style-type: none"> • "Download updates to the Administration Server repository" • "Deliver reports" • "Distribute installation package" • "Install application on secondary Administration Servers remotely" 	<ul style="list-style-type: none"> • "Report on protection status" • "Report on threats" • "Report on most heavily infected devices" • "Report on status of anti-virus databases" • "Report on errors" • "Report on network attacks" • "Summary report on mail system protection applications installed" • "Summary report on perimeter defense applications installed" • "Summary report on types of applications installed" • "Report on users of infected devices" • "Report on incidents" • "Report on events" • "Report on activity of distribution points" • "Report on Secondary Administration Servers" 	<p>None</p>
--	--	--	--	---	-------------

				<p>ion Servers"</p> <ul style="list-style-type: none">• "Report on Device Control events"• "Report on vulnerabilities"• "Report on prohibited applications"• "Report on Web Control"• "Report on encryption status of managed devices"• "Report on encryption status of mass storage devices"• "Report on file encryption errors"• "Report on blockage of access to encrypted files"• "Report on rights to access encrypted devices"• "Report on effective user permissions"• "Report on rights"	
--	--	--	--	--	--

Functional area	Right	User action: right required to perform the action	Task	Report	Other
General features: Deleted objects	<ul style="list-style-type: none"> • Read • Modify 	<ul style="list-style-type: none"> • View deleted objects in the Recycle Bin: Read • Delete objects from the Recycle Bin: Modify 	None	None	None
General features: Event processing	<ul style="list-style-type: none"> • Delete events • Edit event notification settings • Edit event logging settings • Modify 	<ul style="list-style-type: none"> • Change events registration settings: Edit event logging settings • Change events notification settings: Edit event notification settings • Delete events: Delete events 	None	None	Settings: <ul style="list-style-type: none"> • Virus outbreak settings: number of virus detections required to create a virus outbreak event • Virus outbreak settings: period of time for evaluation of virus detections • The maximum number of events stored in the database • Period of time for storing events from the deleted devices

<p>General features: Operations on Administration Server</p>	<ul style="list-style-type: none"> • Read • Modify • Execute • Modify object ACLs • Perform operations on device selections 	<ul style="list-style-type: none"> • Specify ports of Administration Server for the network agent connection : Modify • Specify ports of Activation Proxy launched on the Administration Server: Modify • Specify ports of Activation Proxy for Mobile launched on the Administration Server: Modify • Specify ports of the Web Server for distribution of standalone packages: Modify • Specify ports of the Web Server for distribution of MDM profiles: Modify • Specify SSL ports of the Administration Server for connection via 	<ul style="list-style-type: none"> • "Backup of Administration Server data" • "Database maintenance" 	<p>None</p>	<p>None</p>
---	---	--	--	-------------	-------------

Functional area	Right	User action: right required to perform the action	Task	Report	Other
		<p>Kaspersky Security Center Web Console:</p> <p>Modify</p> <ul style="list-style-type: none"> Specify ports of the Administration Server for mobile connection : Modify Specify the maximum number of events stored in the Administration Server database: Modify Specify the maximum number of events that can be sent by the Administration Server: Modify Specify time period during which events can be sent by the Administration Server: Modify 			

Functional area	Right	User action: right required to perform the action	Task	Report	Other
General features: Kaspersky software deployment	<ul style="list-style-type: none"> • Manage Kaspersky patches • Read • Modify • Execute • Perform operations on device selections 	Approve or decline installation of the patch: Manage Kaspersky patches	None	<ul style="list-style-type: none"> • "Report on license key usage by virtual Administration Server" • "Report on Kaspersky software versions" • "Report on incompatible applications" • "Report on versions of Kaspersky software module updates" • "Report on protection deployment" 	Installation package: "Kaspersky"
General features: Key management	<ul style="list-style-type: none"> • Export key file • Modify 	<ul style="list-style-type: none"> • Export key file: Export key file • Modify Administration Server license key settings: Modify 	None	None	None
General features: Enforced report management	<ul style="list-style-type: none"> • Read • Modify 	<ul style="list-style-type: none"> • Create reports regardless of their ACLs: Write • Execute reports regardless of their ACLs: Read 	None	None	None

Functional area	Right	User action: right required to perform the action	Task	Report	Other
General features: Hierarchy of Administration Servers	Configure hierarchy of Administration Servers	<ul style="list-style-type: none"> Register, update, or delete secondary Administration Servers: Configure hierarchy of Administration Servers 	None	None	None
General features: User permissions	Modify object ACLs	<ul style="list-style-type: none"> Change Security properties of any object: Modify object ACLs Manage user roles: Modify object ACLs Manage internal users: Modify object ACLs Manage security groups: Modify object ACLs Manage aliases: Modify object ACLs 	None	None	None

Functional area	Right	User action: right required to perform the action	Task	Report	Other
<p>General features: Virtual Administration Servers</p>	<ul style="list-style-type: none"> • Manage virtual Administration Servers • Read • Modify • Execute • Perform operations on device selections 	<ul style="list-style-type: none"> • Get list of virtual Administration Servers: Read • Get information on the virtual Administration Server: Read • Create, update, or delete a virtual Administration Server: Manage virtual Administration Servers • Move a virtual Administration Server to another group: Manage virtual Administration Servers • Set administration virtual Server permissions: Manage virtual Administration Servers 	<p>None</p>	<p>"Report on results of installation of third-party software updates"</p>	<p>None</p>

<p>Mobile device management: General</p>	<ul style="list-style-type: none"> • Connect new devices • Send only information commands to mobile devices • Send commands to mobile devices • Manage certificates • Read • Modify 	<ul style="list-style-type: none"> • Get Key Management Service restore data: Read • Delete user certificates: Manage certificates • Get user certificate public part: Read • Check if Public Key Infrastructure is enabled: Read • Check Public Key Infrastructure account: Read • Get Public Key Infrastructure templates: Read • Get Public Key Infrastructure templates by Extended Key Usage certificate: Read • Check if Public Key Infrastructure certificate is revoked: Read • Update user certificate issuance 	<p>None</p>	<p>None</p>	<p>None</p>
--	---	---	-------------	-------------	-------------

		<p>settings:</p> <ul style="list-style-type: none">• Manage certificates• Get user certificate issuance settings: Read• Get packages by application name and version: Read• Set or cancel user certificate: Manage certificates• Renew user certificate: Manage certificates• Set user certificate tag: Manage certificates• Run generation of MDM installation package; cancel generation of MDM installation package: Connect new devices			
--	--	--	--	--	--

Functional area	Right	User action: right required to perform the action	Task	Report	Other
System management: Connectivity	<ul style="list-style-type: none"> • Start RDP sessions • Connect to existing RDP sessions • Initiate tunneling • Save files from devices to the administrator's workstation • Read • Modify • Execute • Perform operations on device selections 	<ul style="list-style-type: none"> • Create desktop sharing session: The right to create desktop sharing session • Create RDP session: Connect to existing RDP sessions • Create tunnel: Initiate tunneling • Save content network list: Save files from devices to the administrator's workstation 	None	"Report on device users"	None

Functional area	Right	User action: right required to perform the action	Task	Report	Other
System management: Hardware inventory	<ul style="list-style-type: none"> • Read • Modify • Execute • Perform operations on device selections 	<ul style="list-style-type: none"> • Get or export hardware inventory object: Read • Add, set or delete hardware inventory object: Write 	None	<ul style="list-style-type: none"> • "Report on hardware registry" • "Report on configuration changes" • "Report on hardware" 	None
System management: Network access control	<ul style="list-style-type: none"> • Read • Modify 	<ul style="list-style-type: none"> • View CISCO settings: Read • Change CISCO settings: Write 	None	None	None

Functional area	Right	User action: right required to perform the action	Task	Report	Other
System management: Operating system deployment	<ul style="list-style-type: none"> • Deploy PXE servers • Read • Modify • Execute • Perform operations on device selections 	<ul style="list-style-type: none"> • Deploy PXE servers: Deploy PXE servers • View a list of PXE servers: Read • Start or stop the installation process on PXE clients: Execute • Manage drivers for WinPE and operating system images: Modify 	"Create installation package upon reference device OS image"	None	Installation package: "OS Image"
System management: Vulnerability and patch management	<ul style="list-style-type: none"> • Read • Modify • Execute • Perform operations on device selections 	<ul style="list-style-type: none"> • View third-party patch properties: Read • Change third-party patch properties: Modify 	<ul style="list-style-type: none"> • "Perform Windows Update synchronization" • "Install Windows Update updates" • "Fix vulnerabilities" • "Install required updates and fix vulnerabilities" 	"Report on software updates"	None

Functional area	Right	User action: right required to perform the action	Task	Report	Other
System management: Remote installation	<ul style="list-style-type: none"> • Read • Modify • Execute • Perform operations on device selections 	<ul style="list-style-type: none"> • View third-party Vulnerability and Patch Management based installation package properties: Read • Change third-party Vulnerability and Patch Management based installation package properties: Modify 	None	None	Installation packages: <ul style="list-style-type: none"> • "Custom application" • "VAPM package"
System management: Software inventory	<ul style="list-style-type: none"> • Read • Modify • Execute • Perform operations on device selections 	None	None	<ul style="list-style-type: none"> • "Report on installed applications" • "Report on applications registry history" • "Report on status of licensed applications groups" • "Report on third-party software license keys" 	None

Predefined user roles

User roles assigned to Kaspersky Security Center users provide them with sets of access rights to application features (on page [684](#)).

You can use the predefined user roles with already configured set of rights, or create new roles and configure the required rights yourself. Some of the predefined user roles available in Kaspersky Security Center can be associated with specific job positions, for example, **Auditor**, **Security Officer**, **Supervisor** (these roles are present in Kaspersky Security Center starting from the version 11). Access rights of these roles are pre-configured in accordance with the standard tasks and scope of duties of the associated positions. The table below shows how roles can be associated with specific job positions.

Table 84. *Examples of roles for specific job positions*

Role	Comment
Auditor	Permits all operations with all types of reports, all viewing operations, including viewing deleted objects (grants the Read and Modify permissions in the Deleted objects area). Does not permit other operations. You can assign this role to a person who performs the audit of your organization.
Supervisor	Permits all viewing operations; does not permit other operations. You can assign this role to a security officer and other managers in charge of the IT security in your organization.
Security Officer	Permits all viewing operations, permits reports management; grants limited permissions in the System management: Connectivity area. You can assign this role to an officer in charge of the IT security in your organization.

The table below shows the access rights assigned to each predefined user role.

Table 85. Access rights of predefined user roles

Role	Description
Administration Server Administrator	<p>Permits all operations in the following functional areas:</p> <ul style="list-style-type: none"> • General features: <ul style="list-style-type: none"> • Basic functionality • Event processing • Hierarchy of Administration Servers • Virtual Administration Servers • System management: <ul style="list-style-type: none"> • Connectivity • Hardware inventory • Software inventory
Administration Server Operator	<p>Grants the Read and Execute rights in all of the following functional areas:</p> <ul style="list-style-type: none"> • General features: <ul style="list-style-type: none"> • Basic functionality • Virtual Administration Servers • System management: <ul style="list-style-type: none"> • Connectivity • Hardware inventory • Software inventory
Auditor	<p>Permits all operations in the following functional areas:</p> <ul style="list-style-type: none"> • General features: <ul style="list-style-type: none"> • Access objects regardless of their ACLs • Deleted objects • Enforced report management <p>You can assign this role to a person who performs the audit of your organization.</p>

Role	Description
Installation Administrator	<p>Permits all operations in the following functional areas:</p> <ul style="list-style-type: none"> • General features: <ul style="list-style-type: none"> • Basic functionality • Kaspersky software deployment • License key management • System management: <ul style="list-style-type: none"> • Operating system deployment • Vulnerability and patch management • Remote installation • Software inventory <p>Grants Read and Execute rights in the General features: Virtual Administration Servers functional area.</p>
Installation Operator	<p>Grants the Read and Execute rights in all of the following functional areas:</p> <ul style="list-style-type: none"> • General features: <ul style="list-style-type: none"> • Basic functionality • Kaspersky software deployment (also grants the Manage Kaspersky patches right in this area) • Virtual Administration Servers • System management: <ul style="list-style-type: none"> • Operating system deployment • Vulnerability and patch management • Remote installation • Software inventory
Kaspersky Endpoint Security Administrator	<p>Permits all operations in the following functional areas:</p> <ul style="list-style-type: none"> • General features: Basic functionality • Kaspersky Endpoint Security area, including all features
Kaspersky Endpoint Security Operator	<p>Grants the Read and Execute rights in all of the following functional areas:</p> <ul style="list-style-type: none"> • General features: Basic functionality • Kaspersky Endpoint Security area, including all features
Main Administrator	<p>Permits all operations in functional areas, <i>except</i> for the following areas:</p> <ul style="list-style-type: none"> • General features: <ul style="list-style-type: none"> • Access objects regardless of their ACLs • Enforced report management

Role	Description
Main Operator	<p>Grants the Read and Execute (where applicable) rights in all of the following functional areas:</p> <ul style="list-style-type: none"> • General features: <ul style="list-style-type: none"> • Basic functionality • Deleted objects • Operations on Administration Server • Kaspersky Lab software deployment • Virtual Administration Servers • Mobile Device Management: General • System management, including all features • Kaspersky Endpoint Security area, including all features
Mobile Device Management Administrator	<p>Permits all operations in the following functional areas:</p> <ul style="list-style-type: none"> • General features: Basic functionality • Mobile Device Management: General
Mobile Device Management Operator	<p>Grants the Read and Execute rights in the General features: Basic functionality functional area.</p> <p>Grants Read and Send only information commands to mobile devices in the following functional areas:</p> <ul style="list-style-type: none"> • Mobile Device Management: General
Security Officer	<p>Permits all operations in the following functional areas:</p> <ul style="list-style-type: none"> • General features: <ul style="list-style-type: none"> • Access objects regardless of their ACLs • Enforced report management <p>Grants the Read, Modify, Execute, Save files from devices to the administrator's workstation, and Perform operations on device selections rights in the System management: Connectivity functional area.</p> <p>You can assign this role to an officer in charge of the IT security in your organization.</p>
Self Service Portal User	<p>Permits all operations in the Mobile Device Management: Self Service Portal functional area. This feature is not supported in Kaspersky Security Center 11 and later version.</p>

Role	Description
Supervisor	Grants the Read right in the General features: Access objects regardless of their ACLs and General features: Enforced report management functional area. You can assign this role to a security officer and other managers in charge of the IT security in your organization.
Vulnerability and Patch Management Administrator	Permits all operations in the General features: Basic functionality and System management (including all features) functional areas.
Vulnerability and Patch Management Operator	Grants the Read and Execute (where applicable) rights in the General features: Basic functionality and System management (including all features) functional areas.

Adding an account of an internal user

► *To add a new internal user account to Kaspersky Security Center:*

1. Go to **USERS & ROLES** → **USERS**.
2. Click **Add**.
3. In the **New entity** window that opens, specify the settings of the new user account:
 - Keep the default option **User**.
 - **Name**.
 - **Password** for the user connection to Kaspersky Security Center.

The password must comply with the following rules:

- The password must be 8 to 16 characters long.
- The password must contain characters from at least three of the groups listed below:
 - Uppercase letters (A-Z)
 - Lowercase letters (a-z)
 - Numbers (0-9)
 - Special characters (@ # \$ % ^ & * - _ ! + = [] { } | : ' , . ? / \ ` ~ " () ;)
- The password must not contain any whitespaces, Unicode characters, or the combination of "." and "@", when "." is placed before "@".

To see the characters that you entered, click and hold the **Show** button.

The number of attempts for entering the password is limited. By default, the maximum number of allowed password entry attempts is 10. You can change the allowed number of attempts to enter a password, as described in "Changing the number of allowed password entry attempts" (see section "Changing the number of allowed password entry attempts" on page [681](#)).

If the user enters an invalid password the specified number of times, the user account is blocked for one hour. You can unblock the user account only by changing the password.

- **Full name**
- **Description**
- **Email address**
- **Phone**

4. Click **OK** to save the changes.

The new user account appears in the list of users and user groups.

Creating a user group

► *To create a user group:*

1. Go to **USERS & ROLES** → **USERS**.
2. Click **Add**.
3. In the **New entity** window opens, select **Group**.
4. Specify the following settings for the new user group:
 - **Group name**
 - **Description**
5. Click **OK** to save the changes.

The new user group appears in the list of users and user groups.

Editing an account of an internal user

► *To edit an internal user account in Kaspersky Security Center:*

1. Go to **USERS & ROLES** → **USERS**.
2. Click the name of the user account that you want to edit.
3. In the user settings window that opens, on the **General** tab, change the settings of the user account:
 - **Description**
 - **Full name**
 - **Email address**
 - **Main phone**
 - **Password** for the user connection to Kaspersky Security Center.

The password must comply with the following rules:

- The password must be 8 to 16 characters long.
- The password must contain characters from at least three of the groups listed below:
 - Uppercase letters (A-Z)

- Lowercase letters (a-z)
- Numbers (0-9)
- Special characters (@ # \$ % ^ & * - _ ! + = [] { } | : ' , . ? / \ ` ~ " () ;)
- The password must not contain any whitespaces, Unicode characters, or the combination of "." and "@", when "." is placed before "@".

To see the entered password, click and hold the **Show** button.

The number of attempts for entering the password is limited. By default, the maximum number of allowed password entry attempts is 10. You can change the allowed number of attempts to enter a password, as described in "Changing the number of allowed password entry attempts" (see section "Changing the number of allowed password entry attempts" on page [681](#)). If the user enters an invalid password the specified number of times, the user account is blocked for one hour. You can unblock the user account only by changing the password.

- If necessary, switch the toggle button to **Disabled** to prohibit the user from connecting to the application. You can disable an account, for example, after an employee leaves the company.
4. On the **Authentication security** tab, you can specify the security settings for this account.
 5. On the **Groups** tab, you can add the user to security groups.
 6. On the **Devices** tab, you can assign devices (see section "Assigning a user as a device owner" on page [1164](#)) to the user.
 7. On the **Roles** tab, you can assign roles (see section "Editing the scope of a user role" on page [1165](#)) to the user.
 8. Click **Save** to save the changes.

The updated user account appears in the list of users and security groups.

Editing a user group

You can edit only internal groups.

► *To edit a user group:*

1. Go to **USERS & ROLES** → **USERS**.
2. Click the name of the user group that you want to edit.
3. In the group settings window that opens, change the settings of the user group:
 - **Name**
 - **Description**
4. Click **Save** to save the changes.

The updated user group appears in the list of users and user groups.

Adding user accounts to an internal group

You can add only accounts of internal users to an internal group.

► To add user accounts to an internal group:

1. Go to **USERS & ROLES** → **USERS**.
2. Select check boxes next to user accounts that you want to add to a group.
3. Click the **Assign group** button.
4. In the **Assign group** window that opens, select the group to which you want to add user accounts.
5. Click the **Assign** button.

The user accounts are added to the group.

Assigning a user as a device owner

► To assign a user as a device owner:

1. Go to **USERS & ROLES** → **USERS**.
2. Click the name of the user account that you want to assign as a device owner.
3. In the user settings window that opens, click the **Devices** tab.
4. Click **Add**.
5. From the device list, select the device that you want to assign to the user.
6. Click **OK**.

The selected device is added to the list of devices assigned to the user.

You can perform the same operation at **DEVICES** → **MANAGED DEVICES**, by clicking the name of the device that you want to assign, and then clicking the **Manage device owner** link.

Deleting a user or a security group

You can delete only internal users or internal security groups.

► To delete a user or a security group:

1. Go to **USERS & ROLES** → **USERS**.
2. Select the check box next to the user or the security group that you want to delete.
3. Click **Delete**.
4. In the window that opens, click **OK**.

The user or the security group is deleted.

Creating a user role

► *To create a user role:*

1. Go to **USERS & ROLES** → **Roles**.
2. Click **Add**.
3. In the **New role name** window that opens, enter the name of the new role.
4. Click **OK** to apply the changes.
5. In the role properties window that opens, change the settings of the role:
 - On the **General** tab, edit the role name.
You cannot edit the name of a predefined role.
 - On the **Settings** tab, edit the role scope (see section "Editing the scope of a user role" on page [1165](#)) and policies and profiles associated with the role.
 - On the **Access rights** tab, edit the rights for access to Kaspersky applications.
6. Click **Save** to save the changes.

The new role appears in the list of user roles.

Editing a user role

► *To edit a user role:*

1. Go to **USERS & ROLES** → **Roles**.
2. Click the name of the role that you want to edit.
3. In the role properties window that opens, change the settings of the role:
 - On the **General** tab, edit the role name.
You cannot edit the name of a predefined role.
 - On the **Settings** tab, edit the role scope (see section "Editing the scope of a user role" on page [1165](#)) and policies and profiles associated with the role.
 - On the **Access rights** tab, edit the rights for access to Kaspersky applications.
4. Click **Save** to save the changes.

The updated role appears in the list of user roles.

Editing the scope of a user role

A *user role scope* is a combination of users and administration groups. Settings associated with a user role apply only to devices that belong to users who have this role, and only if these devices belong to groups associated with this role, including child groups.

To add users, security groups, and administration groups to the scope of a user role, you can use either of the following methods:

► *Method 1:*

1. Go to **USERS & ROLES** → **USERS**.
2. Select check boxes next to the users and security groups that you want to add to the user role scope.
3. Click the **Assign role** button.
The Role Assignment Wizard starts. Proceed through the Wizard by using the **Next** button.
4. On the **Select role** page of the Wizard, select the user role that you want to assign.
5. On the **Define scope** page of the Wizard, select the administration group that you want to add to the user role scope.
6. Click the **Assign role** button to close the Wizard.

The selected users or security groups and the selected administration group are added to the scope of the user role.

► *Method 2:*

1. Go to **USERS & ROLES** → **Roles**.
2. Click the name of the role for which you want to define the scope.
3. In the role properties window that opens, click the **Settings** tab.
4. In the **Role scope** section, click **Add**.
The Role Assignment Wizard starts. Proceed through the Wizard by using the **Next** button.
5. On the **Define scope** page of the Wizard, select the administration group that you want to add to the user role scope.
6. On the **Select users** page of the Wizard, select users and security groups that you want to add to the user role scope.
7. Click the **Assign role** button to close the Wizard.
8. Click the **Close** button (✕) to close the role properties window.

The selected users or security groups and the selected administration group are added to the scope of the user role.

Deleting a user role

► *To delete a user role:*

1. Go to **USERS & ROLES** → **Roles**.
2. Select the check box next to the name of the role that you want to delete.
3. Click **Delete**.
4. In the window that opens, click **OK**.

The user role is deleted.

Associating policy profiles with roles

You can associate user roles with policy profiles. In this case, the activation rule for this policy profile is based on the role: the policy profile becomes active for a user that has the specified role.

For example, the policy bars any GPS navigation software on all devices in an administration group. GPS navigation software is necessary only on a single device in the Users administration group—the device owned by a courier. In this case, you can assign a "Courier" role (see section "About user roles" on page [1137](#)) to its owner, and then create a policy profile allowing GPS navigation software to run only on the devices whose owners are assigned the "Courier" role. All the other policy settings are preserved. Only the user with the role "Courier" will be allowed to run GPS navigation software. Later, if another worker is assigned the "Courier" role, the new worker also can run navigation software on your organization's device. Running GPS navigation software will still be prohibited on other devices in the same administration group.

► *To associate a role with a policy profile:*

1. Go to **USERS & ROLES** → **Roles**.
2. Click the name of the role that you want to associate with a policy profile.
The role properties window opens with the **General** tab selected.
3. Select the **Settings** tab, and scroll down to the **Policies & Profiles** section.
4. Click **Edit**.
5. To associate the role with:
 - **An existing policy profile**—Click the chevron icon (➤) next to the required policy name, and then select the check box next to the profile with which you want to associate the role.
 - **A new policy profile:**
 - a. Select the check box next to the policy for which you want to create a profile.
 - b. Click **New policy profile**.
 - c. Specify a name for the new profile and configure the profile settings.
 - d. Click the **Save** button.
 - e. Select the check box next to the new profile.
6. Click **Assign to role**.

The profile is associated with the role and appears in the role properties. The profile applies automatically to any device whose owner is assigned the role.

Kaspersky Security Network (KSN)

This section describes how to use an online service infrastructure named Kaspersky Security Network (KSN). The section provides the details on KSN, as well as instructions on how to enable KSN, configure access to KSN, and view the statistics of the use of KSN proxy server.

In this chapter

About KSN	1168
Setting up access to Kaspersky Security Network	1169
Enabling and disabling KSN	1171
Viewing the accepted KSN Statement.....	1171
Accepting an updated KSN Statement	1172
Checking whether the distribution point works as KSN Proxy.....	1172

About KSN

Kaspersky Security Network (KSN) is an online service infrastructure that provides access to the online Knowledge Base of Kaspersky, which contains information about the reputation of files, web resources, and software. The use of data from Kaspersky Security Network ensures faster responses by Kaspersky applications to threats, improves the effectiveness of some protection components, and reduces the risk of false positives. KSN allows you to use Kaspersky reputation databases to retrieve information about applications installed on managed devices.

By participating in KSN, you agree to send to Kaspersky in automatic mode information about the operation of Kaspersky applications installed on client devices that are managed through Kaspersky Security Center. Information is transferred in accordance with the current KSN access settings (see section "Setting up access to Kaspersky Security Network" on page [786](#)).

The application prompts you to join KSN while running the Quick Start Wizard. You can start or stop using KSN at any moment when using the application (see section "Enabling and disabling KSN" on page [788](#)).

You use KSN in accordance with the KSN Statement that you read and accept when you enable KSN. If the KSN Statement is updated, it is displayed to you when you update or upgrade Administration Server. You can accept the updated KSN Statement or decline it. If you decline it, you keep using KSN in accordance with the previous version of KSN Statement that you accepted before.

Client devices managed by the Administration Server interact with KSN through KSN Proxy. KSN Proxy provides the following features:


- Client devices can send requests to KSN and transfer information to KSN even if they do not have direct access to the Internet.
- The KSN proxy server caches processed data, thus reducing the load on the outbound channel and the time period spent for waiting for information requested by a client device.

You can configure the KSN proxy server in the **KSN Proxy** section of the Administration Server properties window (see section "Setting up access to Kaspersky Security Network" on page [786](#)).

Setting up access to Kaspersky Security Network

You can set up access to Kaspersky Security Network (KSN) on the Administration Server and on a distribution point.

► *To set up Administration Server access to Kaspersky Security Network (KSN):*

1. Click the **Settings** icon () next to the name of the required Administration Server.

The Administration Server properties window opens.

2. On the **General** tab, select the **KSN Proxy settings** section.
3. Switch the toggle button to the **Enable KSN Proxy on Administration Server ENABLED** position.

Data is sent from client devices to KSN in accordance with the Kaspersky Endpoint Security policy, which is active on those client devices. If this check box is cleared, no data will be sent to KSN from the Administration Server and client devices through Kaspersky Security Center. However, client devices can send data to KSN directly (bypassing Kaspersky Security Center), in accordance with their respective settings. The Kaspersky Endpoint Security for Windows policy, which is active on client devices, determines which data will be sent directly (bypassing Kaspersky Security Center) from those devices to KSN.

4. Switch the toggle button to the **Use Kaspersky Security Network ENABLED** position.

If this option is enabled, client devices send patch installation results to Kaspersky. When enabling this option, make sure to read and accept the terms of the KSN Statement.

If you are using Private KSN, switch the toggle button to the **Use Kaspersky Private Security Network ENABLED** position and click the **Select file with KSN Proxy settings** button to download the settings of Private KSN (files with the extensions pkcs7 and pem). After the settings are downloaded, the interface displays the provider's name and contacts, as well as the creation date of the file with the settings of Private KSN.

When you enable Private KSN, pay attention to the distribution points configured to send KSN requests directly to the Cloud KSN. The distribution points that have Network Agent version 11 (or earlier) installed will continue to send KSN requests to the Cloud KSN. To reconfigure the distribution points to send KSN requests to Private KSN, enable the **Forward KSN requests to Administration Server** option for each distribution point. You can enable this option in the distribution point properties or in the Network Agent policy.

When you switch the toggle button to the **Use Kaspersky Private Security Network ENABLED** position, a message appears with details about Private KSN.

The following Kaspersky applications support Private KSN:

- Kaspersky Security Center 10 Service Pack 1 or later
- Kaspersky Endpoint Security 10 Service Pack 1 for Windows or later
- Kaspersky Security for Virtualization 3.0 Agentless Service Pack 2
- Kaspersky Security for Virtualization 3.0 Service Pack 1 Light Agent

If you enable Private KSN in Kaspersky Security Center, these applications receive information about supporting Private KSN. In the settings window of the application, in the **Kaspersky Security Network** subsection of the **Advanced Threat Protection** section, **KSN provider: Private KSN** is displayed. Otherwise, **KSN provider: Global KSN** is displayed.

If you use application versions earlier than Kaspersky Security for Virtualization 3.0 Agentless Service Pack 2 or earlier than Kaspersky Security for Virtualization 3.0 Service Pack 1 Light Agent when running Private KSN, we recommend that you use secondary Administration Servers for which the use of Private KSN has not been enabled.

Kaspersky Security Center does not send any statistical data to Kaspersky Security Network if Private KSN is configured in the **KSN Proxy settings** section of the Administration Server properties window.

If you have the proxy server settings configured in the Administration Server properties, but your network architecture requires that you use Private KSN directly, enable the **Ignore KSC proxy server settings when connecting to Private KSN** option. Otherwise, requests from the managed applications cannot reach Private KSN.

5. Configure the Administration Server connection to the KSN Proxy service:
 - Under **Connection settings**, for the **TCP port**, specify the number of the TCP port that will be used for connecting to the KSN Proxy server. The default port to connect to the KSN Proxy server is 13111.
 - If you want the Administration Server to connect to the KSN Proxy server through a UDP port, enable the **Use UDP port** option and specify a port number for the **UDP port**. By default, this option is disabled, and TCP port is used. If this option is enabled, the default UDP port to connect to the KSN Proxy server is 15111.
6. Switch the toggle button to the **Connect secondary Administration Servers to KSN through primary Administration Server ENABLED** position.

If this option is enabled, secondary Administration Servers use the primary Administration Server as the KSN proxy server. If this option is disabled, secondary Administration Servers connect to KSN on their own. In this case, managed devices use secondary Administration Servers as KSN proxy servers.


Secondary Administration Servers use the primary Administration Server as a proxy server if in the right pane of the **KSN Proxy settings** section, in the properties of secondary Administration Servers the toggle button is switched to the **Enable KSN Proxy on Administration Server ENABLED** position.

7. Click the **Save** button.

The KSN access settings will be saved.

You can also set up distribution point access to KSN, for example, if you want to reduce the load on the Administration Server. The distribution point that acts as a KSN proxy server sends KSN requests from managed devices to Kaspersky directly, without using the Administration Server.

► *To set up distribution point access to Kaspersky Security Network (KSN):*

1. Make sure that the distribution point is assigned manually (see section "Assigning distribution points manually" on page [1204](#)).
2. In the main application window, click the **Settings** icon () next to the name of the required Administration Server.

The Administration Server properties window opens.


3. On the **General** tab, select the **Distribution points** section.
4. Click the name of the distribution point to open its properties window.

5. In the distribution point properties window, in the **KSN Proxy** section, enable the **Enable KSN Proxy on distribution point side** option, and then enable the **Access KSN Cloud / Private KSN directly over the Internet** option.
6. Click **OK**.

The distribution point will act as a KSN Proxy server.

Enabling and disabling KSN


► *To enable KSN:*

1. Click the **Settings** icon () next to the name of the required Administration Server.
The Administration Server properties window opens.
2. On the **General** tab, select the **KSN Proxy settings]** section.
3. Switch the toggle button to the **Enable KSN Proxy on Administration Server ENABLED** position.
The KSN proxy server is enabled.
4. Switch the toggle button to the **Use Kaspersky Security Network ENABLED** position.
KSN will be enabled.

If the toggle button is enabled, client devices send patch installation results to Kaspersky. When enabling this toggle button, you should read and accept the terms of the KSN Statement.

5. Click the **Save** button.

► *To disable KSN:*

1. Click the **Settings** icon () next to the name of the required Administration Server.
The Administration Server properties window opens.
2. On the **General** tab, select the **KSN Proxy settings]** section.
3. Switch the toggle button to the **Enable KSN Proxy on Administration Server DISABLED** position to disable the KSN Proxy service, or switch the toggle button to the **Use Kaspersky Security Network DISABLED** position.

If this toggle button is disabled, client devices will send no patch installation results to Kaspersky.

If you are using Private KSN, switch the toggle button to the **Use Kaspersky Private Security Network DISABLED** position.


KSN will be disabled.

4. Click the **Save** button.

Viewing the accepted KSN Statement

When you enable Kaspersky Security Network (KSN), you must read and accept the KSN Statement. You can view the accepted KSN Statement at any time.

► *To view the accepted KSN Statement:*

1. Click the **Settings** icon () next to the name of the required Administration Server.

The Administration Server properties window opens.

2. On the **General** tab, select the **KSN Proxy settings** section.
3. Click the **View Kaspersky Security Network Statement** link.

In the window that opens, you can view the text of the accepted KSN Statement.

Accepting an updated KSN Statement

You use KSN in accordance with the KSN Statement (see section "Viewing the accepted KSN Statement" on page [1171](#)) that you read and accept when you enable KSN. If the KSN Statement is updated, it is displayed to you when you update or upgrade Administration Server. You can accept the updated KSN Statement or decline it. If you decline it, you keep using KSN in accordance with the version of the KSN Statement that you previously accepted.

After updating or upgrading Administration Server, the updated KSN Statement is displayed automatically. If you decline the updated KSN Statement, you still can view and accept it later.

► *To view and then accept or decline an updated KSN Statement:*

1. Click the **Several news and updates of different categories available** link in the upper-right corner of the main application window.

The **Notifications** window opens.

2. Click the **View the updated KSN Statement** link.

The **Kaspersky Security Network Statement update** window opens.

3. Carefully read the KSN Statement, and then make your decision by clicking one of the following buttons:
 - **I accept the updated KSN Statement**
 - **Use KSN under the old Statement**

Depending on your choice, KSN keeps working in accordance with the terms of the current or updated KSN Statement. You can view the text of the accepted KSN Statement (see section "Viewing the accepted KSN Statement" on page [1171](#)) in the properties of Administration Server at any time.

Checking whether the distribution point works as KSN Proxy

On a managed device assigned to work as a distribution point, you can enable KSN Proxy. A managed device works as KSN Proxy when the ksnproxy service is running on the device. You can check, turn on, or turn off this service on the device locally.

► *To check whether the distribution point works as KSN Proxy:*

1. On the distribution point device, in Windows, open **Services (All Programs → Administrative Tools → Services)**.
2. In the list of services, check whether the ksnproxy service is running.

If the ksnproxy service is running, then Network Agent on the device participates in Kaspersky Security Network and works as KSN Proxy for the managed devices included in the scope of the distribution point.

If you want, you may turn off the ksnproxy service. In this case, Network Agent on the distribution point stops participating in Kaspersky Security Network. This requires local administrator rights.

Scenario: Upgrading Kaspersky Security Center and managed security applications

This section describes the main brief scenario for Kaspersky Security Center and managed security applications upgrade.

The Kaspersky Security Center and managed security applications upgrade proceeds in stages:

a. Planning the resources

Assess how much disk space your database occupies. Make sure that you have enough disk space to store the backup copy (see section "Backup and restoration of Administration Server settings" on page [615](#)) of the Administration Server settings and the database.

b. Getting the installer file for Kaspersky Security Center

Get the executable file for the current version of Kaspersky Security Center and save it on the device that will work as the Administration Server. Read the Release Notes of the version of Kaspersky Security Center that you want to use.

c. Creating a backup copy of the previous version

Use the data backup and recovery utility (see section "Data backup and recovery utility (klbackup)" on page [618](#)) to create a backup copy of the Administration Server data.

d. Running the installer


Run the executable file for the latest version (see section "Installing Kaspersky Security Center (Standard installation)" on page [966](#)) of Kaspersky Security Center. When running the file, specify that you have a backup copy and specify its location. Your data will be restored from the backup.

e. Upgrading the managed applications

You can upgrade the application if there is a newer version available. Read the list of supported Kaspersky applications and make sure that your version of Kaspersky Security Center is compatible with this application. Then perform the upgrade of the application as described in its release notes.

Results

Upon completion of the upgrade scenario, make sure that new version of Administration Server is successfully installed in Microsoft Management Console. Click **Help** → **About Kaspersky Security Center**. The version is displayed.

To make sure that you are using the new version of Administration Server in Kaspersky Security Center 13 Web Console, at the top of the screen click the **Settings** icon () next to the name of the Administration Server. In the Administration Server properties window that opens, on the **General** tab, select the **General** section. The version is displayed.

If you upgraded a managed security application, make sure that it is correctly installed on the managed device(s). For more information, please refer to the documentation of this application.

Updating Kaspersky databases and applications

This section describes steps you must take to regularly update the following:

- Kaspersky databases and software modules
- Installed Kaspersky applications, including Kaspersky Security Center components and security applications

In this chapter

Scenario: Regular updating Kaspersky databases and applications	1174
About updating Kaspersky databases, software modules, and applications	1178
Creating the task for downloading updates to the repository of the Administration Server	1184
Creating the task for downloading updates to the repositories of distribution points	1189
Enabling and disabling automatic updating and patching for Kaspersky Security Center components	1194
Automatic installation of updates for Kaspersky Endpoint Security for Windows	1195
Approving and declining software updates.....	1197
Updating Administration Server.....	1198
Verifying downloaded updates	1198
Enabling and disabling the offline model of update download	1200
Updating Kaspersky databases and software modules on offline devices	1200
Adjustment of distribution points and connection gateways.....	1201

Scenario: Regular updating Kaspersky databases and applications

This section provides a scenario for regular updating of Kaspersky databases, software modules, and applications. After you complete the Configuring network protection scenario (see section "Scenario: Configuring network protection" on page [364](#)), you must maintain the reliability of the protection system to make sure that the Administration Servers and managed devices are kept protected against various threats, including viruses, network attacks, and phishing attacks.

Network protection is kept up-to-date by regular updates of the following:

- Kaspersky databases and software modules
- Installed Kaspersky applications, including Kaspersky Security Center components and security applications

When you complete this scenario, you can be sure of the following:

- Your network is protected by the most recent Kaspersky software, including Kaspersky Security Center components and security applications.

- The anti-virus databases and other Kaspersky databases critical for the network safety are always up-to-date.

Prerequisites

The managed devices must have a connection to the Administration Server. If they do not have a connection, consider updating Kaspersky databases, software modules, and applications manually (see section "Updating Kaspersky databases and software modules on offline devices" on page [1200](#)) or directly from the Kaspersky update servers.

Administration Server must have a connection to the Internet.

Before you start, make sure that you have done the following:

1. Deployed the Kaspersky security applications to the managed devices according to the scenario of deploying Kaspersky applications through Kaspersky Security Center 13 Web Console (see section "Scenario: Kaspersky applications deployment through Kaspersky Security Center 13 Web Console" on page [1023](#)).
2. Created and configured all required policies, policy profiles, and tasks according to the scenario of configuring network protection (see section "Scenario: Configuring network protection" on page [364](#)).
3. Assigned an appropriate amount of distribution points (see section "Calculating the number and configuration of distribution points" on page [134](#)) in accordance with the number of managed devices and the network topology.

Updating Kaspersky databases and applications proceeds in stages:

a. Choosing an update scheme

There are several schemes (see section "About updating Kaspersky databases, software modules, and applications" on page [406](#)) that you can use to install updates to Kaspersky Security Center components and security applications. Choose the scheme or several schemes that meet the requirements of your network best.

b. Creating the task for downloading updates to the repository of the Administration Server

This task is created automatically by Kaspersky Security Center Quick Start Wizard. If you did not run the Wizard, create the task now.

This task is required to download updates from Kaspersky update servers to the repository of the Administration Server, as well as to update Kaspersky databases and software modules for Kaspersky Security Center. After the updates are downloaded, they can be propagated to the managed devices.

If your network has assigned distribution points, the updates are automatically downloaded from the Administration Server repository to the repositories of the distribution points. In this case the managed devices included in the scope of a distribution point download the updates from the repository of the distribution point instead of the Administration Server repository.

How-to instructions:

- Administration Console: Creating the task for downloading updates to the repository of the Administration Server (on page [413](#))

or

- Kaspersky Security Center 13 Web Console: Creating the task for downloading updates to the repository of the Administration Server (on page [1184](#))

c. Creating the task for downloading updates to the repositories of distribution points (optional)

By default, the updates are downloaded to the distribution points from the Administration server. You can configure Kaspersky Security Center to download the updates to the distribution points directly from

Kaspersky update servers. Download to the repositories of distribution points is preferable if the traffic between the Administration Server and the distribution points is more expensive than the traffic between the distribution points and Kaspersky update servers, or if your Administration Server does not have Internet access.

When your network has assigned distribution points and the *Download updates to the repositories of distribution points* task is created, the distribution points download updates from Kaspersky update servers, and not from the Administration Server repository.

How-to instructions:

- Administration Console: Creating the task for downloading updates to the repositories of distribution points (see section "Creating the Downloading updates to the repositories of distribution points task" on page [417](#))

or

- Kaspersky Security Center 13 Web Console: Creating the task for downloading updates to the repositories of distribution points (on page [1189](#))

d. Configuring distribution points

When your network has assigned distribution points (see section "Assigning a device a distribution point manually" on page [427](#)), make sure that the **Deploy updates** option is enabled in the properties of all required distribution points. When this option is disabled for a distribution point, the devices included in the scope of the distribution point download updates from the repository of the Administration Server.

If you want the managed devices to receive updates only from the distribution points, enable the **Distribute files through distribution points only** option in the Network Agent policy (see section "Network Agent policy settings" on page [665](#)).

e. Optimizing the update process by using the offline model of update download or diff files (optional)

You can optimize the update process by using the offline model of update download (on page [442](#)) (enabled by default) or by using diff files (see section "Using diff files for updating Kaspersky databases and software modules" on page [412](#)). For each network segment, you have to choose which of these two features to enable, because they cannot work simultaneously.

When the offline model of update download is enabled, Network Agent downloads the required updates to the managed device once the updates are downloaded to the Administration Server repository, before the security application requests the updates. This enhances the reliability of the update process. To use this feature, enable the **Download updates and anti-virus databases from the Administration Server in advance** option in the Network Agent policy (see section "Network Agent policy settings" on page [665](#)).

If you do not use the offline model of update download, you can optimize traffic between the Administration Server and the managed devices by using diff files. When this feature is enabled, the Administration Server or a distribution point downloads diff files instead of entire files of Kaspersky databases or software modules. A diff file describes the differences between two versions of a file of a database or software module. Therefore, a diff file occupies less space than an entire file. This results in decrease in the traffic between the Administration Server or distribution points and the managed devices. To use this feature, enable the **Download diff files** option in the properties of the Download updates to the Administration Server repository task and/or the Download updates to the repositories of distribution points task.

How-to instructions: Using diff files for updating Kaspersky databases and software modules (on page [412](#))

- Administration Console: Enabling and disabling the offline model of update download (on page [443](#))

or

- Kaspersky Security Center 13 Web Console: Enabling and disabling the offline model of update download (on page [1200](#))

f. Verifying downloaded updates (optional)

Before installing the downloaded updates, you can verify the updates through the Update verification task. This task sequentially runs the device update tasks and virus scan tasks configured through settings for the specified collection of test devices. Upon obtaining the task results, the Administration Server starts or blocks the update propagation to the remaining devices.

The Update verification task can be performed as part of the *Download updates to the repository of the Administration Server* task. In the properties of the Download updates to the repository of the Administration Server task, enable the **Verify updates before distributing** option in the Administration Console or the **Run update verification** option in Kaspersky Security Center 13 Web Console.

How-to instructions:

- Administration Console: Verifying downloaded updates (on page [422](#))

or

- Kaspersky Security Center 13 Web Console: Verifying downloaded updates (on page [1198](#))

g. Approving and declining software updates

By default, the downloaded software updates have the *Undefined* status. You can change the status to *Approved* or *Declined*. The approved updates are always installed. If an update requires reviewing and accepting the terms of the End User License Agreement, then you first need to accept the terms. After that the update can be propagated to the managed devices. The undefined updates can only be installed on Network Agent and other Kaspersky Security Center components (see section "Automatic updating and patching for Kaspersky Security Center components" on page [457](#)) in accordance with the Network Agent policy settings. The updates for which you set *Declined* status will not be installed on devices. If a declined update for a security application was previously installed, Kaspersky Security Center will try to uninstall the update from all devices. Updates for Kaspersky Security Center components cannot be uninstalled.

How-to instructions:

- Administration Console: Approving and declining software updates (on page [435](#))

or

- Kaspersky Security Center 13 Web Console: Approving and declining software updates (on page [1197](#))

h. Configuring automatic installation of updates and patches for Kaspersky Security Center components

Starting from version 10 Service Pack 2, the downloaded updates and patches for Network Agent and other Kaspersky Security Center components (see section "Automatic updating and patching for Kaspersky Security Center components" on page [457](#)) are installed automatically. If you have left the **Automatically install applicable updates and patches for components that have the Undefined status** option enabled in the Network Agent properties, then all updates will be installed automatically after they are downloaded to the repository (or several repositories). If this option is disabled, Kaspersky patches that have been downloaded and tagged with the *Undefined* status will be installed only after you change their status to *Approved*.

For Network Agent versions earlier than 10 Service Pack 2, make sure that the **Update Network Agent modules** option is enabled in the properties of the Download updates to the repository of the Administration Server task or the Download updates to the repositories of distribution points task.

How-to instructions:

- Administration Console: Enabling and disabling automatic updating and patching for Kaspersky Security Center components (on page [458](#))

or

- Kaspersky Security Center 13 Web Console: Enabling and disabling automatic updating and patching for Kaspersky Security Center components (on page [1194](#))

i. Installation of updates for the Administration Server

Software updates for the Administration Server do not depend on the update statuses. They are not installed automatically and must be preliminarily approved by the administrator on the **Monitoring** tab in the Administration Console (**Administration Server <server name>** → **Monitoring**) or on the **NOTIFICATIONS** section in Kaspersky Security Center 13 Web Console (**MONITORING & REPORTING** → **NOTIFICATIONS**). After that, the administrator must explicitly run installation of the updates.

j. Configuring automatic installation of updates for the security applications

Create the Update tasks for the managed applications to provide timely updates to the applications, software modules and Kaspersky databases, including anti-virus databases. To ensure timely updates, we recommend that you select the **When new updates are downloaded to the repository** option when configuring the task schedule (see section "General task settings" on page [1081](#)).

By default, updates for Kaspersky Endpoint Security for Windows and Kaspersky Endpoint Security for Linux are installed only after you change the update status to *Approved*. You can change the update settings in the Update task.

If an update requires reviewing and accepting the terms of the End User License Agreement, then you first need to accept the terms. After that the update can be propagated to the managed devices.

How-to instructions:

- Administration Console: Automatic installation of Kaspersky Endpoint Security updates on devices (on page [441](#))

or

- Kaspersky Security Center 13 Web Console: Automatic installation of Kaspersky Endpoint Security updates on devices (see section "Automatic installation of updates for Kaspersky Endpoint Security for Windows" on page [1195](#))

Results

Upon completion of the scenario, Kaspersky Security Center is configured to update Kaspersky databases and installed Kaspersky applications after the updates are downloaded to the repository of the Administration Server or to the repositories of distribution points. You can then proceed to monitoring the network status.

About updating Kaspersky databases, software modules, and applications

To be sure that the protection of your Administration Servers and managed devices is up-to-date, you must provide timely updates of the following:

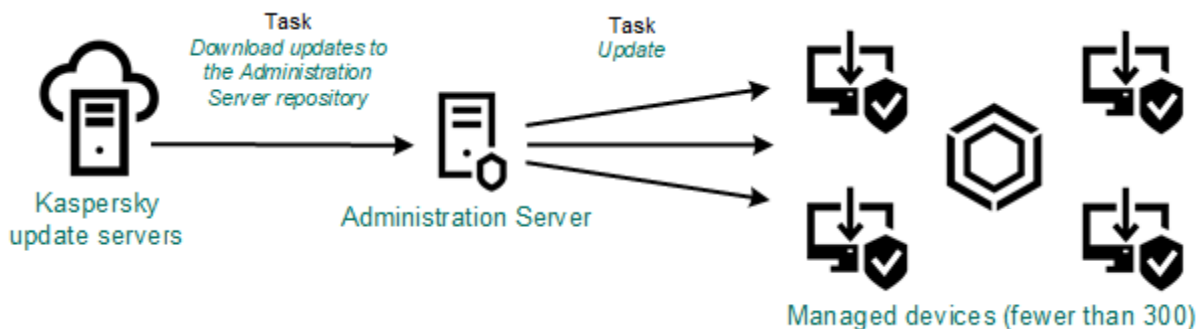
- Kaspersky databases and software modules
- Installed Kaspersky applications, including Kaspersky Security Center components and security applications

Depending on the configuration of your network, you can use the following schemes of downloading and distributing the required updates to the managed devices:

- Using the *Download updates to the Administration Server repository* task
- Using two tasks:
 - The *Download updates to the Administration Server repository* task
 - The *Download updates to the repositories of distribution points* task
- Manually through a local folder, a shared folder, or an FTP server
- Directly from Kaspersky update servers to Kaspersky Endpoint Security for Windows on the managed devices

Using the *Download updates to the Administration Server repository* task

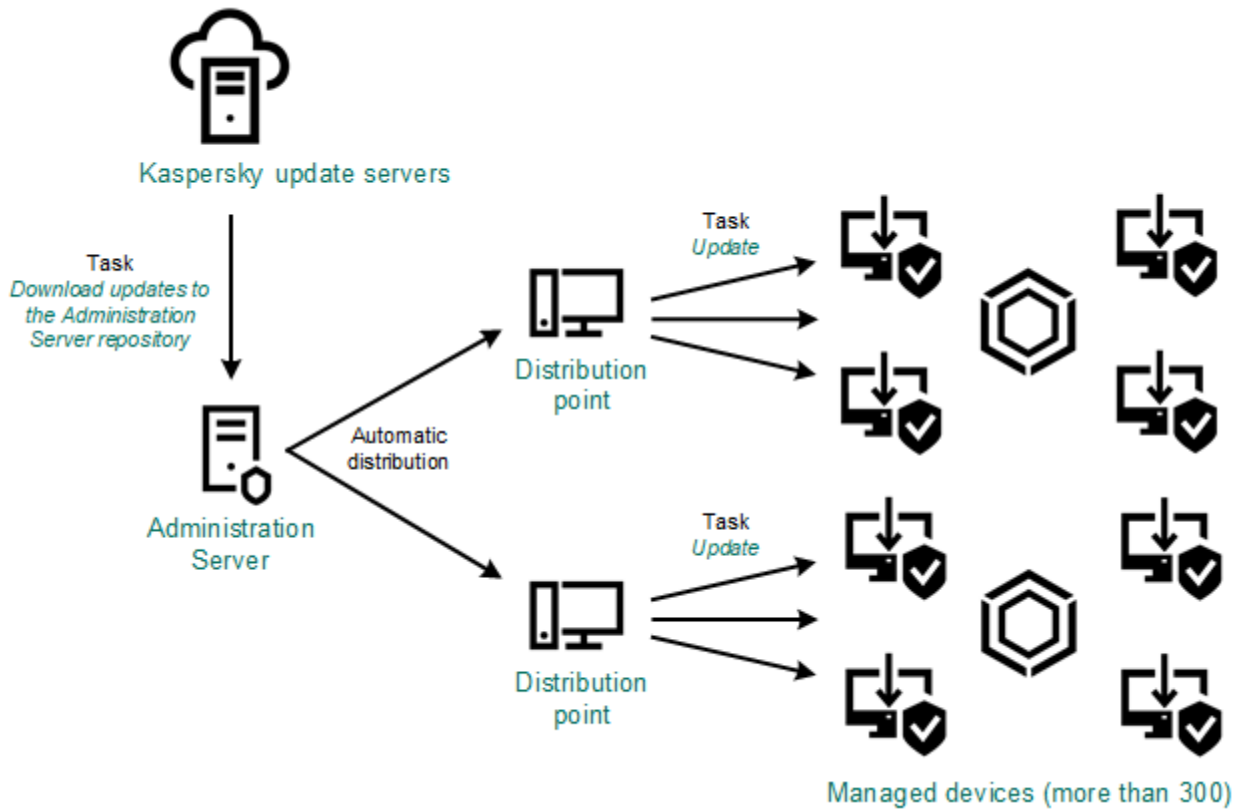
In this scheme, Kaspersky Security Center downloads updates through the *Download updates to the Administration Server repository* task. In small networks that contain less than 300 managed devices in a single network segment or less than 10 managed devices in each network segment, the updates are distributed to the managed devices directly from the Administration Server repository (see figure below).



By default, the Administration Server communicates with Kaspersky update servers and downloads updates by using the HTTPS protocol. You can configure the Administration Server to use the HTTP protocol instead of HTTPS.

If your network contains more than 300 managed devices in a single network segment or if your network consists of several network segments with more than 9 managed devices in each network segment, we recommend that you use distribution points (see section "About distribution points" on page [133](#)) to propagate the updates to the managed devices (see figure below). Distribution points reduce the load on the Administration Server and optimize traffic between the Administration Server and the managed devices. You can calculate (see section "Calculating the number and configuration of distribution points" on page [134](#)) the number and configuration of distribution points required for your network.

In this scheme, the updates are automatically downloaded from the Administration Server repository to the repositories of the distribution points. The managed devices included in the scope of a distribution point download the updates from the repository of the distribution point instead of the Administration Server repository.



When the *Download updates to the Administration Server repository* task is complete, the following updates are downloaded to the Administration Server repository:

- Kaspersky databases and software modules for Kaspersky Security Center
These updates are installed automatically.
- Kaspersky databases and software modules for the security applications on the managed devices
These updates are installed through the Update task for Kaspersky Endpoint Security for Windows (see section "Automatic installation of updates for Kaspersky Endpoint Security for Windows" on page [1195](#)).
- Updates for the Administration Server
These updates are not installed automatically. The administrator must explicitly approve and run installation of the updates.

Local administrator rights are required for installing patches on the Administration Server.

- Updates for the components of Kaspersky Security Center
By default, these updates are installed automatically. You can change the settings in the Network Agent policy (see section "Enabling and disabling automatic updating and patching for Kaspersky Security Center components" on page [1194](#)).
- Updates for the security applications

By default, Kaspersky Endpoint Security for Windows installs only those updates that you approve (see section "Approving and declining software updates" on page [1197](#)). The updates are installed through the Update task and can be configured in the properties of this task.

The Download updates to the repository of the Administration Server task is not available on virtual Administration Servers. The repository of the virtual Administration Server displays updates downloaded to the primary Administration Server.

You can configure the updates to be verified for operability and errors on a set of test devices. If the verification is successful, the updates are distributed to other managed devices.

Each Kaspersky application requests required updates from Administration Server. Administration Server aggregates these requests and downloads only those updates that are requested by any application. This ensures that the same updates are not downloaded multiple times and that unnecessary updates are not downloaded at all. When running the *Download updates to the Administration Server repository* task, Administration Server sends the following information to Kaspersky update servers automatically in order to ensure the downloading of relevant versions of Kaspersky databases and software modules:

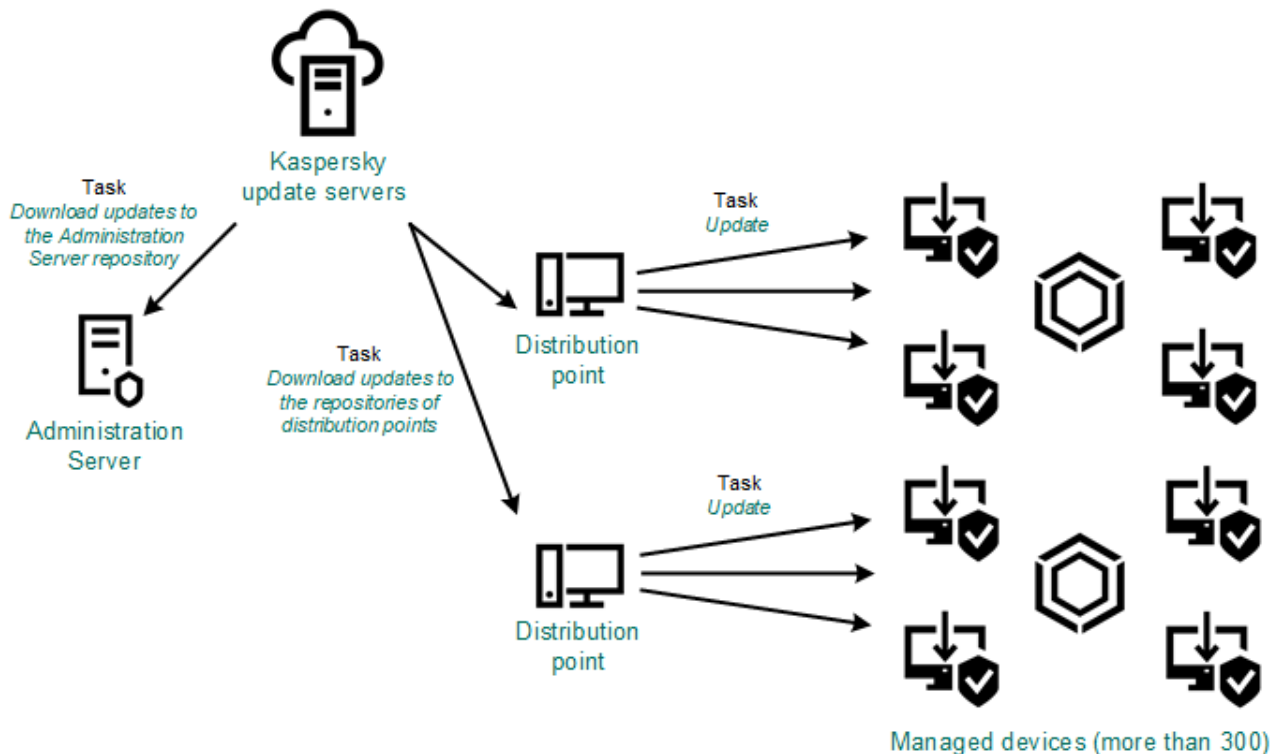
- Application ID and version
- Application setup ID
- Active key ID
- *Download updates to the repository of the Administration Server* task run ID

None of the transmitted information contains personal or other confidential data. AO Kaspersky Lab protects information in accordance with requirements established by law.

Using two tasks: the Download updates to the Administration Server repository task and the Download updates to the repositories of distribution points task

You can download updates to the repositories of distribution points directly from the Kaspersky update servers instead of the Administration Server repository, and then distribute the updates to the managed devices (see figure below). Download to the repositories of distribution points is preferable if the traffic between the Administration

Server and the distribution points is more expensive than the traffic between the distribution points and Kaspersky update servers, or if your Administration Server does not have Internet access.



By default, the Administration Server and distribution points communicate with Kaspersky update servers and download updates by using the HTTPS protocol. You can configure the Administration Server and/or distribution points to use the HTTP protocol instead of HTTPS.

To implement this scheme, create the *Download updates to the repositories of distribution points* task in addition to the *Download updates to the Administration Server repository* task. After that the distribution points will download updates from Kaspersky update servers, and not from the Administration Server repository.

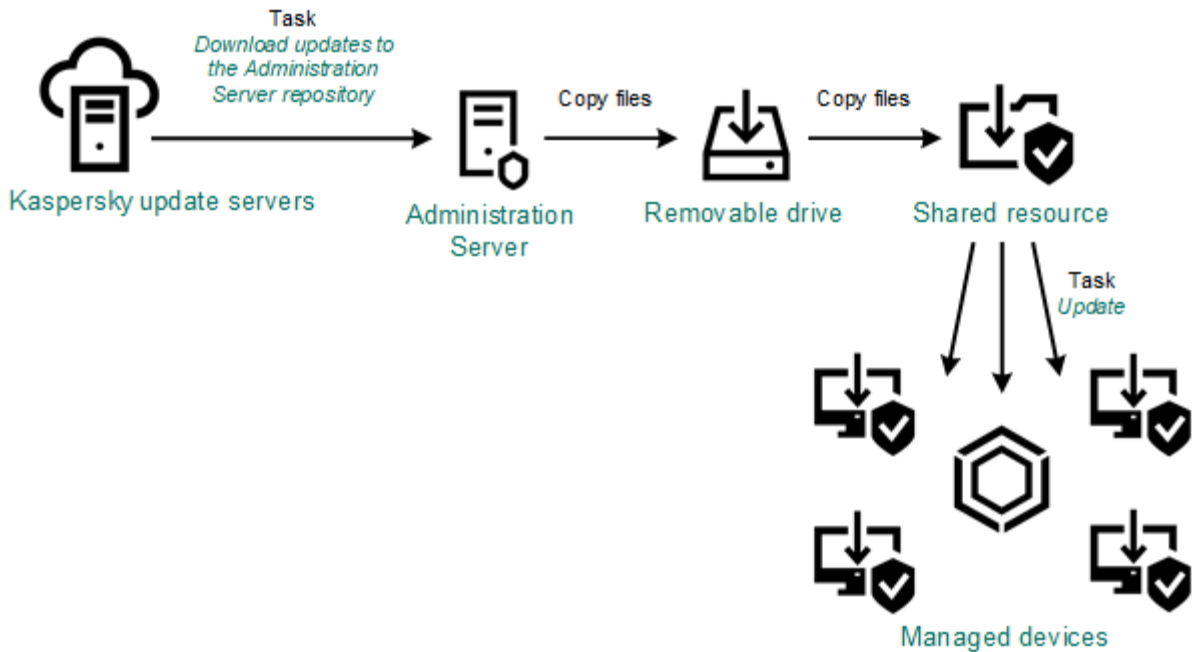
The *Download updates to the repositories of distribution points* task works only on distribution point devices running Windows. Distribution point devices running Linux or macOS cannot download updates from Kaspersky update servers.

If one or more devices running Linux or macOS are within the scope of the *Download updates to the repositories of distribution points* task, the task completes with the *Failed* status, even if it has successfully completed on all Windows devices.

The *Download updates to the Administration Server repository* task is also required for this scheme, because this task is used to download Kaspersky databases and software modules for Kaspersky Security Center.

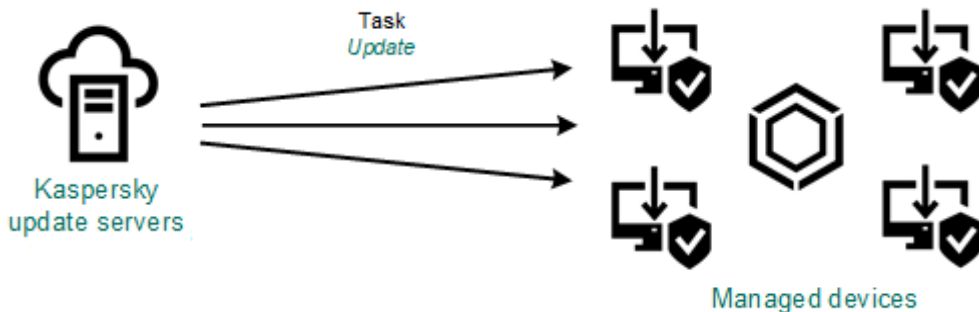
Manually through a local folder, a shared folder, or an FTP server

If the client devices do not have a connection to the Administration Server, you can use a local folder or a shared resource as a source for updating Kaspersky databases, software modules, and applications (see section "Updating Kaspersky databases and software modules on offline devices" on page [1200](#)). In this scheme, you need to copy required updates from the Administration Server repository to a removable drive, then copy the updates to the local folder or the shared resource specified as an update source in the settings of Kaspersky Endpoint Security for Windows (see figure below).



Directly from Kaspersky update servers to Kaspersky Endpoint Security for Windows on the managed devices

On the managed devices, you can configure Kaspersky Endpoint Security for Windows to receive updates directly from Kaspersky update servers (see figure below).



In this scheme, the security application does not use the repositories provided by Kaspersky Security Center. To receive updates directly from Kaspersky update servers, specify Kaspersky update servers as an update source in the interface of the security application. For a full description of these settings, please refer to the Kaspersky Endpoint Security for Windows documentation.

See also:

Scenario: Regular updating Kaspersky databases and applications[1174](#)

Creating the task for downloading updates to the repository of the Administration Server

The *Download updates to the Administration Server repository* task of the Administration Server is created automatically by the Kaspersky Security Center Quick Start Wizard. You can create only one *Download updates to the Administration Server repository* task. Therefore, you can create a *Download updates to the Administration Server repository* task only if this task was removed from the Administration Server tasks list.

This task is required to download updates from Kaspersky update servers to the repository of the Administration Server. The list of updates includes:

- Updates to databases and software modules for Administration Server
- Updates to databases and software modules for Kaspersky security applications
- Updates to Kaspersky Security Center components
- Updates to Kaspersky security applications

After the updates are downloaded, they can be propagated to the managed devices.

► To create a *Download updates to the Administration Server repository* task:

1. Go to **DEVICES** → **TASKS**.
2. Click **Add**.
The New Task Wizard starts. Proceed through the Wizard by using the **Next** button.
3. For the Kaspersky Security Center application, select the **Download updates to the Administration Server repository** task type.
4. Specify the name for the task that you are creating. A task name cannot be more than 100 characters long and cannot include any special characters ("*<>?:|)").
5. If on the **Finish task creation** page you enable the **Open task details when creation is complete** option, you can modify the default task settings. If you do not enable this option, the task is created with the default settings. You can modify the default settings later, at any time.
6. Click the **Create** button.
The task is created and displayed in the list of tasks.
7. Click the name of the created task to open the task properties window.
8. In the task properties window, on the **Application settings** tab, specify the following settings:
 - **Sources of updates**

The following resources can be used as a source of updates for the Administration Server:

- Kaspersky update servers.
HTTP(S) servers at Kaspersky from which Kaspersky applications download database and application module updates. By default, the Administration Server communicates with Kaspersky update servers and

downloads updates by using the HTTPS protocol. You can configure the Administration Server to use the HTTP protocol instead of HTTPS.

Selected by default.

- **Primary Administration Server.** (This option might not work in Kaspersky Security Center 13 Web Console.)
This resource applies to tasks created for a secondary or virtual Administration Server.
- **Local or network folder.**

A local or network folder that contains the latest updates. A network folder can be an FTP or HTTP server, or an SMB share. When selecting a local folder, you must specify a folder on the device that has Administration Server installed.

An FTP or HTTP server or a network folder used by an update source must contain a folders structure (with updates) that matches the structure created when using Kaspersky update servers.

- **Content of updates:**
 - **Download diff files**

This option enables the downloading diff files feature (see section "Using diff files for updating Kaspersky databases and software modules" on page [412](#)).

By default, this option is disabled.

- **Other settings:**
 - **Force update of secondary Administration Servers**

If this option is enabled, the Administration Server starts the update tasks on the secondary Administration Servers as soon as new updates are downloaded. Otherwise, the update tasks on the secondary Administration Servers start according to their schedules.

By default, this option is disabled.

- **Copy downloaded updates to additional folders**

After the Administration Server receives updates, it copies them to the specified folders. Use this option if you want to manually manage the distribution of updates on your network.

For example, you may want to use this option in the following situation: the network of your organization consists of several independent subnets, and devices from each of the subnets do not have access to other subnets. However devices in all of the subnets have access to a common network share. In this case, you set Administration Server in one of the subnets to download updates from Kaspersky update servers, enable this option, and then specify this network share. In downloaded updates to the repository tasks for other Administration Servers, specify the same network share as the update source.

By default, this option is disabled.

- **Do not force updating of devices and secondary Administration Servers unless copying is complete**

The tasks of downloading updates to client devices and secondary Administration Servers start only after those updates are copied from the main update folder to additional update folders.

This option must be enabled if client devices and secondary Administration Servers download updates from additional network folders.

By default, this option is disabled.

- **Update Network Agent modules (for Network Agent versions earlier than 10 Service Pack 2)**

If this option is enabled, updates for software modules of Network Agent are installed automatically after the Administration Server completes the download updates to the repository task. Otherwise, updates received for Network Agent modules can be installed manually.

By default, this option is enabled.

- **Run update verification:**
 - **Run update verification**

Administration Server downloads updates from the source, saves them to a temporary repository, and runs the task defined in the **Update verification task** field. If the task completes successfully, the updates are copied from the temporary repository to a shared folder on the Administration Server and then distributed to all devices for which the Administration Server acts as the source of updates (tasks with the **When new updates are downloaded to the repository** schedule type are started). The task of downloading updates to the repository is finished only after completion of the update verification task.

By default, this option is disabled.

1. In the task properties window, on the **Schedule** tab, create a schedule for task start. If necessary, specify the following settings:

- **Scheduled start:**

Select the schedule according to which the task runs, and configure the selected schedule.

- **Manually** (selected by default)

The task does not run automatically. You can only start it manually.

- **Every N minutes**

The task runs regularly, with the specified interval in minutes, starting from the specified time on the day that the task is created.

By default, the task runs every 30 minutes, starting from the current system time.

- **Every N hours**

The task runs regularly, with the specified interval in hours, starting from the specified date and time.

By default, the task runs every six hours, starting from the current system date and time.

- **Every N days**

The task runs regularly, with the specified interval in days. Additionally, you can specify a date and time of the first task run. These additional options become available, if they are supported by the application for which you create the task.

By default, the task runs every day, starting from the current system date and time.

- **Every N weeks**

The task runs regularly, with the specified interval in weeks, on the specified day of week and at the specified time.

By default, the task runs every Monday at the current system time.

- **Daily (daylight saving time is not supported)**

The task runs regularly, with the specified interval in days. This schedule does not support observance of daylight saving time (DST). It means that when clocks jump one hour forward or backward at the beginning or ending of DST, the actual task start time does not change.

We do not recommend that you use this schedule. It is needed for backward compatibility of Kaspersky Security Center.

By default, the task starts every day at the current system time.

- **Weekly**

The task runs every week on the specified day and at the specified time.

- **By days of week**

The task runs regularly, on the specified days of week, at the specified time.

By default, the task runs every Friday at 6:00:00 P.M.

- **Monthly**

The task runs regularly, on the specified day of the month, at the specified time.

In months that lack the specified day, the task runs on the last day.

By default, the task runs on the first day of each month, at the current system time.

- **Every month on specified days of selected weeks**

The task runs regularly, on the specified days of each month, at the specified time.

By default, no days of month are selected; the default start time is 6:00:00 P.M.

- **On virus outbreak**

The task runs after a *Virus outbreak* event occurs. Select application types that will monitor virus outbreaks. The following application types are available:

- Anti-virus for workstations and file servers
- Anti-virus for perimeter defense
- Anti-virus for mail systems

By default, all application types are selected.

You may want to run different tasks depending on the anti-virus application type that reports a virus outbreak. In this case, remove the selection of the application types that you do not need.

- **On completing another task**

The current task starts after another task completes. You can select how the previous task must complete (successfully or with error) to trigger the start of the current task. For example, you may want to run the Manage devices task with the **Turn on the device** option and, after it completes, run the Virus scan task.

- **Run missed tasks**

This option determines the behavior of a task if a client device is not visible on the network when the task is about to start.

If this option is enabled, the system attempts to start the task the next time the Kaspersky application is run on the client device. If the task schedule is **Manually, Once** or **Immediately**, the task is started immediately after the device becomes visible on the

network or immediately after the device is included in the task scope.

If this option is disabled, only scheduled tasks run on client devices; for **Manually, Once** and **Immediately**, tasks run only on those client devices that are visible on the network. For example, you may want to disable this option for a resource-consuming task that you want to run only outside of business hours.

By default, this option is enabled.

- **Use automatically randomized delay for task starts**

If this option is enabled, the task is started on client devices randomly within a specified time interval, that is, *distributed task start*. A distributed task start helps to avoid a large number of simultaneous requests by client devices to the Administration Server when a scheduled task is running.

The distributed start time is calculated automatically when a task is created, depending on the number of client devices to which the task is assigned. Later, the task is always started on the calculated start time. However when task settings are edited or the task is started manually, the calculated value of the task start time changes.

If this option is disabled, the task starts on client devices according to the schedule.

- **Use randomized delay for task starts within an interval of (min)**

If this option is enabled, the task is started on client devices randomly within the specified time interval. A distributed task start helps to avoid a large number of simultaneous requests by client devices to the Administration Server when a scheduled task is running.

If this option is disabled, the task starts on client devices according to the schedule.

By default, this option is disabled. The default time interval is one minute.

1. Click the **Save** button.

The task is created and configured.

When Administration Server performs the *Download updates to the Administration Server repository* task, updates to databases and software modules are downloaded from the updates source and stored in the shared folder of Administration Server. If you create this task for an administration group, it will only be applied to Network Agents included in the specified administration group.

Updates are distributed to client devices and secondary Administration Servers from the shared folder of Administration Server.

See also:

Scenario: Regular updating Kaspersky databases and applications	1174
Verifying downloaded updates	422
Download updates to the repository of the Administration Server task settings	934

Creating the task for downloading updates to the repositories of distribution points

The *Downloading updates to the repositories of distribution points* task works only on distribution point devices running Windows. Distribution point devices running Linux or macOS cannot download updates from Kaspersky update servers. If at least one device running Linux or macOS is within the task scope, the task will have the *Failed* status. Even if the task is completed successfully on all Windows devices, it will return an error on the remaining devices.

You can create the *Download updates to the repositories of distribution points* task for an administration group. This task will run for distribution points included in the specified administration group.

You can use this task, for example, if traffic between the Administration Server and the distribution point(s) is more expensive than traffic between the distribution point(s) and Kaspersky update servers, or if your Administration Server does not have Internet access.

This task is required to download updates from Kaspersky update servers to the repositories of distribution points. The list of updates includes:

- Updates to databases and software modules for Kaspersky security applications
- Updates to Kaspersky Security Center components
- Updates to Kaspersky security applications

After the updates are downloaded, they can be propagated to the managed devices.

► To create the *Download updates to the repositories of distribution points* task, for a selected administration group:

1. Go to **DEVICES** → **TASKS**.
2. Click the **Add** button.
The New Task Wizard starts. Proceed through the Wizard by using the **Next** button.
3. For the Kaspersky Security Center application, in the **Task type** field select **Download updates to the repositories of distribution points**.
4. Specify the name for the task that you are creating. A task name cannot be more than 100 characters long and cannot include any special characters ("* <> ? \ ; |").
5. Select an option button to specify the administration group, the device selection, or the devices to which the task applies.
6. At the **Finish task creation** step, if you enable the **Open task details when creation is complete** option, you can modify the default task settings. If you do not enable this option, the task is created with the default settings. You can modify the default settings later, at any time.
7. Click the **Create** button.
The task is created and displayed in the list of tasks.
8. Click the name of the created task to open the task properties window.
9. On the **Application settings** tab of the task properties window, specify the following settings:
 - **Sources of updates**

The following resources can be used as a source of updates for the distribution point:

- **Kaspersky update servers.**
HTTP(S) servers at Kaspersky from which Kaspersky applications download database and application module updates.
This option is selected by default.
- A local or network folder that contains the latest updates. A network folder can be an FTP or HTTP server, or an SMB share. When selecting a local folder, you must specify a folder on the device that has Administration Server installed.

An FTP or HTTP server or a network folder used by an update source must contain a folders structure (with updates) that matches the structure created when Kaspersky update servers are used.

- **Folder for storing updates**

The folder is used to download updates. Specify a local folder on the devices that are assigned to act as distribution point. You can use system variables.

- **Update Network Agent modules**

If this option is enabled, updates for software modules of Network Agent are installed automatically after the Administration Server completes the download updates to the repository task. Otherwise, updates received for Network Agent modules can be installed manually.

By default, this option is enabled.

- **Download diff files**

This option enables the downloading diff files feature (see section "Using diff files for updating Kaspersky databases and software modules" on page [412](#)).

By default, this option is disabled.

1. Create a schedule for task start. If necessary, specify the following settings:

- **Scheduled start:**

Select the schedule according to which the task runs, and configure the selected schedule.

- **Manually** (selected by default)

The task does not run automatically. You can only start it manually.

- **Every N minutes**

The task runs regularly, with the specified interval in minutes, starting from the specified time on the day that the task is created.

By default, the task runs every 30 minutes, starting from the current system time.

- **Every N hours**

The task runs regularly, with the specified interval in hours, starting from the specified date and time.

By default, the task runs every six hours, starting from the current system date and time.

- **Every N days**

The task runs regularly, with the specified interval in days. Additionally, you can specify a

date and time of the first task run. These additional options become available, if they are supported by the application for which you create the task.

By default, the task runs every day, starting from the current system date and time.

- **Every N weeks**

The task runs regularly, with the specified interval in weeks, on the specified day of week and at the specified time.

By default, the task runs every Monday at the current system time.

- **Daily (daylight saving time not supported)**

The task runs regularly, with the specified interval in days. This schedule does not support observance of daylight saving time (DST). It means that when clocks jump one hour forward or backward at the beginning or ending of DST, the actual task start time does not change.

We do not recommend that you use this schedule. It is needed for backward compatibility of Kaspersky Security Center.

By default, the task starts every day at the current system time.

- **Weekly**

The task runs every week on the specified day and at the specified time.

- **By days of week**

The task runs regularly, on the specified days of week, at the specified time.

By default, the task runs every Friday at 6:00:00 P.M.

- **Monthly**

The task runs regularly, on the specified day of the month, at the specified time.

In months that lack the specified day, the task runs on the last day.

By default, the task runs on the first day of each month, at the current system time.

- **Every month on specified days of selected weeks**

The task runs regularly, on the specified days of each month, at the specified time.

By default, no days of month are selected; the default start time is 6:00:00 P.M.

- **On virus outbreak**

The task runs after a *Virus outbreak* event occurs. Select application types that will monitor virus outbreaks. The following application types are available:

- Anti-virus for workstations and file servers
- Anti-virus for perimeter defense
- Anti-virus for mail systems

By default, all application types are selected.

You may want to run different tasks depending on the anti-virus application type that reports a virus outbreak. In this case, remove the selection of the application types that you do not need.

- **On completing another task**

The current task starts after another task completes. You can select how the previous task must complete (successfully or with error) to trigger the start of the current task. For

example, you may want to run the Manage devices task with the **Turn on the device** option and, after it completes, run the Virus scan task.

- **Run missed tasks**

This option determines the behavior of a task if a client device is not visible on the network when the task is about to start.

If this option is enabled, the system attempts to start the task the next time the Kaspersky application is run on the client device. If the task schedule is **Manually, Once** or **Immediately**, the task is started immediately after the device becomes visible on the network or immediately after the device is included in the task scope.

If this option is disabled, only scheduled tasks run on client devices; for **Manually, Once** and **Immediately**, tasks run only on those client devices that are visible on the network. For example, you may want to disable this option for a resource-consuming task that you want to run only outside of business hours.

By default, this option is enabled.

- **Use automatically randomized delay for task starts**

If this option is enabled, the task is started on client devices randomly within a specified time interval, that is, *distributed task start*. A distributed task start helps to avoid a large number of simultaneous requests by client devices to the Administration Server when a scheduled task is running.

The distributed start time is calculated automatically when a task is created, depending on the number of client devices to which the task is assigned. Later, the task is always started on the calculated start time. However when task settings are edited or the task is started manually, the calculated value of the task start time changes.

If this option is disabled, the task starts on client devices according to the schedule.

- **Use randomized delay for task starts within an interval of (min)**

If this option is enabled, the task is started on client devices randomly within the specified time interval. A distributed task start helps to avoid a large number of simultaneous requests by client devices to the Administration Server when a scheduled task is running.

If this option is disabled, the task starts on client devices according to the schedule.

By default, this option is disabled. The default time interval is one minute.

1. Click the **Save** button.

The task is created and configured.

In addition to the settings that you specify during task creation, you can change other properties of a created task.

When the *Download updates to the repositories of distribution points* task is performed, updates for databases and software modules are downloaded from the update source and stored in the shared folder. Downloaded updates will only be used by distribution points that are included in the specified administration group and that have no update download task explicitly set for them.

The previous versions of the application (Kaspersky Security Center 10 Service Pack 2 and earlier) allowed you to create the update download task for distribution points as a local task only. Starting from Kaspersky Security Center 10 Service Pack 3, this restriction has been lifted, which has resulted in decreased traffic rates.

S
e
e
a
l
s
o:

D
o
w
n
l
o
a
d
u
p
d
a
t
e
s
t
o
t
h
e
r
e
p
o
s
i
t
o
r
i
e
s
o
f
d
i
s
t
r
i
b
u
t
i
o
n

Enabling and disabling automatic updating and patching for Kaspersky Security Center components

Updates and patches for the Administration Server can be installed only manually, after obtaining explicit approval from the administrator.

Automatic installation of updates and patches for Kaspersky Security Center components is enabled by default during Network Agent installation on the device. You can disable it during Network Agent installation, or disable it later by using a policy.

► *To disable automatic updating and patching for Kaspersky Security Center components during local installation of Network Agent on a device:*

1. Start local installation of Network Agent on the device (see section "Local installation of Network Agent" on page [178](#)).
2. At the **Advanced settings** step, clear the **Automatically install applicable updates and patches for components that have Undefined status** check box.
3. Follow the instructions of the Wizard.

Network Agent with disabled automatic updating and patching for Kaspersky Security Center components will be installed on the device. You can enable automatic updating and patching later by using a policy.

► *To disable automatic updating and patching for Kaspersky Security Center components during Network Agent installation on the device through an installation package:*

1. Go to **OPERATIONS** → **REPOSITORIES** → **INSTALLATION PACKAGES**.
2. Click the **Kaspersky Security Center Network Agent <version number>** package.
3. In the properties window, open the **Settings** tab.
4. Turn off the **Automatically install applicable updates and patches for components that have the Undefined status** toggle button.

Network Agent with disabled automatic updating and patching for Kaspersky Security Center components will be installed from this package. You can enable automatic updating and patching later by using a policy.

If this check box was selected (or cleared) during Network Agent installation on the device, you can subsequently enable (or disable) automatic updating by using the Network Agent policy.

► *To enable or disable automatic updating and patching for Kaspersky Security Center components by using the Network Agent policy:*

1. Go to **DEVICES** → **POLICIES & PROFILES**.
2. Click the Network Agent policy.
3. In the policy properties window, open the **Application settings** tab.
4. In the **Manage patches and updates** section, turn on or off the **Automatically install applicable updates and patches for components that have the Undefined status** toggle button to enable or disable, respectively, automatic updating and patching.
5. Set the lock (🔒) for this toggle button.

The policy will be applied to the selected devices, and automatic updating and patching for Kaspersky Security Center components will be enabled (or disabled) on these devices.

See also:

Scenario: Regular updating Kaspersky databases and applications.....	1174
Automatic updating and patching for Kaspersky Security Center components.....	457

Automatic installation of updates for Kaspersky Endpoint Security for Windows

You can configure automatic updates of databases and software modules of Kaspersky Endpoint Security for Windows on client devices.

► *To configure download and automatic installation of updates of Kaspersky Endpoint Security for Windows on devices:*

1. Go to **DEVICES** → **TASKS**.
2. Click the **Add** button.

The New Task Wizard starts. Proceed through the Wizard by using the **Next** button.

3. For the Kaspersky Endpoint Security for Windows application, select **Update** as the task subtype.
4. Specify the name for the task that you are creating. A task name cannot be more than 100 characters long and cannot include any special characters ("* <> ? \ : |).
5. Choose the task scope.
6. Specify the administration group, the device selection, or the devices to which the task applies.
7. At the **Finish task creation** step, if you enable the **Open task details when creation is complete** option, you can modify the default task settings. If you do not enable this option, the task is created with the default settings. You can modify the default settings later, at any time.
8. Click the **Create** button.

The task is created and displayed in the list of tasks.
9. Click the name of the created task to open the task properties window.
10. On the **Application settings** tab of the task properties window, define the update task settings in local or mobile mode:
 - **Local mode:** Connection is established between the device and the Administration Server.
 - **Mobile mode:** No connection is established between Kaspersky Security Center and the device (for example, when the device is not connected to the Internet).
11. Enable the update sources that you want to use to update databases and application modules for Kaspersky Endpoint Security for Windows. If required, change positions of the sources in the list by using the **Move up** and **Move down** buttons. If several update sources are enabled, Kaspersky Endpoint Security for Windows tries to connect to them one after another, starting from the top of the list, and performs the update task by retrieving the update package from the first available source.
12. Enable the **Install approved application module updates** option to download and install software module updates together with the application databases.

If the option is enabled, Kaspersky Endpoint Security for Windows notifies the user about available software module updates and includes software module updates in the update package when running the update task. Kaspersky Endpoint Security for Windows installs only those updates for which you have set the *Approved* status; they will be installed locally through the application interface or through Kaspersky Security Center.

You can also enable the **Automatically install critical application module updates** option. If any updates are available for software modules, Kaspersky Endpoint Security for Windows automatically installs those that have *Critical* status; the remaining updates will be installed after you approve them.

If updating the software module requires reviewing and accepting the terms of the License Agreement and Privacy Policy, the application installs updates after the terms of the License Agreement and Privacy Policy have been accepted by the user.
13. Select the **Copy updates to folder** check box in order for the application to save downloaded updates to a folder, and then specify the folder path.
14. Schedule the task. To ensure timely updates, we recommend that you select the **When new updates are downloaded to the repository** option.
15. Click **Save**.

When the **Update** task is running, the application sends requests to Kaspersky update servers.

Some updates require installation of the latest versions of management plug-ins.

See also:

Scenario: Regular updating Kaspersky databases and applications [1174](#)

Approving and declining software updates

The settings of an update installation task may require approval of updates that are to be installed. You can approve updates that must be installed and decline updates that must not be installed.

For example, you may want to first check the installation of updates in a test environment and make sure that they do not interfere with the operation of devices, and only then allow the installation of these updates on client devices.

► *To approve or decline one or several updates:*

1. Go to **OPERATIONS** → **KASPERSKY APPLICATIONS**, and in the drop-down list select **SEAMLESS UPDATES**.

A list of available updates appears.

Updates of managed applications may require a specific minimum version of Kaspersky Security Center to be installed. If this version is later than your current version, these updates are displayed but cannot be approved. Also, no installation packages can be created from such updates until you upgrade Kaspersky Security Center. You are prompted to upgrade your Kaspersky Security Center instance to the required minimum version.

2. Select the updates that you want to approve or decline.
3. Click **Approve** to approve the selected updates or **Decline** to decline the selected updates.

The default value is *Undefined*.

The updates to which you assign *Approved* status are placed in a queue for installation.

The updates to which you assign *Declined* status are uninstalled (if possible) from all devices on which they were previously installed. Also, they will not be installed on other devices in future.

Some updates for Kaspersky applications cannot be uninstalled. If you set *Declined* status for them, Kaspersky Security Center will not uninstall these updates from the devices on which they were previously installed. However, these updates will never be installed on other devices in future. If you set *Declined* status for third-party software updates, these updates will not be installed on devices for which they were planned but have not yet been installed. Updates will remain on devices on which they were already installed. If you have to delete the updates, you can manually delete them locally.

See also:

Scenario: Regular updating Kaspersky databases and applications[1174](#)

Updating Administration Server

You can install Administration Server updates by using Update Administration Server Wizard.

► *To install an Administration Server update:*

1. Go to **OPERATIONS** → **KASPERSKY APPLICATIONS** → **SEAMLESS UPDATES**.
2. Run the Update Administration Server Wizard in one of the following ways:
 - Click the name of an Administration Server update in the list of updates, and in the window that opens, click the **Run Update Administration Server Wizard** link.
 - Click the **Run Update Administration Server Wizard** link in the notification field at the top of the window.
3. In the Update Administration Server Wizard window, select one of the following to specify when to install an update:
 - **Install now.** Select this option if you want to install the update now.
 - **Postpone installation.** Select this option if you want to install the update later. In this case, a notification about this update will be displayed.
 - **Ignore update.** Select this option if you do not want to install an update and do not want to receive notifications about this update.
4. Select the **Create backup copy of Administration Server before update installation** option if you want to create a backup of Administration Server before installing the update.
5. Click the **OK** button to finish the wizard.

In the backup process is interrupted, the update installation process is also interrupted.

Verifying downloaded updates

Before installing updates to the managed devices, you can first check the updates for operability and errors through the Update verification task. The Update verification task is performed automatically as part of the *Download updates to the Administration Server repository* task. The Administration Server downloads updates from the source, saves them in the temporary repository, and runs the update verification task. If the task completes successfully, the updates are copied from the temporary repository to the Administration Server shared folder (<Kaspersky Security Center> installation folder>\Share\Updates). They are distributed to all client devices for which the Administration Server is the source of updates.

If, as a result of the update verification task, updates located in the temporary repository are incorrect or if the update verification task completes with an error, such updates are not copied to the shared folder. The Administration Server retains the previous set of updates. Also, the tasks that have the **When new updates are**

downloaded to the repository schedule type are not started then. These operations are performed at the next start of the *Download updates to the Administration Server repository* task if scanning of the new updates completes successfully.

A set of updates is considered invalid if any of the following conditions is met on at least one test device:

- An update task error occurred.
- The real-time protection status of the security application changed after the updates were applied.
- An infected object was detected during running of the on-demand scan task.
- A runtime error of a Kaspersky application occurred.

If none of the listed conditions is true for any test device, the set of updates is considered valid, and the update verification task is considered to have completed successfully.

► *To make Kaspersky Security Center verify downloaded updates before distributing them to client devices:*

1. Go to **DEVICES** → **TASKS**.
2. Click the **Download updates to the Administration Server repository** task.
3. In the task properties window that opens, in the **Application settings** tab, click the **Configure** button next to **Run update verification**.
4. In the **Update verification** window that opens, enable the **Run update verification** option.
5. Select the update verification task in one of the following ways:
 - By clicking the **Edit** link to choose an existing update verification task.
 - By clicking the **New task** button to create an update verification task.

The New Task Wizard starts. Follow the instructions of the Wizard.

When creating the update verification task, select the administration group that contains devices on which the task will be run. Devices included in this group are called *test devices*.

It is recommended to use devices with the most reliable protection and the most popular application configuration across the network. This approach increases the quality of scans, and minimizes the risk of false positives and the probability of virus detection during scans. If viruses are detected on test devices, the update verification task is considered unsuccessful.

6. Click **OK** to close the properties window of the *Download updates to the Administration Server repository* task.

The automatic update verification is enabled.

See also:

Scenario: Regular updating Kaspersky databases and applications [1174](#)

Enabling and disabling the offline model of update download

We recommend that you avoid disabling the offline model of update download. Disabling it may cause failures in update delivery to devices. In certain cases, a Kaspersky Technical Support specialist may recommend that you disable the **Download updates and anti-virus databases from Administration Server in advance** option. Then, you will have to make sure that the task for receiving updates for Kaspersky applications has been set up.

► To enable or disable the offline model of update download for an administration group:

1. Go to **DEVICES** → **POLICIES & PROFILES**.
2. Click **Groups**.
3. In the administration group structure, select the administration group for which you need to enable the offline model of update download.
4. Click the Network Agent policy.

The properties window of the Network Agent policy opens.

By default, settings of child policies are inherited from parent policies and cannot be modified. If the policy that you want to modify is inherited, you first need to create a new policy for Network Agent in the required administration group. In the newly created policy, you can modify the settings that are not locked in the parent policy.

5. In the **Application settings** tab, select the **Manage patches and updates** section.
6. Enable or disable the **Download updates and anti-virus databases from the Administration Server in advance** option to enable or disable, respectively, the offline model of update download.

By default, the offline model of update download is enabled.

The offline model of update download will be enabled or disabled.

See also:

Scenario: Regular updating Kaspersky databases and applications	1174
Offline model of update download	442

Updating Kaspersky databases and software modules on offline devices

Updating Kaspersky databases and software modules on managed devices is an important task for maintaining protection of the devices against viruses and other threats. Administrators usually configure regular updates (see section "Scenario: Regular updating Kaspersky databases and applications" on page [1174](#)) through usage of the Administration Server repository or repositories of distribution points.

When you need to update databases and software modules on a device (or a group of devices) that is not connected to the Administration Server (primary or secondary), a distribution point or the Internet, you have to use

alternative sources of updates, such as an FTP server or a local folder. In this case you have to deliver the files of the required updates by using a mass storage device, such as a flash drive or an external hard drive.

You can copy the required updates from:

- The Administration Server.
To be sure the Administration Server repository contains the updates required for the security application installed on an offline device, at least one of the managed online devices must have the same security application installed. This application must be configured to receive the updates from the Administration Server repository through the Download updates to the Administration Server repository task.
- Any device that has the same security application installed and configured to receive the updates from the Administration Server repository, a distribution point repository, or directly from the Kaspersky update servers.

Below is an example of configuring updates of databases and software modules by copying them from the Administration Server repository.

► *To update Kaspersky databases and software modules on offline devices:*

1. Connect the removable drive to the device where the Administration Server is installed.
2. Copy the updates files to the removable drive.

By default, the updates are located at: \\<server name>\KLSHARE\Updates.

Alternatively, you can configure Kaspersky Security Center to regularly copy the updates to the folder that you select. For this purpose, use the **Copy downloaded updates to additional folders** option in the properties of the Download updates to the Administration Server repository task. If you specify a folder located on a flash drive or an external hard drive as a target folder for this option, this mass storage device will always contain the latest version of the updates.

3. On offline devices, configure the security application (for example, Kaspersky Endpoint Security for Windows) to receive updates from a local folder or a shared resource, such as an FTP server or a shared folder.
4. Copy the updates files from the removable drive to the local folder or the shared resource that you want to use as an update source.
5. On the offline device that requires update installation, start the update task of Kaspersky Endpoint Security for Windows.

After the update task is complete, the Kaspersky databases and software modules are up-to-date on the device.

See also:

Scenario: Regular updating Kaspersky databases and applications	1174
Creating the task for downloading updates to the repository of the Administration Server	1184

Adjustment of distribution points and connection gateways

A structure of administration groups in Kaspersky Security Center performs the following functions:

- Sets the scope of policies

There is an alternate way of applying relevant collections of settings on devices, by using *policy profiles*. In this case, the scope of policies is set with tags, device locations in Active Directory organizational units, membership in Active Directory security groups, etc (see section "Hierarchy of policies, using policy profiles" on page [385](#)).

- Sets the scope of group tasks

There is an approach to defining the scope of group tasks that is not based on a hierarchy of administration groups: use of tasks for device selections and tasks for specific devices.

- Sets access rights to devices, virtual Administration Servers, and secondary Administration Servers
- Assigns distribution points

When building the structure of administration groups, you must take into account the topology of the organization's network for the optimum assignment of distribution points. The optimum distribution of distribution points allows you to save traffic on the organization's network.

Depending on the organizational schema and network topology, the following standard configurations can be applied to the structure of administration groups:

- Single office
- Multiple small remote offices

Devices functioning as distribution points must be protected, including physical protection, against any unauthorized access.

In this section

Standard configuration of distribution points: Single office.....	1202
Standard configuration of distribution points: Multiple small remote offices.....	1203
Assigning distribution points automatically	1203
Assigning distribution points manually.....	1204
Modifying the list of distribution points for an administration group.....	1207

Standard configuration of distribution points: Single office

In a standard "single-office" configuration, all devices are on the organization's network so they can "see" each other. The organization's network may consist of a few separate parts (networks or network segments) linked by narrow channels.

The following methods of building the structure of administration groups are possible:

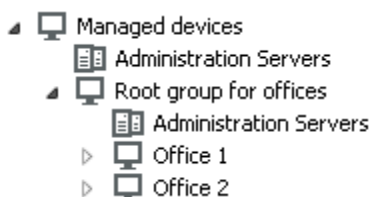
- Building the structure of administration groups taking into account the network topology. The structure of administration groups may not reflect the network topology with absolute precision. A match between the separate parts of the network and certain administration groups would be enough. You can use automatic assignment of distribution points or assign them manually.
- Building the structure of administration groups, without taking the network topology into account. In this case, you must disable automatic assignment of distribution points, and then assign one or several devices to act as distribution points for a root administration group in each of the separate parts of the network, for example, for the **Managed devices** group. All distribution points will be at the same level and will feature

the same scope spanning all devices on the organization's network. In this case, each Network Agent in version 10 Service Pack 1 or later will connect to the distribution point that has the shortest route. The route to a distribution point can be traced with the tracert utility.

Standard configuration of distribution points: Multiple small remote offices

This standard configuration provides for a number of small remote offices, which may communicate with the head office over the Internet. Each remote office is located behind the NAT, that is, connection from one remote office to another is not possible because offices are isolated from one another.

The configuration must be reflected in the structure of administration groups: a separate administration group must be created for each remote office (groups **Office 1** and **Office 2** in the figure below).



One or multiple distribution points must be assigned to each administration group that correspond to an office. Distribution points must be devices at the remote office that have a sufficient amount of free disk space. Devices deployed in the **Office 1** group, for example, will access distribution points assigned to the **Office 1** administration group.

If some users move between offices physically, with their laptops, you must select two or more devices (in addition to the existing distribution points) in each remote office and assign them to act as distribution points for a top-level administration group (**Root group for offices** in the figure above).

Example: A laptop is deployed in the **Office 1** administration group and then is moved physically to the office that corresponds to the **Office 2** administration group. After the laptop is moved, Network Agent attempts to access the distribution points assigned to the **Office 1** group, but those distribution points are unavailable. Then, Network Agent starts attempting to access the distribution points that have been assigned to the **Root group for offices**. Because remote offices are isolated from one another, attempts to access distribution points assigned to the **Root group for offices** administration group will only be successful when Network Agent attempts to access distribution points in the **Office 2** group. That is, the laptop will remain in the administration group that corresponds to the initial office, but the laptop will use the distribution point of the office where it is physically located at the moment.

Assigning distribution points automatically

We recommend that you assign distribution points automatically. In this case, Kaspersky Security Center will select on its own which devices must be assigned distribution points.

► *To assign distribution points automatically:*

1. In the main application window, click the **Settings** icon (🔧) next to the name of the required Administration Server.
The Administration Server properties window opens.
2. On the **General** tab, select the **Distribution points** section.
3. Select the **Automatically assign distribution points** option.

If automatic assignment of devices as distribution points is enabled, you cannot configure distribution points manually or edit the list of distribution points.

4. Click the **Save** button.

Administration Server assigns and configures distribution points automatically.


Assigning distribution points manually

Kaspersky Security Center allows you to manually assign devices to act as distribution points.

We recommend that you assign distribution points automatically. In this case, Kaspersky Security Center will select on its own which devices must be assigned distribution points. However, if you have to opt out of assigning distribution points automatically for any reason (for example, if you want to use exclusively assigned servers), you can assign distribution points manually after you calculate their number and configuration (see section "Calculating the number and configuration of distribution points" on page [134](#)).

Devices functioning as distribution points must be protected, including physical protection, against any unauthorized access.

► *To manually assign a device to act as distribution point:*

1. In the main application window, click the **Settings** icon () next to the name of the required Administration Server.

The Administration Server properties window opens.

2. On the **General** tab, select the **Distribution points** section.
3. Select the **Manually assign distribution points** option.
4. Click the **Assign** button.
5. Select the device that you want to make a distribution point.

When selecting a device, keep in mind the operation features of distribution points and the requirements set for the device that acts as distribution point.

6. Select the administration group that you want to include in the scope of the selected distribution point.
7. Click the **Add** button.

The distribution point that you have added will be displayed in the list of distribution points, in the **Distribution points** section.

8. Select the newly added distribution point in the list to open its properties window.
9. Configure the distribution point in the properties window:

- The **General** section contains the settings of interaction between the distribution point and client devices:
 - **SSL port number**

The number of the SSL port for encrypted connection between client devices and the distribution point using SSL.

By default, port 13000 is used.

- **Use multicast**

If this check box is selected, IP multicasting will be used for automatic distribution of installation packages to client devices within the group.

IP multicasting decreases the time required to install an application from an installation package to a group of client devices, but increases the installation time when you install an application to a single client device.

- **IP multicast address**

IP address that will be used for multicasting. You can define an IP address in the range of 224.0.0.0 – 239.255.255.255

By default, Kaspersky Security Center automatically assigns a unique IP multicast address within the given range.

- **IP multicast port number**

Number of the port for IP multicasting.

By default, the port number is 15001. If the device with Administration Server installed is specified as the distribution point, port 13001 is used for SSL connection by default.

- **Deploy updates**

If this check box is selected, updates are distributed to client devices through this distribution point.

By default, this check box is selected.

- **Deploy installation packages**

If this check box is selected, installation packages with this update are distributed to client devices through this distribution point.

By default, this check box is selected.

- In the **Scope** section, specify the scope to which the distribution point will distribute updates (administration groups and / or network location).

Only devices running a Windows operating system can determine their network location. Network location cannot be determined for devices running other operating systems.

- In the **KSN Proxy** section, you can configure the application to use the distribution point to forward KSN requests from the managed devices:

- **Enable KSN Proxy on distribution point side**

The KSN Proxy service is run on the device that is used as a distribution point. Use this feature to redistribute and optimize traffic on the network.

The distribution point sends the KSN statistics, which are listed in the Kaspersky Security Network statement, to Kaspersky. By default, the KSN statement is located in %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\ksneula.

By default, this option is disabled. Enabling this option takes effect only if the **Use Administration Server as proxy server** and **I agree to use Kaspersky Security Network** options are enabled (see section "Setting up access to Kaspersky Security Network" on page [786](#)) in the Administration Server properties window.

You can assign a node of an active-passive cluster to a distribution point and enable KSN Proxy on this node.

- **Forward KSN requests to Administration Server**

The distribution point forwards KSN requests from the managed devices to the Administration Server.

By default, this option is enabled.

- **Access KSN Cloud / Private KSN directly over the Internet**

The distribution point forwards KSN requests from managed devices to the KSN Cloud or Private KSN. The KSN requests generated on the distribution point itself are also sent directly to the KSN Cloud or Private KSN.

The distribution points that have Network Agent version 11 (or earlier) installed cannot access Private KSN directly. If you want to reconfigure the distribution points to send KSN requests to Private KSN, enable the **Forward KSN requests to Administration Server** option for each distribution point.

The distribution points that have Network Agent version 12 (or later) installed can access Private KSN directly.

- **Ignore KSC proxy server settings when connecting to Private KSN**

Enable this option, if you have the proxy server settings configured in the distribution point properties or in the Network Agent policy, but your network architecture requires that you use Private KSN directly. Otherwise, requests from the managed applications cannot reach Private KSN.

- **TCP port**

The number of the TCP port that the managed devices will use to connect to KSN Proxy server. The default port number is 13111.

- **UDP port.**

If you need the managed devices to connect to KSN Proxy server through a UDP port, enable the **Use UDP port** option and specify a **UDP port** number. By default, this option is enabled. The default UDP port to connect to the KSN Proxy server is 15111.

- Configure the polling of Windows domains, Active Directory, and IP ranges by the distribution point:

- **Windows domains**

You can enable device discovery for Windows domains and set the schedule for the discovery.

- **Active Directory**

You can enable network polling for Active Directory and set the schedule for the poll.

If you select the **Enable network polling** check box, you can select one of the following options:

- **Poll current Active Directory domain.**
- **Poll Active Directory domain forest.**
- **Poll selected Active Directory domains only.** If you select this option, add one or more Active Directory domains to the list.

- **IP ranges**

You can enable device discovery for IP ranges.

If you select the **Enable range polling** check box, you can add scan ranges and set the schedule for them.

You can add IP ranges to the list of scanned ranges (see section "Adding IP ranges to

the scanned ranges list of a distribution point" on page [594](#)).

- In the **Advanced** section, specify the folder that the distribution point must use to store distributed data:

- **Use default folder**

If you select this option, the application uses the Network Agent installation folder on the distribution point.

- **Use specified folder**

If you select this option, in the field below, you can specify the path to the folder. It can be a local folder on the distribution point, or it can be a folder on any device on the corporate network.

The user account used on the distribution point to run Network Agent must have read/write access to the specified folder.

1. Click the **OK** button.

The selected devices act as distribution points.

Modifying the list of distribution points for an administration group

This section describes features applicable only to Kaspersky Security Center 11.1 Web Console or a later version.

You can view the list of distribution points assigned to a specific administration group and modify the list by adding or removing distribution points.

► *To view and modify the list of distribution points assigned to an administration group:*

1. Go to **DEVICES** → **Groups**.
2. In the administration group structure, select the administration group for which you want to view the assigned distribution points.
3. Click the **DISTRIBUTION POINTS** tab.
4. Add new distribution points for the administration group by using the **Assign** button or remove the assigned distribution points by using the **Unassign** button.

Depending on your modifications, the new distribution points are added to the list or existing distribution points are removed from the list.

Managing third-party applications on client devices

This section describes the features of Kaspersky Security Center that are related to the management of third-party applications installed on client devices.

In this section

Installation of third-party software updates.....	1208
Fixing third-party software vulnerabilities	1236
Managing applications run on client devices	1257
Creating an installation package of a third-party application from the Kaspersky database.....	1273
Viewing and modifying the settings of an installation package of a third-party application from the Kaspersky database	1274
Settings of an installation package of a third-party application from the Kaspersky database	1274

Installation of third-party software updates

This section describes the features of Kaspersky Security Center that are related to the installation of updates for the third-party applications installed on client devices.

In this section

Scenario: Updating third-party software	1208
About third-party software updates.....	1211
Installing third-party software updates.....	1212
Creating the Find vulnerabilities and required updates task	1216
Find vulnerabilities and required updates task settings.....	1219
Creating the Install required updates and fix vulnerabilities task	1221
Adding rules for update installation	1225
Creating the Install Windows Update updates task.....	1229
Viewing information about available third-party software updates	1231
Exporting the list of available software updates to a file.....	1232
Approving and declining third-party software updates	1233
Creating the Perform Windows Update synchronization task	1234
Updating third-party applications automatically.....	1236

Scenario: Updating third-party software

This section provides a scenario for updating third-party software installed on the client devices. The third-party software includes applications from Microsoft and other software vendors. Updates for Microsoft applications are provided by the Windows Update service.

Prerequisites

Administration Server must have a connection to the Internet to install updates of third-part software other than Microsoft software.

By default, Internet connection is not required for Administration Server to install Microsoft software updates on the managed devices. For example, the managed devices can download the Microsoft software updates directly from Microsoft Update servers or from Windows Server with Microsoft Windows Server Update Services (WSUS) deployed in your organization's network. Administration Server must be connected to the Internet when you use Administration Server as WSUS server.

Stages

Updating third-party software proceeds in stages:

a. Searching for required updates

To find the third-party software updates required for the managed devices, run the *Find vulnerabilities and required updates* task. When this task is complete, Kaspersky Security Center receives the lists of detected vulnerabilities and required updates for the third-party software installed on the devices that you specified in the task properties.

The *Find vulnerabilities and required updates* task is created automatically by the Administration Server Quick Start Wizard. If you did not run the Wizard, create the task or run the Quick Start Wizard now.

How-to instructions:

- Administration Console: Scanning applications for vulnerabilities (on page [464](#)), Scheduling the Find vulnerabilities and required updates task (on page [372](#))

or

- Kaspersky Security Center 13 Web Console: Creating the Find vulnerabilities and required updates task (see section "Creating the Find vulnerabilities and required updates task" on page [1216](#)), Find vulnerabilities and required updates task settings (on page [1219](#))

b. Analyzing the list of found updates

View the **SOFTWARE UPDATES** list and decide which updates you want to install. To view detailed information about each update, click the update name in the list. For each update in the list, you can also view the statistics on the update installation on client devices.

How-to instructions:

- Administration Console: Viewing information about available updates (on page [434](#))

or

- Kaspersky Security Center 13 Web Console: Viewing information about available third-party software updates (on page [1231](#))

c. Configuring installation of updates

When Kaspersky Security Center received the list of the third-party software updates, you can install them on client devices by using the *Install required updates and fix vulnerabilities* task or the *Install Windows Update updates* task. Create one of these tasks. You can create these tasks on the **TASKS** tab or by using the **SOFTWARE UPDATES** list.

The *Install required updates and fix vulnerabilities* task is used to install updates for Microsoft applications, including the updates provided by the Windows Update service, and updates of other vendors' products. Note that this task can be created only if you have the license for the Vulnerability and Patch Management feature.

The *Install Windows Update updates* task does not require a license, but it can be used to install Windows Update updates only.

To install some software updates you must accept the End User License Agreement (EULA) for the installation software. If you decline the EULA, the software update will not be installed.

You can start an update installation task by schedule. When specifying the task schedule, make sure that the update installation task starts after the *Find vulnerabilities and required updates* task is complete.

How-to instructions:

- Administration Console: Fixing vulnerabilities in applications (on page [469](#)), Viewing information about available updates (on page [434](#))

or

- Kaspersky Security Center 13 Web Console: Creating the Install required updates and fix vulnerabilities task (on page [1221](#)), Creating the Install Windows Update updates task (on page [1229](#)), Viewing information about available third-party software updates (on page [1231](#))

d. Scheduling the tasks

To be sure that the update list is always up-to-date, schedule the *Find vulnerabilities and required updates* task to run the task automatically from time to time. The default frequency is once a week.

If you have created the *Install required updates and fix vulnerabilities* task, you can schedule it to run with the same frequency as the *Find vulnerabilities and required updates* task or less often. When scheduling the *Install Windows Update updates* task, note that for this task you must define the list of updates every time before starting this task.

When scheduling the tasks, make sure that an update installation task starts after the *Find vulnerabilities and required updates* task is complete.

e. Approving and declining software updates (optional)

If you have created the *Install required updates and fix vulnerabilities* task, you can specify rules for update installation in the task properties. If you have created the *Install Windows Update updates* task, skip this step.

For each rule, you can define the updates to install depending on the update status: *Undefined*, *Approved* or *Declined*. For example, you may want to create a specific task for servers and set a rule for this task to allow installation of only Windows Update updates and only those ones that have *Approved* status. After that you manually set the *Approved* status for those updates that you want to install. In this case the Windows Update updates that have the *Undefined* or *Declined* status will not be installed on the servers that you specified in the task.

The usage of the *Approved* status to manage update installation is efficient for a small amount of updates. To install multiple updates, use the rules that you can configure in the *Install required updates and fix vulnerabilities* task. We recommend that you set the *Approved* status for only those specific updates that do not meet the criteria specified in the rules. When you manually approve a large amount of updates, performance of Administration Server decreases and may lead to Administration Server overload.

By default, the downloaded software updates have the *Undefined* status. You can change the status to *Approved* or *Declined* in the **SOFTWARE UPDATES** list (**OPERATIONS** → **PATCH MANAGEMENT** → **SOFTWARE UPDATES**).

How-to instructions:

- Administration Console: Approving and declining software updates (on page [435](#))

or

- Kaspersky Security Center 13 Web Console: Approving and declining third-party software updates (on page [1233](#))

f. Configuring Administration Server to work as Windows Server Update Services (WSUS) server (optional)

By default, Windows Update updates are downloaded to the managed devices from Microsoft servers. You can change this setting to use the Administration Server as WSUS server. In this case, the Administration Server synchronizes the update data with Windows Update at the specified frequency and provides updates in centralized mode to Windows Update on networked devices.

To use the Administration Server as WSUS server, create the Perform Windows Update synchronization task and select the **Use Administration Server as WSUS server** check box in the Network Agent policy.

How-to instructions:

- Administration Console: Synchronizing updates from Windows Update with Administration Server (on page [436](#)), Configuring Windows updates in a Network Agent policy (on page [455](#))

or

- Kaspersky Security Center 13 Web Console: Creating the Perform Windows Update synchronization task (on page [1234](#))

g. Running an update installation task

Start the *Install required updates and fix vulnerabilities* task or the *Install Windows Update updates* task. When you start these tasks, updates are downloaded and installed on managed devices. After the task is complete, make sure that it has the *Completed successfully* status in the task list.

h. Create the report on results of update installation of third-party software (optional)

To view detailed statistics on the update installation, create the **Report on results of installation of third-party software updates**.

How-to instructions:

- Administration Console: Creating and viewing a report (on page [509](#))

or

- Kaspersky Security Center 13 Web Console: Generating and viewing a report (on page [1287](#))

Results

If you have created and configured the *Install required updates and fix vulnerabilities* task, the updates are installed on the managed devices automatically. When new updates are downloaded to the Administration Server repository, Kaspersky Security Center checks whether they meet the criteria specified in the update rules. All new updates that meet the criteria will be installed automatically at the next task run.

If you have created the *Install Windows Update updates* task, only those updates specified in the *Install Windows Update updates* task properties are installed. In future, if you want to install new updates downloaded to the Administration Server repository, you must add the required updates to the list of updates in the existing task or create a new *Install Windows Update updates* task.

About third-party software updates

Kaspersky Security Center enables you to manage updates of third-party software installed on managed devices and fix vulnerabilities in Microsoft applications and other software makers' products through installation of required updates.

Kaspersky Security Center searches for updates through the *Find vulnerabilities and required updates* task. When this task is complete, Administration Server receives the lists of detected vulnerabilities and required updates for the third-party software installed on the devices that you specified in the task properties. After viewing information about available updates, you can install them on devices.

Kaspersky Security Center updates some applications by removing the previous version of the application and installing the new one.

A user interaction may be required when you update a third-party application or fix a vulnerability in a third-party application on a managed device. For example, the user may be prompted to close the third-party application if it's currently open.

You can find the details of third-party software that can be updated through Kaspersky Security Center by visiting the Technical Support website, on the Kaspersky Security Center page (<https://support.kaspersky.com/14758>), in the **Server Management** section.

Tasks for installation of third-party software updates

When metadata of the third-party software updates is downloaded to the repository, you can install the updates on client devices by using the following tasks:

- The *Install required updates and fix vulnerabilities* (see section "*Creating the Install required updates and fix vulnerabilities task*" on page [1221](#)) task

The *Install required updates and fix vulnerabilities* task is used to install updates for Microsoft applications, including the updates provided by the Windows Update service, and updates of other vendors' products. Note that this task can be created only if you have the license for the Vulnerability and Patch Management feature.

When this task is complete, the updates are installed on the managed devices automatically. When metadata of new updates is downloaded to the Administration Server repository, Kaspersky Security Center checks whether the updates meet the criteria specified in the update rules. All new updates that meet the criteria will be downloaded and installed automatically at the next task run.

- The *Install Windows Update updates* (see section "*Creating the Install Windows Update updates task*" on page [1229](#)) task

The *Install Windows Update updates* task does not require a license, but it can be used to install Windows Update updates only.

When this task is complete, only those updates that are specified in the task properties are installed. In future, if you want to install new updates downloaded to the Administration Server repository, you must add the required updates to the list of updates in the existing task or create a new *Install Windows Update updates* task.

Using Administration Server as WSUS server

Information about available updates for Microsoft Windows is provided by the Windows Update service. The Administration Server can be used as the Windows Server Update Services (WSUS) server. To use Administration Server as the WSUS server, you create the Perform Windows Update synchronization task and select the **Use Administration Server as WSUS server** check box in the Network Agent policy (see section "*Network Agent policy settings*" on page [665](#)). After you have configured data synchronization with Windows Update, Administration Server provides updates to Windows Update services on devices in centralized mode and with the set frequency.

Installing third-party software updates

The features provided under the Vulnerability and Patch Management license are only available in MMC-based Administration Console, and Kaspersky Security Center 12.2 Web Console or later versions.

You can install third-party software updates on managed devices by creating and running one of the following tasks:

- *Install required updates and fix vulnerabilities* (see section "Creating the *Install required updates and fix vulnerabilities* task" on page [1221](#))

The *Install required updates and fix vulnerabilities* task can be created only if you have a license for the Vulnerability and Patch Management feature. You can use this task to install both Windows Update updates provided by Microsoft and updates of other vendors' products.

- *Install Windows Update updates* (see section "Creating the *Install Windows Update updates* task" on page [1229](#))

You can use the *Install Windows Update updates* task to install Windows Update updates only.

A user interaction may be required when you update a third-party application or fix a vulnerability in a third-party application on a managed device. For example, the user may be prompted to close the third-party application if it's currently open.

As an option, you can create a task to install the required updates in the following ways:

- By opening the update list and specifying which updates to install.

As a result, a new task to install the selected updates is created. As an option, you can add the selected updates to an existing task.

- By running the Update Installation Wizard.

The Update Installation Wizard is only available under the Vulnerability and Patch Management license (see section "Kaspersky Security Center licensing options" on page [320](#)).

The Wizard simplifies creation and configuration of an update installation task, and allows you to eliminate the creation of redundant tasks that contain the same updates to install.

Installing third-party software updates by using the update list

► *To install third-party software updates by using the list of updates:*

1. Open one of the lists of updates:

- To open the general update list, go to **OPERATIONS** → **PATCH MANAGEMENT** → **SOFTWARE UPDATES**.
- To open the update list for a managed device, go to **DEVICES** → **MANAGED DEVICES** → <device name> → **Advanced** → **Available updates**.
- To open the update list for a specific application, go to **OPERATIONS** → **THIRD-PARTY APPLICATIONS** → **APPLICATIONS REGISTRY** → <application name> → **Available updates**.

A list of available updates appears.

2. Select the check boxes next to the updates that you want to install.
3. Click the **Install updates** button.

To install some software updates, you must accept the End User License Agreement (EULA). If you decline the EULA, the software update is not installed.

4. Select one of the following options:

- **New task**

The Add Task Wizard (see section "Creating a task" on page [1080](#)) starts. If you have the Vulnerability and Patch Management license (see section "Kaspersky Security Center licensing options" on page [320](#)), the *Install required updates and fix vulnerabilities* task is preselected. If you do not have the license, the *Install Windows Update updates* task is preselected. Follow the steps of the Wizard to complete the task creation.

- **Install update (add rule to specified task)**

Select a task to which you want to add the selected updates. If you have the Vulnerability and Patch Management license (see section "Kaspersky Security Center licensing options" on page [320](#)), select an *Install required updates and fix vulnerabilities* task. A new rule to install the selected updates will be automatically added to the selected task. If you do not have the license, select an *Install Windows Update updates* task. The selected updates will be added to the task properties.

The task properties window opens. Click the **Save** button to save the changes.

If you have chosen to create a new task, the task is created and displayed in the task list at **DEVICES** → **TASKS**. If you have chosen to add the updates to an existing task, the updates are saved in the task properties.

To install third-party software updates, start the *Install required updates and fix vulnerabilities* task or the *Install Windows Update updates* task. You can start any of these tasks manually (see section "Starting a task manually" on page [1080](#)) or specify schedule settings in the properties of the task that you start. When specifying the task schedule, make sure that the update installation task starts after the *Find vulnerabilities and required updates* task is complete.

Installing third-party software updates by using the Update Installation Wizard

The Update Installation Wizard is only available under the Vulnerability and Patch Management license (see section "Kaspersky Security Center licensing options" on page [320](#)).

► To create a task to install third-party software updates by using the Update Installation Wizard:

1. Select **OPERATIONS** → **PATCH MANAGEMENT**, and in the drop-down list, select **SOFTWARE UPDATES**.

A list of available updates appears.

2. Select the check box next to the update that you want to install.
3. Click the **Run Update Installation Wizard** button.

The Update Installation Wizard starts. The **Select the update installation task** page displays the list of all existing tasks of the following types:

- *Install required updates and fix vulnerabilities*
- *Install Windows Update updates*

- *Fix vulnerabilities*

You cannot modify the tasks of the last two types to install new updates. To install new updates, you can only use the *Install required updates and fix vulnerabilities* tasks.

4. If you want the Wizard to display only those tasks that install the update that you selected, then enable the **Show only tasks that install this update** option.
5. Choose what you want to do:
 - To start a task, select the check box next to the task name, and then click the **Start** button.
 - To add a new rule to an existing task:
 - a. Select the check box next to the task name, and then click the **Add rule** button.
 - b. On the page that opens, configure the new rule:
 - **Installation rule for updates of this importance level**
 - **Installation rule for updates of this importance level according to MSRC** (available only for Windows Update updates)
 - **Installation rule for updates by this vendor** (available only for updates of third-party applications)
 - **Installation rule for updates of the type**
 - **Installation rule for the selected update**
 - **Approve selected updates**

The selected update will be approved for installation. Enable this option if some applied rules of update installation allow installation of approved updates only.

By default, this option is disabled.

- **Automatically install all previous application updates that are required to install the selected updates**

Keep this option enabled if you agree with the installation of interim application versions when this is required for installing the selected updates.

If this option is disabled, only the selected versions of applications are installed. Disable this option if you want to update applications in a straightforward manner, without attempting to install successive versions incrementally. If installing the selected updates is not possible without installing previous versions of applications, the updating of the application fails.

For example, you have version 3 of an application installed on a device and you want to update it to version 5, but version 5 of this application can be installed only over version 4. If this option is enabled, the software first installs version 4, and then installs version 5. If this option is disabled, the software fails to update the application.

By default, this option is enabled.

- a. Click the **Add** button.
- To create a new task:
 - a. Click the **New task** button.
 - b. On the page that opens, configure the new rule:
 - **Installation rule for updates of this importance level**

- **Installation rule for updates of this importance level according to MSRC** (available only for Windows Update updates)
- **Installation rule for updates by this vendor** (available only for updates of third-party applications)
- **Installation rule for updates of the type**
- **Installation rule for the selected update**
- **Approve selected updates**

The selected update will be approved for installation. Enable this option if some applied rules of update installation allow installation of approved updates only.

By default, this option is disabled.

- **Automatically install all previous application updates that are required to install the selected updates**

Keep this option enabled if you agree with the installation of interim application versions when this is required for installing the selected updates.

If this option is disabled, only the selected versions of applications are installed. Disable this option if you want to update applications in a straightforward manner, without attempting to install successive versions incrementally. If installing the selected updates is not possible without installing previous versions of applications, the updating of the application fails.

For example, you have version 3 of an application installed on a device and you want to update it to version 5, but version 5 of this application can be installed only over version 4. If this option is enabled, the software first installs version 4, and then installs version 5. If this option is disabled, the software fails to update the application.

By default, this option is enabled.

- a. Click the **Add** button.

If you have chosen to start a task, you can close the Wizard. The task will complete in background mode. No further actions are required.

If you have chosen to add a rule to an existing task, the task properties window opens. The new rule is already added to the task properties. You can view or modify the rule or other task settings. Click the **Save** button to save the changes.

If you have chosen to create a new task, you continue to create the task (see section "Creating the Install required updates and fix vulnerabilities task" on page [1221](#)) in the New Task Wizard. The new rule that you added in the Update Installation Wizard is displayed in the New Task Wizard. When you complete the New Task Wizard, the *Install required updates and fix vulnerabilities* task is added to the task list.

Creating the Find vulnerabilities and required updates task

Through the Find vulnerabilities and required updates task, Kaspersky Security Center receives the lists of detected vulnerabilities and required updates for the third-party software installed on the managed devices.

The Find vulnerabilities and required updates task is created automatically when the Quick Start Wizard (see section "Quick Start Wizard (Kaspersky Security Center 13 Web Console)" on page [993](#)) is running. If you did not run the Wizard, you can create the task manually.

► *To create the Find vulnerabilities and required updates task:*

1. In the main application window, go to **DEVICES** → **TASKS**.
2. Click **Add**.
The Add Task Wizard starts. Proceed through the Wizard by using the **Next** button.
3. For the Kaspersky Security Center application, select the **Find vulnerabilities and required updates** task type.
4. Specify the name for the task that you are creating. A task name cannot be more than 100 characters long and cannot include any special characters ("*<>?\":|").
5. Select devices to which the task will be assigned.
6. If on the **Finish task creation** page you enable the **Open task details when creation is complete** option, you can modify the default task settings. If you do not enable this option, the task is created with the default settings. You can modify the default settings later, at any time.
7. Click the **Create** button.
The task is created and displayed in the list of tasks.
8. Click the name of the created task to open the task properties window.
9. In the task properties window, specify the general task settings (on page [1081](#)).
10. On the **Application settings** tab, specify the following settings:

- **Search for vulnerabilities and updates listed by Microsoft**

When searching for vulnerabilities and updates, Kaspersky Security Center uses the information about applicable Microsoft updates from the source of Microsoft updates, which are available at the present moment.

For example, you may want to disable this option if you have different tasks with different settings for Microsoft updates and updates of third-party applications.

By default, this option is enabled.

- **Connect to the update server to update data**

Windows Update Agent on a managed device connects to the source of Microsoft updates. The following servers can act as a source of Microsoft updates:

- Kaspersky Security Center Administration Server (see the settings of Network Agent policy (see section "Network Agent policy settings" on page [665](#)))
- Windows Server with Microsoft Windows Server Update Services (WSUS) deployed in your organization's network
- Microsoft Updates servers

If this option is enabled, Windows Update Agent on a managed device connects to the source of Microsoft updates to refresh the information about applicable Microsoft Windows updates.

If this option is disabled, Windows Update Agent on a managed device uses the information about applicable Microsoft Windows updates that was received from the source of Microsoft updates earlier and that is stored in the device's cache.

Connecting to the source of Microsoft updates can be resource-consuming. You might want to disable this option if you set regular connection to this source of updates in another task or in the properties of Network Agent policy, in the section **Software updates and vulnerabilities**. If you do not want to disable this option, then, to reduce the Server overload, you can configure the task schedule to randomize delay for task starts

within 360 minutes.

By default, this option is enabled.

Combination of the following options of the settings of Network Agent policy defines the mode of getting updates:

- Windows Update Agent on a managed device connects to the Update Server to get updates only if the **Connect to the update server to update data** option is enabled and the **Active** option, in the **Windows Update search mode** settings group, is selected.
- Windows Update Agent on a managed device uses the information about applicable Microsoft Windows updates that was received from the source of Microsoft updates earlier and that is stored in the device's cache, if the **Connect to the update server to update data** option is enabled and the **Passive** option, in the **Windows Update search mode** settings group, is selected, or if the **Connect to the update server to update data** option is disabled and the **Active** option, in the **Windows Update search mode** settings group, is selected.
- Irrespective of the **Connect to the update server to update data** option's status (enabled or disabled), if **Disabled** option, in the **Windows Update search mode** settings group is selected, Kaspersky Security Center does not request any information about updates.

- **Search for third-party vulnerabilities and updates listed by Kaspersky**

If this option is enabled, Kaspersky Security Center searches for vulnerabilities and required updates for third-party applications (applications made by software vendors other than Kaspersky and Microsoft) in Windows Registry and in the folders specified under **Specify paths for advanced search of applications in file system**. The full list of supported third-party applications is managed by Kaspersky.

If this option is disabled, Kaspersky Security Center does not search for vulnerabilities and required updates for third-party applications. For example, you may want to disable this option if you have different tasks with different settings for Microsoft Windows updates and updates of third-party applications.

By default, this option is enabled.

- **Specify paths for advanced search of applications across the file system**

The folders in which Kaspersky Security Center searches for third-party applications that require vulnerability fix and update installation. You can use system variables.

Specify the folders to which applications are installed. By default, the list contains system folders to which most of the applications are installed.

- **Enable advanced diagnostics**

If this feature is enabled, Network Agent writes traces even if tracing is disabled for Network Agent in Kaspersky Security Center Remote Diagnostics Utility. Traces are written to two files in turn; the total size of both files is determined by the **Maximum size, in MB, of advanced diagnostics files** value. When both files are full, Network Agent starts writing to them again. The files with traces are stored in the %WINDIR%\Temp folder. These files are accessible in the remote diagnostics utility (see section "Remote diagnostics of client devices. Kaspersky Security Center remote diagnostics utility" on page [651](#)), you can download or delete them there.

If this feature is disabled, Network Agent writes traces according to the settings in Kaspersky Security Center Remote Diagnostics Utility. No additional traces are written.

When creating a task, you do not have to enable advanced diagnostics. You may want to

use this feature later if, for example, a task run fails on some of the devices and you want to collect additional information during another task run.

By default, the feature is disabled.

- **Maximum size, in MB, of advanced diagnostics files**

The default value is 100 MB, and available values are between 1 MB and 2 048 MB. You may be asked to change the default value by Kaspersky Technical Support specialists when information in the advanced diagnostics files sent by you is not enough to troubleshoot the problem.

1. Click the **Save** button.

The task is created and configured.

If the task results contain a warning of the 0x80240033 "Windows Update Agent error 80240033 ("License terms could not be downloaded.")" error, you can resolve this issue through the Windows Registry (see section "Problems with tasks when using Administration Server as WSUS server" on page [886](#)).

See also:

Scenario: Finding and fixing vulnerabilities in third-party software	459
Scenario: Updating third-party software	1208

Find vulnerabilities and required updates task settings

The *Find vulnerabilities and required updates* task is created automatically when the Quick Start Wizard is running. If you did not run the Wizard, you can create the task manually.

In addition to the general task settings (on page [1081](#)), you can specify the following settings when creating the *Find vulnerabilities and required updates* task or later, when configuring the properties of the created task:

- **Search for vulnerabilities and updates listed by Microsoft**

When searching for vulnerabilities and updates, Kaspersky Security Center uses the information about applicable Microsoft updates from the source of Microsoft updates, which are available at the present moment.

For example, you may want to disable this option if you have different tasks with different settings for Microsoft updates and updates of third-party applications.

By default, this option is enabled.

- **Connect to the update server to update data**

Windows Update Agent on a managed device connects to the source of Microsoft updates. The following servers can act as a source of Microsoft updates:

- Kaspersky Security Center Administration Server (see the settings of Network Agent policy (see section "Network Agent policy settings" on page [665](#)))
- Windows Server with Microsoft Windows Server Update Services (WSUS) deployed

- in your organization's network
- Microsoft Updates servers

If this option is enabled, Windows Update Agent on a managed device connects to the source of Microsoft updates to refresh the information about applicable Microsoft Windows updates.

If this option is disabled, Windows Update Agent on a managed device uses the information about applicable Microsoft Windows updates that was received from the source of Microsoft updates earlier and that is stored in the device's cache.

Connecting to the source of Microsoft updates can be resource-consuming. You might want to disable this option if you set regular connection to this source of updates in another task or in the properties of Network Agent policy, in the section **Software updates and vulnerabilities**. If you do not want to disable this option, then, to reduce the Server overload, you can configure the task schedule to randomize delay for task starts within 360 minutes.

By default, this option is enabled.

Combination of the following options of the settings of Network Agent policy defines the mode of getting updates:

- Windows Update Agent on a managed device connects to the Update Server to get updates only if the **Connect to the update server to update data** option is enabled and the **Active** option, in the **Windows Update search mode** settings group, is selected.
- Windows Update Agent on a managed device uses the information about applicable Microsoft Windows updates that was received from the source of Microsoft updates earlier and that is stored in the device's cache, if the **Connect to the update server to update data** option is enabled and the **Passive** option, in the **Windows Update search mode** settings group, is selected, or if the **Connect to the update server to update data** option is disabled and the **Active** option, in the **Windows Update search mode** settings group, is selected.
- Irrespective of the **Connect to the update server to update data** option's status (enabled or disabled), if **Disabled** option, in the **Windows Update search mode** settings group is selected, Kaspersky Security Center does not request any information about updates.

- **Search for third-party vulnerabilities and updates listed by Kaspersky**

If this option is enabled, Kaspersky Security Center searches for vulnerabilities and required updates for third-party applications (applications made by software vendors other than Kaspersky and Microsoft) in Windows Registry and in the folders specified under **Specify paths for advanced search of applications in file system**. The full list of supported third-party applications is managed by Kaspersky.

If this option is disabled, Kaspersky Security Center does not search for vulnerabilities and required updates for third-party applications. For example, you may want to disable this option if you have different tasks with different settings for Microsoft Windows updates and updates of third-party applications.

By default, this option is enabled.

- **Specify paths for advanced search of applications across the file system**

The folders in which Kaspersky Security Center searches for third-party applications that require vulnerability fix and update installation. You can use system variables.

Specify the folders to which applications are installed. By default, the list contains system folders to which most of the applications are installed.

- **Enable advanced diagnostics**

If this feature is enabled, Network Agent writes traces even if tracing is disabled for Network Agent in Kaspersky Security Center Remote Diagnostics Utility. Traces are written to two files in turn; the total size of both files is determined by the **Maximum size, in MB, of advanced diagnostics files** value. When both files are full, Network Agent starts writing to them again. The files with traces are stored in the %WINDIR%\Temp folder. These files are accessible in the remote diagnostics utility (see section "Remote diagnostics of client devices. Kaspersky Security Center remote diagnostics utility" on page [651](#)), you can download or delete them there.

If this feature is disabled, Network Agent writes traces according to the settings in Kaspersky Security Center Remote Diagnostics Utility. No additional traces are written.

When creating a task, you do not have to enable advanced diagnostics. You may want to use this feature later if, for example, a task run fails on some of the devices and you want to collect additional information during another task run.

By default, the feature is disabled.

- **Maximum size, in MB, of advanced diagnostics files**

The default value is 100 MB, and available values are between 1 MB and 2 048 MB. You may be asked to change the default value by Kaspersky Technical Support specialists when information in the advanced diagnostics files sent by you is not enough to troubleshoot the problem.

Recommendations on the task schedule

When scheduling the *Find vulnerabilities and required updates* task, make sure that two options—**Run missed tasks** and **Use automatically randomized delay for task starts**—are enabled.

By default, the *Find vulnerabilities and required updates* task is set to start at 6:00 PM. If the organization's workplace rules provide for shutting down all devices at this time, the *Find vulnerabilities and required updates* task will run after the devices are turned on again, that is, in the morning of the next day. Such activity may be undesirable because a vulnerability scan may increase the load on CPUs and disk subsystems. You must set up the most convenient schedule for the task based on the workplace rules adopted in the organization.

See also:

Scanning applications for vulnerabilities.....	464
Scenario: Updating third-party software	1208
General task settings	928

Creating the Install required updates and fix vulnerabilities task

The *Install required updates and fix vulnerabilities* task is only available under the Vulnerability and Patch Management license (see section "Kaspersky Security Center licensing options" on page [320](#)). The features provided under the Vulnerability and Patch Management license are only available in MMC-based Administration Console, and Kaspersky Security Center 12.2 Web Console or later versions.

The *Install required updates and fix vulnerabilities* task is used to update and fix vulnerabilities in third-party software, including Microsoft software, installed on the managed devices. This task allows you to install multiple updates and fix multiple vulnerabilities according to certain rules.

To install updates or fix vulnerabilities by using the *Install required updates and fix vulnerabilities* task, you can do either of the following:

- Run the Update Installation Wizard (see section "Installing third-party software updates" on page [1212](#)) or the Vulnerability Fix Wizard (see section "Fixing vulnerabilities in third-party software" on page [1241](#)).
- Create a new *Install required updates and fix vulnerabilities* task.
- Add a rule for update installation (see section "Adding rules for update installation" on page [1225](#)) to an existing *Install required updates and fix vulnerabilities* task.

► *To create an Install required updates and fix vulnerabilities task:*

1. In the main application window, go to **DEVICES** → **TASKS**.
2. Click **Add**.
The Add Task Wizard starts. Proceed through the Wizard by using the **Next** button.
3. For the Kaspersky Security Center application, select the **Install required updates and fix vulnerabilities** task type.
4. Specify the name for the task that you are creating. A task name cannot be more than 100 characters long and cannot include any special characters ("*<>?:\|).").
5. Select devices to which the task will be assigned.
6. Specify the rules for update installation (see section "Adding rules for update installation" on page [1225](#)), and then specify the following settings:
 - **Start installation at device restart or shutdown**

If this option is enabled, updates are installed when the device is restarted or shut down. Otherwise, updates are installed according to a schedule.

Use this option if installing the updates might affect the device performance.

By default, this option is disabled.

- **Install required general system components**

If this option is enabled, before installing an update the application automatically installs all general system components (prerequisites) that are required to install the update. For example, these prerequisites can be operating system updates

If this option is disabled, you may have to install the prerequisites manually.

By default, this option is disabled.

- **Allow installation of new application versions during updates**

If this option is enabled, updates are allowed when they result in installation of a new version of a software application.

If this option is disabled, the software is not upgraded. You can then install new versions of the software manually or through another task. For example, you may use this option if your company infrastructure is not supported by a new software version or if you want to check an upgrade in a test infrastructure.

By default, this option is enabled.

Upgrading an application may cause malfunction of dependent applications installed on client devices.

- **Download updates to the device without installing them**

If this option is enabled, the application downloads updates to the device but does not install them automatically. You can then install downloaded updates manually.

Microsoft updates are downloaded to the system Windows storage. Updates of third-party applications (applications made by software vendors other than Kaspersky and Microsoft) are downloaded to the folder specified in the **Folder for downloading updates** field.

If this option is disabled, the updates are installed to the device automatically.

By default, this option is disabled.

- **Folder for downloading updates**

This folder is used to download updates of third-party applications (applications made by software vendors other than Kaspersky and Microsoft).

- **Enable advanced diagnostics**

If this feature is enabled, Network Agent writes traces even if tracing is disabled for Network Agent in Kaspersky Security Center Remote Diagnostics Utility. Traces are written to two files in turn; the total size of both files is determined by the **Maximum size, in MB, of advanced diagnostics files** value. When both files are full, Network Agent starts writing to them again. The files with traces are stored in the %WINDIR%\Temp folder. These files are accessible in the remote diagnostics utility (see section "Remote diagnostics of client devices. Kaspersky Security Center remote diagnostics utility" on page [651](#)), you can download or delete them there.

If this feature is disabled, Network Agent writes traces according to the settings in Kaspersky Security Center Remote Diagnostics Utility. No additional traces are written.

When creating a task, you do not have to enable advanced diagnostics. You may want to use this feature later if, for example, a task run fails on some of the devices and you want to collect additional information during another task run.

By default, the feature is disabled.

- **Maximum size, in MB, of advanced diagnostics files**

The default value is 100 MB, and available values are between 1 MB and 2 048 MB. You may be asked to change the default value by Kaspersky Technical Support specialists when information in the advanced diagnostics files sent by you is not enough to troubleshoot the problem.

1. Specify operating system restart settings:

- **Do not restart the device**

Client devices are not restarted automatically after the operation. To complete the operation, you must restart a device (for example, manually or through a device management task). Information about the required restart is saved in the task results and in the device status. This option is suitable for tasks on servers and other devices where continuous operation is critical.

- **Restart the device**

Client devices are always restarted automatically if a restart is required for completion of the operation. This option is useful for tasks on devices that provide for regular pauses in their operation (shutdown or restart).

- **Prompt user for action**

The restart reminder is displayed on the screen of the client device, prompting the user to restart it manually. Some advanced settings can be defined for this option: text of the message for the user, the message display frequency, and the time interval after which a restart will be forced (without the user's confirmation). This option is most suitable for workstations where users must be able to select the most convenient time for a restart.

By default, this option is selected.

- **Repeat prompt every (min)**

If this option is enabled, the application prompts the user to restart the operating system with the specified frequency.

By default, this option is enabled. The default interval is 5 minutes. Available values are between 1 and 1 440 minutes.

If this option is disabled, the prompt is displayed only once.

- **Restart after (min)**

After prompting the user, the application forces restart of the operating system upon expiration of the specified time interval.

By default, this option is enabled. The default delay is 30 minutes. Available values are between 1 and 1 440 minutes.

- **Wait time before forced closure of applications in blocked sessions (min)**

Applications are forced to close when the user's device goes locked (automatically after a specified interval of inactivity, or manually).

If this check box is selected, applications are forced to close on the locked device upon expiration of the time interval specified in the entry field.

If this check box is cleared, applications do not close on the locked device.

By default, this check box is cleared.

1. If on the **Finish task creation** page you enable the **Open task details when creation is complete** option, you can modify the default task settings. If you do not enable this option, the task is created with the default settings. You can modify the default settings later, at any time.
2. Click the **Finish** button.
The task is created and displayed in the list of tasks.
3. Click the name of the created task to open the task properties window.
4. In the task properties window, specify the general task settings (on page [1081](#)) according to your needs.
5. Click the **Save** button.

The task is created and configured.

If the task results contain a warning of the 0x80240033 "Windows Update Agent error 80240033 ("License terms could not be downloaded.")" error, you can resolve this issue through the Windows Registry (see section "Problems with tasks when using Administration Server as WSUS server" on page [886](#)).

See also:

Scenario: Updating third-party software[1208](#)

Adding rules for update installation

This feature is only available under the Vulnerability and Patch Management license (see section "Kaspersky Security Center licensing options" on page [320](#)).

The features provided under the Vulnerability and Patch Management license are only available in MMC-based Administration Console, and Kaspersky Security Center 12.2 Web Console or later versions.

When installing software updates or fixing software vulnerabilities by using the *Install required updates and fix vulnerabilities* task, you must specify rules for the update installation. These rules determine the updates to install and the vulnerabilities to fix.

The exact settings depend on whether you add a rule for all updates, for Windows Update updates, or for updates of third-party applications (applications made by software vendors other than Kaspersky and Microsoft). When adding a rule for Windows Update updates or updates of third-party applications, you can select specific applications and application versions for which you want to install updates. When adding a rule for all updates, you can select specific updates that you want to install and vulnerabilities that you want to fix by means of installing updates.

You can add a rule for update installation in the following ways:

- By adding a rule while creating a new *Install required updates and fix vulnerabilities* task (see section "Creating the *Install required updates and fix vulnerabilities* task" on page [1221](#)).
- By adding a rule on the **Application Settings** tab in the properties window of an existing *Install required updates and fix vulnerabilities* task.
- Through the Update Installation Wizard (see section "Installing third-party software updates" on page [1212](#)) or the Vulnerability Fix Wizard (see section "Fixing vulnerabilities in third-party software" on page [1241](#)).

► To add a new rule for all updates:

1. Click the **Add** button.

The Rule Creation Wizard starts. Proceed through the Wizard by using the Next button.

2. On the **Rule type** page, select **Rule for all updates**.
3. On the **General criteria** page, use the drop-down lists to specify the following settings:
 - Set of updates to install

Select the updates that must be installed on client devices:

- **Install approved updates only.** This installs only approved updates.
 - **Install all updates (except declined).** This installs updates with the *Approved* or *Undefined* approval status.
 - **Install all updates (including declined).** This installs all updates, regardless of their approval status. Select this option with caution. For example, use this option if you want to check installation of some declined updates in a test infrastructure.
- **Fix vulnerabilities with a severity level equal to or higher than**

Sometimes software updates may impair the user experience with the software. In such cases, you may decide to install only those updates that are critical for the software operation and to skip other updates.

If this option is enabled, the updates fix only those vulnerabilities for which the severity level set by Kaspersky is equal to or higher than the value selected in the list (**Medium**, **High**, or **Critical**). Vulnerabilities with a severity level lower than the selected value are not fixed.

If this option is disabled, the updates fix all vulnerabilities regardless of their severity level.

By default, this option is disabled.

1. On the **Updates** page, select the updates to be installed:

- **Install all suitable updates**

Install all software updates that meet the criteria specified on the **General criteria** page of the Wizard. Selected by default.

- **Install only updates from the list**

Install only software updates that you select manually from the list. This list contains all available software updates.

For example, you may want to select specific updates in the following cases: to check their installation in a test environment, to update only critical applications, or to update only specific applications.

- **Automatically install all previous application updates that are required to install the selected updates**

Keep this option enabled if you agree with the installation of interim application versions when this is required for installing the selected updates.

If this option is disabled, only the selected versions of applications are installed. Disable this option if you want to update applications in a straightforward manner, without attempting to install successive versions incrementally. If installing the selected updates is not possible without installing previous versions of applications, the updating of the application fails.

For example, you have version 3 of an application installed on a device and you want to update it to version 5, but version 5 of this application can be installed only over version 4. If this option is enabled, the software first installs version 4, and then installs version 5. If this option is disabled, the software fails to update the application.

By default, this option is enabled.

1. On the **Vulnerabilities** page, select vulnerabilities that will be fixed by installing the selected updates:

- **Fix all vulnerabilities that match other criteria**

Fix all vulnerabilities that meet the criteria specified on the **General criteria** page of the Wizard. Selected by default.

- **Fix only vulnerabilities from the list**

Fix only vulnerabilities that you select manually from the list. This list contains all detected vulnerabilities.

For example, you may want to select specific vulnerabilities in the following cases: to check their fix in a test environment, to fix vulnerabilities only in critical applications, or to fix vulnerabilities only in specific applications.

1. On the **Name** page, specify the name for the rule that you are adding. You can later change this name in the **Settings** section of the properties window of the created task.

After the Rule Creation Wizard completes its operation, the new rule is added and displayed in the rule list in the New Task Wizard or in the task properties.

► To add a new rule for Windows Update updates:

1. Click the **Add** button.

The Rule Creation Wizard starts. Proceed through the Wizard by using the Next button.

2. On the **Rule type** page, select **Rule for Windows Update**.

3. On the **General criteria** page, specify the following settings:

- Set of updates to install

Select the updates that must be installed on client devices:

- **Install approved updates only.** This installs only approved updates.
- **Install all updates (except declined).** This installs updates with the *Approved* or *Undefined* approval status.
- **Install all updates (including declined).** This installs all updates, regardless of their approval status. Select this option with caution. For example, use this option if you want to check installation of some declined updates in a test infrastructure.

- **Fix vulnerabilities with a severity level equal to or higher than**

Sometimes software updates may impair the user experience with the software. In such cases, you may decide to install only those updates that are critical for the software operation and to skip other updates.

If this option is enabled, the updates fix only those vulnerabilities for which the severity level set by Kaspersky is equal to or higher than the value selected in the list (**Medium**, **High**, or **Critical**). Vulnerabilities with a severity level lower than the selected value are not fixed.

If this option is disabled, the updates fix all vulnerabilities regardless of their severity level.

By default, this option is disabled.

- **Fix vulnerabilities with an MSRC severity level equal to or higher than**

Sometimes, software updates may impair the user experience with the software. In such cases, you may decide to install only those updates that are critical for the software operation and to skip other updates.

If this option is enabled, the updates fix only those vulnerabilities for which the severity level set by Microsoft Security Response Center (MSRC) is equal to or higher than the value selected in the list (**Low**, **Medium**, **High**, or **Critical**). Vulnerabilities with a severity level lower than the selected value are not fixed.

If this option is disabled, the updates fix all vulnerabilities regardless of their severity level.

By default, this option is disabled.

1. On the **Applications** page, select the applications and application versions for which you want to install updates. By default, all applications are selected.
2. On the **Categories of updates** page, select the categories of updates to be installed. These categories are the same as in Microsoft Update Catalog. By default, all categories are selected.
3. On the **Name** page, specify the name for the rule that you are adding. You can later change this name in the **Settings** section of the properties window of the created task.

After the Rule Creation Wizard completes its operation, the new rule is added and displayed in the rule list in the New Task Wizard or in the task properties.

► To add a new rule for updates of third-party applications:

1. Click the **Add** button.

The Rule Creation Wizard starts. Proceed through the Wizard by using the Next button.

2. On the **Rule type** page, select **Rule for third-party updates**.
3. On the **General criteria** page, specify the following settings:

- **Set of updates to install**

Select the updates that must be installed on client devices:

- **Install approved updates only.** This installs only approved updates.
- **Install all updates (except declined).** This installs updates with the *Approved* or *Undefined* approval status.
- **Install all updates (including declined).** This installs all updates, regardless of their approval status. Select this option with caution. For example, use this option if you want to check installation of some declined updates in a test infrastructure.

- **Fix vulnerabilities with a severity level equal to or higher than**

Sometimes software updates may impair the user experience with the software. In such cases, you may decide to install only those updates that are critical for the software operation and to skip other updates.

If this option is enabled, the updates fix only those vulnerabilities for which the severity level set by Kaspersky is equal to or higher than the value selected in the list (**Medium**, **High**, or **Critical**). Vulnerabilities with a severity level lower than the selected value are not fixed.

If this option is disabled, the updates fix all vulnerabilities regardless of their severity level.

By default, this option is disabled.

1. On the **Applications** page, select the applications and application versions for which you want to install updates. By default, all applications are selected.
2. On the **Name** page, specify the name for the rule that you are adding. You can later change this name in the Settings section of the properties window of the created task.

After the Rule Creation Wizard completes its operation, the new rule is added and displayed in the rule list in the New Task Wizard or in the task properties.

Creating the Install Windows Update updates task

The *Install Windows Update updates* task allows you to install software updates provided by the Windows Update service on managed devices.

If you do not have the Vulnerability and Patch Management license (see section "Kaspersky Security Center licensing options" on page [320](#)), you cannot create new tasks of the *Install Windows Update updates* type. To install new updates, you can add them to an existing *Install Windows Update updates* task. We recommend that you use the *Install required updates and fix vulnerabilities* (see section "Creating the Install required updates and fix vulnerabilities task" on page [1221](#)) task instead of the *Install Windows Update updates* task. The *Install required updates and fix vulnerabilities* task enables you to install multiple updates and fix multiple vulnerabilities automatically, according to the rules (see section "Adding rules for update installation" on page [1225](#)) that you define. In addition, this task enables you to install updates from software vendors other than Microsoft.

A user interaction may be required when you update a third-party application or fix a vulnerability in a third-party application on a managed device. For example, the user may be prompted to close the third-party application if it's currently open.

► *To create the Install Windows Update updates task:*

1. In the main application window, go to **DEVICES** → **TASKS**.
2. Click **Add**.

The Add Task Wizard starts. Proceed through the Wizard by using the **Next** button.

3. For the Kaspersky Security Center application, select the **Install Windows Update updates** task type.
4. Specify the name for the task that you are creating.
A task name cannot be more than 100 characters long and cannot include any special characters ("*<>?\\:|).

5. Select devices to which the task will be assigned.
6. Click the **Add** button.

The list of updates opens.

7. Select the Windows Update updates that you want to install, and then click **OK**.
8. Specify the operating system restart settings:

- **Do not restart the device**

Client devices are not restarted automatically after the operation. To complete the operation, you must restart a device (for example, manually or through a device management task). Information about the required restart is saved in the task results and in the device status. This option is suitable for tasks on servers and other devices where continuous operation is critical.

- **Restart the device**

Client devices are always restarted automatically if a restart is required for completion of the operation. This option is useful for tasks on devices that provide for regular pauses in their operation (shutdown or restart).

- **Prompt user for action**

The restart reminder is displayed on the screen of the client device, prompting the user to restart it manually. Some advanced settings can be defined for this option: text of the message for the user, the message display frequency, and the time interval after which a restart will be forced (without the user's confirmation). This option is most suitable for workstations where users must be able to select the most convenient time for a restart.

By default, this option is selected.

- **Repeat prompt every (min)**

If this option is enabled, the application prompts the user to restart the operating system with the specified frequency.

By default, this option is enabled. The default interval is 5 minutes. Available values are between 1 and 1 440 minutes.

If this option is disabled, the prompt is displayed only once.

- **Restart after (min)**

After prompting the user, the application forces restart of the operating system upon expiration of the specified time interval.

By default, this option is enabled. The default delay is 30 minutes. Available values are between 1 and 1 440 minutes.

- **Wait time before forced closure of applications in blocked sessions (min)**

Running applications may prevent a restart of the client device. For example, if a document is being edited in a word processing application and is not saved, the application does not allow the device to restart.

If this option is enabled, such applications on a locked device are forced to close before the device restart. As a result, users may lose their unsaved changes.

If this option is disabled, a locked device is not restarted. The task status on this device states that a device restart is required. Users have to manually close all applications running on locked devices and restart these devices.

By default, this option is disabled.

1. Specify the account settings:

- **Default account**

The task will be run under the same account as the application that performs this task.

By default, this option is selected.

- **Specify account**

Fill in the **Account** and **Password** fields to specify the details of an account under which the task is run. The account must have sufficient rights for this task.

- **Account**

Account under which the task is run.

- **Password**

Password of the account under which the task will be run.

2. If you want to modify the default task settings, enable the **Open task details when creation is complete** option on the **Finish task creation** page. If you do not enable this option, the task is created with the default settings. You can modify the default settings later, at any time.

3. Click the **Finish** button.

The task is created and displayed in the list of tasks.

4. Click the name of the created task to open the task properties window.
5. In the task properties window, specify the general task settings (on page [1081](#)) according to your needs.
6. Click the **Save** button.

The task is created and configured.


Viewing information about available third-party software updates

You can view the list of available updates for third-party software, including Microsoft software, installed on client devices.

► *To view a list of available updates for third-party applications installed on client devices:*

1. Select **OPERATIONS** → **PATCH MANAGEMENT**.
2. Select **SOFTWARE UPDATES** in the drop-down list.

A list of available updates appears.

You can specify a filter to view the list of software updates. Click the **Filter** icon () in the upper right corner of the software updates list to manage the filter. You can also select one of preset filters from the **Preset filters** drop-down list above the software vulnerabilities list.

► *To view the properties of an update:*

1. Click the name of the required software update.
2. The properties window of the update opens, displaying information grouped on the following tabs:
 - **General**
 - **Attributes**
 - **Devices**
 - **Fixed vulnerabilities**
 - **Crossover of updates** (available for Microsoft updates only)
 - **Tasks to install this update**

► *To view the statistics of an update installation:*

1. Select the check box next to the required software update.
2. Click the **Statistics of update installation statuses** button.

The diagram of the update installation statuses is displayed. Clicking a status opens a list of devices on which the update has the selected status.

You can view information about available software updates for third-party software, including Microsoft software, installed on the selected managed device running Windows.

► *To view a list of available updates for third-party software installed on the selected managed device:*

1. Select **DEVICES** → **MANAGED DEVICES**.

The list of managed devices is displayed.

2. In the list of managed devices, click the link with the name of the device for which you want to view third-party software updates.

The properties window of the selected device is displayed.

3. In the properties window of the selected device, select the **Advanced** tab.

4. In the left pane, select the **Available updates** section. If you want to view only installed updates, enable the **Show installed updates** option.

The list of available third-party software updates for the selected device is displayed.

See also:

Scenario: Updating third-party software..... [1208](#)

Exporting the list of available software updates to a file

You can export the list of updates for third-party software, including Microsoft software, that is displayed at the moment to the CSV or TXT files. You can use these files, for example, to send them to your information security manager or to store them for purposes of statistics.

► *To export to a text file the list of available updates for third-party software installed on all managed devices:*

1. On the **OPERATIONS** tab, in the **PATCH MANAGEMENT** drop-down list, select **SOFTWARE UPDATES**.

The page displays a list of available updates for third-party software installed on all managed devices.

2. Click the **Export rows to TXT file** or **Export rows to CSV file** button, depending on the format prefer for export.

The file containing the list of available updates for third-party software, including Microsoft software, is downloaded to the device that you use at the moment.

► *To export to a text file the list of available updates for third-party software installed on the selected managed device:*

1. Open the list of available third-party software updates on the selected managed device (see section "Viewing information about available third-party software updates" on page [1231](#)).

2. Select the software updates you want to export.

Skip this step if you want to export a complete list of software updates.

If you want to export a complete list of software updates, only updates displaying on the current page will be exported.

If you want to export only installed updates, select the **Show installed updates** check box.

3. Click the **Export rows to TXT file** or the **Export rows to CSV file** button, depending on the format you prefer for export.

The file containing the list of updates for third-party software, including Microsoft software, installed on the selected managed device is downloaded to the device you are using at the moment.

Approving and declining third-party software updates

When you configure the *Install required updates and fix vulnerabilities* task, you can create a rule that requires a specific status of updates that are to be installed. For example, an update rule can allow installation of the following:

- Only approved updates
- Only approved and undefined updates
- All updates irrespective of the update statuses

You can approve updates that must be installed and decline updates that must not be installed.

The usage of the *Approved* status to manage update installation is efficient for a small amount of updates. To install multiple updates, use the rules that you can configure in the *Install required updates and fix vulnerabilities* task. We recommend that you set the *Approved* status for only those specific updates that do not meet the criteria specified in the rules. When you manually approve a large amount of updates, performance of Administration Server decreases and may lead to Administration Server overload.

► *To approve or decline one or several updates:*

1. Select **OPERATIONS** → **PATCH MANAGEMENT**, and in the drop-down list select **SOFTWARE UPDATES**.

A list of available updates appears.

2. Select the updates that you want to approve or decline.
3. Click **Approve** to approve the selected updates or **Decline** to decline the selected updates.

The default value is *Undefined*.

The selected updates have the statuses that you defined.

As an option, you can change the approval status in the properties of a specific update.

► *To approve or decline an update in its properties:*

1. Select **OPERATIONS** → **PATCH MANAGEMENT**, and then select **SOFTWARE UPDATES** in the drop-down list.

A list of available updates appears.

2. Click the name of the update that you want to approve or decline.

The update properties window opens.

3. In the **General** section, select a status for the update by changing the **Update approval status** option. You can select the *Approved*, *Declined*, or *Undefined* status.
4. Click the **Save** button to save the changes.

The selected update has the status that you defined.

If you set **Declined** status for third-party software updates, these updates will not be installed on devices for which they were planned for installation but have not yet been installed. Updates will remain on devices on which they were already installed. If you have to delete them, you can manually delete them locally.

See also:

Scenario: Updating third-party software	1208
Creating the Install required updates and fix vulnerabilities task	1221

Creating the Perform Windows Update synchronization task

The *Perform Windows Update synchronization* task is only available under the Vulnerability and Patch Management license (see section "Kaspersky Security Center licensing options" on page [320](#)). The features provided under the Vulnerability and Patch Management license are only available in MMC-based Administration Console, and Kaspersky Security Center 12.2 Web Console or later versions.

The *Perform Windows Update synchronization* task is required if you want to use the Administration Server as a WSUS server. In this case, the Administration Server downloads Windows updates to the database, and provides the updates to Windows Update on client devices, in the centralized mode through Network Agents. If the network does not use a WSUS server, each client device downloads Microsoft updates from external servers independently.

The *Perform Windows Update synchronization* task only downloads metadata from Microsoft servers. Kaspersky Security Center downloads the updates when you run an update installation task and only those updates that you select for installation.

Microsoft regularly deletes outdated updates from the company's servers so the number of current updates is always between 200 000 and 300 000. In Kaspersky Security Center 10 Service Pack 2 Maintenance Release 1 and earlier versions, all updates were retained: no outdated updates were deleted. As a result, the database continuously grew in size. To reduce disk space usage and database size, deletion of outdated updates that are no longer present on Microsoft update servers has been implemented in Kaspersky Security Center 10 Service Pack 3.

When running the **Perform Windows Update synchronization** task, the application receives a list of current updates from a Microsoft update server. Next, Kaspersky Security Center compiles a list of updates that have become outdated. At the next start of the **Find vulnerabilities and required updates** task, Kaspersky Security Center flags all outdated updates and sets the deletion time for them. At the next start of the **Perform Windows Update synchronization** task, all updates flagged for deletion 30 days ago are deleted. Kaspersky Security Center also checks for outdated updates that were flagged for deletion more than 180 days ago, and then deletes those older updates.

When the **Perform Windows Update synchronization** task completes and outdated updates are deleted, the database may still have the hash codes pertaining to the files of deleted updates, as well as corresponding files in the %AllUsersProfile%\Application Data\KasperskyLab\adminkit\1093\working\wusfiles files (if they were

downloaded earlier). You can run the **Administration Server maintenance** (see section "**Administration Server maintenance**" on page [892](#)) task to delete these outdated records from the database and corresponding files.

► *To create the Perform Windows Update synchronization task:*

1. In the main application window, go to **DEVICES** → **TASKS**.
2. Click **Add**.
The Add Task Wizard starts. Proceed through the Wizard by using the **Next** button.
3. For the Kaspersky Security Center application, select the **Perform Windows Update synchronization** task type.
4. Specify the name for the task that you are creating. A task name cannot be more than 100 characters long and cannot include any special characters ("*<>?:|)").
5. Enable the **Download express installation files** option if you want the express update files to be downloaded when running the task.

When Kaspersky Security Center synchronizes updates with Microsoft Windows Update Servers, information about all files is saved in the Administration Server database. All files required for an update are also downloaded to the drive during interaction with the Windows Update Agent. In particular, Kaspersky Security Center saves information about express update files to the database and downloads them when necessary. Downloading express update files leads to decreased free space on the drive.

To avoid a decrease in disk space volume and to reduce traffic, disable the **Download express installation files** option.

6. Select the applications for which you want to download updates.
If the **All applications** check box is selected, updates will be downloaded for all existing applications, and for all applications that may be released in the future.
7. Select the categories of updates that you want to download to the Administration Server.
If the **All categories** check box is selected, updates will be downloaded for all existing updates categories, and for all categories that may appear in the future.
8. Select the localization languages for the updates that you want to download to the Administration Server. Select one of the following options:
 - **Download all languages, including new ones**
If this option is selected, all the available localization languages of updates will be downloaded to Administration Server. By default, this option is selected.
 - **Download selected languages**
If this option is selected, you can select from the list localization languages of updates that should be downloaded to Administration Server.
9. Specify which account to use when running the task. Select one of the following options:
 - **Default account**
The task will be run under the same account as the application that performs this task.
By default, this option is selected.
 - **Specify account**
Fill in the **Account** and **Password** fields to specify the details of an account under which the task is run. The account must have sufficient rights for this task.

10. If on the **Finish task creation** page you enable the **Open task details when creation is complete** option, you can modify the default task settings. If you do not enable this option, the task is created with the default settings. You can modify the default settings later, at any time.

11. Click the **Finish** button.

The task is created and displayed in the list of tasks.

12. To open the task properties window, click the name of the created task.

13. In the task properties window, specify the general task settings (on page [1081](#)) according to your needs.

14. Click the **Save** button.

The task is created and configured.

See also:

Scenario: Finding and fixing vulnerabilities in third-party software	459
Scenario: Updating third-party software.....	1208

Updating third-party applications automatically

Some third-party applications can be updated automatically. The application vendor defines whether or not the application supports the auto-update feature. If a third-party application installed on a managed device supports auto-update, you can specify the auto-update setting in the application properties. After you change the auto-update setting, Network Agents apply the new setting on each managed device on which the application is installed.

The auto-update setting is independent of the other objects and settings of the Vulnerability and Patch Management feature. For example, this setting does not depend on an update approval status or the update installation tasks, such as *Install required updates and fix vulnerabilities*, *Install Windows Update updates*, and *Fix vulnerabilities*.

► *To configure the auto-update setting for a third-party application:*

1. Go to **OPERATIONS** → **THIRD-PARTY APPLICATIONS** → **APPLICATIONS REGISTRY**.

2. Click the name of the application for which you want to change the auto-update setting.

To simplify the search, you can filter the list by the **Automatic Updates status** column.

The application properties window opens.

3. In the **General** section, select a value for the following setting:

Automatic Updates status

4. Click the **Save** button to save the changes.

The auto-update setting is applied to the selected application.

Fixing third-party software vulnerabilities

This section describes the features of Kaspersky Security Center that relate to fixing vulnerabilities in the software installed on managed devices.

In this section

Scenario: Finding and fixing vulnerabilities in third-party software	1237
About finding and fixing software vulnerabilities	1240
Fixing vulnerabilities in third-party software.....	1241
Creating the Fix vulnerabilities task.....	1244
Creating the Install required updates and fix vulnerabilities task	1246
Adding rules for update installation	1250
Selecting user fixes for vulnerabilities in third-party software.....	1253
Viewing information about software vulnerabilities detected on all managed devices.....	1254
Viewing information about software vulnerabilities detected on the selected managed device.....	1255
Viewing statistics of vulnerabilities on managed devices	1255
Exporting the list of software vulnerabilities to a file	1256
Ignoring software vulnerabilities	1256

Scenario: Finding and fixing vulnerabilities in third-party software

This section provides a scenario for finding and fixing vulnerabilities on the managed devices running Windows. You can find and fix software vulnerabilities in the operating system and in third-party software, including Microsoft software.

Prerequisites

- Kaspersky Security Center is deployed in your organization.
- There are managed devices running Windows in your organization.
- Internet connection is required for Administration Server to perform the following tasks:
 - To make a list of recommended fixes for vulnerabilities in Microsoft software. The list is created and regularly updated by Kaspersky specialists.
 - To fix vulnerabilities in third-part software other than Microsoft software.

Stages

Finding and fixing software vulnerabilities proceeds in stages:

a. Scanning for vulnerabilities in the software installed on the managed devices

To find vulnerabilities in the software installed on the managed devices, run the *Find vulnerabilities and required updates* task. When this task is complete, Kaspersky Security Center receives the lists of detected vulnerabilities and required updates for the third-party software installed on the devices that you specified in the task properties.

The *Find vulnerabilities and required updates* task is created automatically by Kaspersky Security Center Quick Start Wizard. If you did not run the Wizard, start it now or create the task manually.

How-to instructions:

- Administration Console: Scanning applications for vulnerabilities (on page [464](#)), Scheduling the Find vulnerabilities and required updates task (on page [372](#))

or

- Kaspersky Security Center 13 Web Console: Creating the Find vulnerabilities and required updates task (see section "Creating the Find vulnerabilities and required updates task" on page [1216](#)), Find vulnerabilities and required updates task settings (on page [1219](#))

b. Analyzing the list of detected software vulnerabilities

View the **Software vulnerabilities** list and decide which vulnerabilities are to be fixed. To view detailed information about each vulnerability, click the vulnerability name in the list. For each vulnerability in the list, you can also view the statistics on the vulnerability on managed devices.

How-to instructions:

- Administration Console: Viewing information about software vulnerabilities (on page [463](#)), Viewing statistics of vulnerabilities on managed devices (on page [463](#))

or

- Kaspersky Security Center 13 Web Console: Viewing information software vulnerabilities (see section "Viewing information about software vulnerabilities detected on all managed devices" on page [1254](#)), Viewing statistics of vulnerabilities on managed devices (on page [1255](#))

c. Configuring vulnerabilities fix

When the software vulnerabilities are detected, you can fix the software vulnerabilities on the managed devices by using the *Install required updates and fix vulnerabilities* (see section "Creating the *Install required updates and fix vulnerabilities task*" on page [1221](#)) task or the *Fix vulnerabilities* (see section "Creating the *Fix vulnerabilities task*" on page [1244](#)) task.

The *Install required updates and fix vulnerabilities* task is used to update and fix vulnerabilities in third-party software, including Microsoft software, installed on the managed devices. This task allows you to install multiple updates and fix multiple vulnerabilities according to certain rules. Note that this task can be created only if you have the license for the Vulnerability and Patch Management feature. To fix software vulnerabilities the *Install required updates and fix vulnerabilities* task uses recommended software updates.

The *Fix vulnerabilities* task does not require the license option for the Vulnerability and Patch Management feature. To use this task, you must manually specify user fixes for vulnerabilities in third-party software listed in the task settings. The *Fix vulnerabilities* task uses recommended fixes for Microsoft software and user fixes for third-party software.

You can start Vulnerabilities Fix Wizard that creates one of these tasks automatically, or you can create one of these tasks manually.

How-to instructions:

- Administration Console: Selecting user fixes for vulnerabilities in third-party software (on page [481](#)), Fixing vulnerabilities in applications (on page [469](#))

or

- Kaspersky Security Center 13 Web Console: Selecting user fixes for vulnerabilities in third-party software (on page [1253](#)), Fixing vulnerabilities in third-party software (on page [1241](#)), Creating the *Install required updates and fix vulnerabilities task* (on page [1221](#))

d. Scheduling the tasks

To be sure that the vulnerabilities list is always up-to-date, schedule the *Find vulnerabilities and required updates* task to run it automatically from time to time. The recommended average frequency is once a week.

If you have created the *Install required updates and fix vulnerabilities* task, you can schedule it to run with the same frequency as the *Find vulnerabilities and required updates* task or less often. When scheduling the *Fix vulnerabilities* task, note that you have to select fixes for Microsoft software or specify user fixes for third-party software every time before starting the task.

When scheduling the tasks, make sure that a task to fix vulnerability starts after the *Find vulnerabilities and required updates* task is complete.

e. Ignoring software vulnerabilities (optional)

If you want, you can ignore software vulnerabilities to be fixed on all managed devices or only on the selected managed devices.

How-to instructions:

- Administration Console: Ignoring software vulnerabilities (on page [480](#))

or

- Kaspersky Security Center 13 Web Console: Ignoring software vulnerabilities (on page [1256](#))

f. Running a vulnerability fix task

Start the *Install required updates and fix vulnerabilities* task or the *Fix vulnerability* task. When the task is complete, make sure that it has the *Completed successfully* status in the task list.

g. Create the report on results of fixing software vulnerabilities (optional)

To view detailed statistics on the vulnerabilities fix, generate the Report on vulnerabilities. The report displays information about software vulnerabilities that are not fixed. Thus you can have an idea about finding and fixing vulnerabilities in third-party software, including Microsoft software, in your organization.

How-to instructions:

- Administration Console: Creating and viewing a report (on page [509](#))

or

- Kaspersky Security Center 13 Web Console: Generating and viewing a report (on page [1287](#))

h. Checking configuration of finding and fixing vulnerabilities in third-party software

Be sure you have done the following:

- Obtained and reviewed the list of software vulnerabilities on managed devices
- Ignored software vulnerabilities if you wanted
- Configured the task to fix vulnerabilities
- Scheduled the tasks to find and to fix software vulnerabilities so that they start sequentially
- Checked that the task to fix software vulnerabilities was run

Results

If you have created and configured the *Install required updates and fix vulnerabilities* task, the vulnerabilities are fixed on the managed devices automatically. When the task is run, it correlates the list of available software updates to the rules specified in the task settings. All software updates that meet the criteria in the rules will be downloaded to the Administration Server repository and will be installed to fix software vulnerabilities.

If you have created the *Fix vulnerabilities* task, only software vulnerabilities in Microsoft software are fixed.

About finding and fixing software vulnerabilities

Kaspersky Security Center detects and fixes software vulnerabilities on managed devices running Microsoft Windows families operating systems. Vulnerabilities are detected in the operating system and in third-party software, including Microsoft software.

Finding software vulnerabilities

To find software vulnerabilities, Kaspersky Security Center uses characteristics from the database of known vulnerabilities. This database is created by Kaspersky specialists. It contains information about vulnerabilities, such as vulnerability description, vulnerability detect date, vulnerability severity level. You can find the details of software vulnerabilities on Kaspersky website (<https://threats.kaspersky.com/en/>).

Kaspersky Security Center uses the *Find vulnerabilities and required updates* task to find software vulnerabilities.

Fixing software vulnerabilities

To fix software vulnerabilities Kaspersky Security Center uses software updates issued by the software vendors. The software updates metadata is downloaded to the Administration Server repository as a result of the following tasks run:

- *Download updates to the Administration Server repository.* This task is intended to download updates metadata for Kaspersky and third-party software. This task is created automatically by the Kaspersky Security Center Quick Start Wizard. You can create the Download updates to the Administration Server repository task (see section "Creating the task for downloading updates to the repository of the Administration Server" on page [1184](#)) manually.
- *Perform Windows Update synchronization.* This task is intended to download updates metadata for Microsoft software.

Software updates to fix vulnerabilities can be represented as full distribution packages or patches. Software updates that fix software vulnerabilities are named *fixes*. *Recommended fixes* are those that are recommended for installation by Kaspersky specialists. *User fixes* are those that are manually specified for installation by users. To install a user fix, you have to create an installation package containing this fix.

If you have the Kaspersky Security Center license with the Vulnerability and Patch Management feature, to fix software vulnerabilities you can use *Install required updates and fix vulnerabilities* task. This task automatically fixes multiple vulnerabilities installing recommended fixes. For this task, you can manually configure certain rules to fix multiple vulnerabilities.

If you do not have the Kaspersky Security Center license with the Vulnerability and Patch Management feature, to fix software vulnerabilities, you can use the *Fix vulnerabilities* task. By means of this task, you can fix vulnerabilities by installing recommended fixes for Microsoft software and user fixes for other third-party software.

A user interaction may be required when you update a third-party application or fix a vulnerability in a third-party application on a managed device. For example, the user may be prompted to close the third-party application if it's currently open.

To fix some software vulnerabilities, you must accept the End User License Agreement (EULA) of the software that is being installed, if EULA acceptance is requested. If you decline the EULA, the software vulnerability is not fixed.

Fixing vulnerabilities in third-party software

The features provided under the Vulnerability and Patch Management license are only available in MMC-based Administration Console, and Kaspersky Security Center 12.2 Web Console or later versions.

After you obtain the software vulnerabilities list, you can fix software vulnerabilities on managed devices that are running Windows. You can fix software vulnerabilities in the operating system and in third-party software, including Microsoft software, by creating and running the *Fix vulnerabilities* (see section "Creating the Fix vulnerabilities task" on page [1244](#)) task or the *Install required updates and fix vulnerabilities* (see section "Creating the Install required updates and fix vulnerabilities task" on page [1221](#)) task.

A user interaction may be required when you update a third-party application or fix a vulnerability in a third-party application on a managed device. For example, the user may be prompted to close the third-party application if it's currently open.

As an option, you can create a task to fix software vulnerabilities in the following ways:

- By opening the vulnerability list and specifying which vulnerabilities to fix.
As a result, a new task to fix software vulnerabilities is created. As an option, you can add the selected vulnerabilities to an existing task.
- By running the Vulnerability Fix Wizard.

The Vulnerability Fix Wizard is only available under the Vulnerability and Patch Management license (see section "Kaspersky Security Center licensing options" on page [320](#)).

The Wizard simplifies creation and configuration of a vulnerability fix task and allows you to eliminate the creation of redundant tasks that contain the same updates to install.

Fixing software vulnerabilities by using the vulnerability list

► *To fix software vulnerabilities:*

1. Open one of the lists of vulnerabilities:
 - To open the general vulnerability list, go to **OPERATIONS** → **PATCH MANAGEMENT** → **Software vulnerabilities**.
 - To open the vulnerability list for a managed device, go to **DEVICES** → **MANAGED DEVICES** → <device name> → **Advanced** → **Software vulnerabilities**.
 - To open the vulnerability list for a specific application, go to **OPERATIONS** → **THIRD-PARTY APPLICATIONS** → **APPLICATIONS REGISTRY** → <application name> → **Vulnerabilities**.

A page with a list of vulnerabilities in the third-party software is displayed.

2. Select one or more vulnerabilities in the list, and then click the **Fix vulnerability** button.

If a recommended software update to fix one of the selected vulnerabilities is absent, an informative message is displayed.

To fix some software vulnerabilities, you must accept the End User License Agreement (EULA) for installing the software, if EULA acceptance is requested. If you decline the EULA, the software vulnerability is not fixed.

3. Select one of the following options:

- **New task**

The Add Task Wizard (see section "Creating a task" on page [1080](#)) starts. If you have the Vulnerability and Patch Management license (see section "Kaspersky Security Center licensing options" on page [320](#)), the *Install required updates and fix vulnerabilities* task is preselected. If you do not have the license, the *Fix vulnerabilities* task is preselected. Follow the steps of the Wizard to complete the task creation.

- **Fix vulnerability (add rule to specified task)**

Select a task to which you want to add the selected vulnerabilities. If you have the Vulnerability and Patch Management license (see section "Kaspersky Security Center licensing options" on page [320](#)), select an *Install required updates and fix vulnerabilities* task. A new rule to fix the selected vulnerabilities will be automatically added to the selected task. If you do not have the license, select a *Fix vulnerabilities* task. The selected vulnerabilities will be added to the task properties.

The task properties window opens. Click the **Save** button to save the changes.

If you have chosen to create a new task, the task is created and displayed in the task list at **DEVICES** → **TASKS**. If you have chosen to add the vulnerabilities to an existing task, the vulnerabilities are saved in the task properties.

To fix the third-party software vulnerabilities, start the *Install required updates and fix vulnerabilities* task or the *Fix vulnerabilities* task. If you have created the *Fix vulnerabilities* task, you must manually specify the software updates to fix the software vulnerabilities listed in the task settings.

Fixing software vulnerabilities by using the Vulnerability Fix Wizard

The Vulnerability Fix Wizard is only available under the Vulnerability and Patch Management license (see section "Kaspersky Security Center licensing options" on page [320](#)).

► *To fix software vulnerabilities by using the Vulnerability Fix Wizard:*

1. On the **OPERATIONS** tab, in the **PATCH MANAGEMENT** drop-down list, select **Software vulnerabilities**.
A page with a list of vulnerabilities in the third-party software installed on managed devices is displayed.
2. Select the check box next to the vulnerability that you want to fix.
3. Click the **Run Vulnerability Fix Wizard** button.

The Vulnerability Fix Wizard starts. The **Select the vulnerability fix task** page displays the list of all existing tasks of the following types:

- *Install required updates and fix vulnerabilities*
- *Install Windows Update updates*
- *Fix vulnerabilities*

You cannot modify the last two types of tasks to install new updates. To install new updates, you can only use the *Install required updates and fix vulnerabilities* task.

4. If you want the Wizard to display only those tasks that fix the vulnerability that you selected, then enable the **Show only tasks that fix this vulnerability** option.
5. Choose what you want to do:
 - To start a task, select the check box next to the task name, and then click the **Start** button.
 - To add a new rule to an existing task:
 - a. Select the check box next to the task name, and then click the **Add rule** button.
 - b. On the page that opens, configure the new rule:
 - **Rule for fixing vulnerabilities of this severity level**
 - **Rule for fixing vulnerabilities by means of updates of the same type as the update defined as recommended for the selected vulnerability** (available only for Microsoft software vulnerabilities)
 - **Rule for fixing vulnerabilities in applications from the selected vendor** (available only for third-party software vulnerabilities)
 - **Rule for fixing a vulnerability in all versions of the selected application** (available only for third-party software vulnerabilities)
 - **Rule for fixing the selected vulnerability**
 - **Approve updates that fix this vulnerability**

The selected update will be approved for installation. Enable this option if some applied rules of update installation allow installation of approved updates only.

By default, this option is disabled.

- a. Click the **Add** button.
- To create a new task:
 - a. Click the **New task** button.
 - b. On the page that opens, configure the new rule:
 - **Rule for fixing vulnerabilities of this severity level**
 - **Rule for fixing vulnerabilities by means of updates of the same type as the update defined as recommended for the selected vulnerability** (available only for Microsoft software vulnerabilities)
 - **Rule for fixing vulnerabilities in applications from the selected vendor** (available only for third-party software vulnerabilities)
 - **Rule for fixing a vulnerability in all versions of the selected application** (available only for third-party software vulnerabilities)
 - **Rule for fixing the selected vulnerability**
 - **Approve updates that fix this vulnerability**

The selected update will be approved for installation. Enable this option if some applied rules of update installation allow installation of approved updates only.

By default, this option is disabled.

- a. Click the **Add** button.

If you have chosen to start a task, you can close the Wizard. The task will complete in background mode. No further actions are required.

If you have chosen to add a rule to an existing task, the task properties window opens. The new rule is already added to the task properties. You can view or modify the rule or other task settings. Click the **Save** button to save the changes.

If you have chosen to create a new task, you continue to create the task (see section "Creating the Install required updates and fix vulnerabilities task" on page [1221](#)) in the New Task Wizard. The new rule that you added in the Vulnerability Fix Wizard is displayed in the New Task Wizard. When you complete the New Task Wizard, the *Install required updates and fix vulnerabilities* task is added to the task list.

Creating the Fix vulnerabilities task

The *Fix vulnerabilities* task allows you fix software vulnerabilities on managed devices that are running Windows. You can fix software vulnerabilities in third-party software, including Microsoft software.

If you have the Vulnerability and Patch Management license (see section "Kaspersky Security Center licensing options" on page [320](#)), you cannot create new tasks of the *Fix vulnerabilities* type. To fix new vulnerabilities, you can add them to an existing *Fix vulnerabilities* task. We recommend that you use the *Install required updates and fix vulnerabilities* (see section "Creating the Install required updates and fix vulnerabilities task" on page [1221](#)) task instead of the *Fix vulnerabilities* task. The *Install required updates and fix vulnerabilities* task enables you to install multiple updates and fix multiple vulnerabilities automatically, according to the rules (see section "Adding rules for update installation" on page [1225](#)) that you define.

A user interaction may be required when you update a third-party application or fix a vulnerability in a third-party application on a managed device. For example, the user may be prompted to close the third-party application if it's currently open.

► To create the *Fix vulnerabilities* task:

1. In the main application window, go to **DEVICES** → **TASKS**.

2. Click **Add**.

The Add Task Wizard starts. Proceed through the Wizard by using the **Next** button.

3. For the Kaspersky Security Center application, select the **Fix vulnerabilities** task type.
4. Specify the name for the task that you are creating.

A task name cannot be more than 100 characters long and cannot include any special characters ("* <> ? \ : |).

5. Select devices to which the task will be assigned.
6. Click the **Add** button.

The list of vulnerabilities opens.

7. Select the vulnerabilities that you want to fix, and then click **OK**.

Microsoft software vulnerabilities usually have recommended fixes. No additional actions are required for them. For vulnerabilities in software from other vendors, you first need to specify a user fix for each vulnerability (see section "Selecting user fixes for vulnerabilities in third-party software" on page [1253](#)) that you want to fix. After that, you will be able to add those vulnerabilities into the *Fix vulnerabilities* task.

8. Specify the operating system restart settings:

- **Do not restart the device**

Client devices are not restarted automatically after the operation. To complete the operation, you must restart a device (for example, manually or through a device management task). Information about the required restart is saved in the task results and in the device status. This option is suitable for tasks on servers and other devices where continuous operation is critical.

- **Restart the device**

Client devices are always restarted automatically if a restart is required for completion of the operation. This option is useful for tasks on devices that provide for regular pauses in their operation (shutdown or restart).

- **Prompt user for action**

The restart reminder is displayed on the screen of the client device, prompting the user to restart it manually. Some advanced settings can be defined for this option: text of the message for the user, the message display frequency, and the time interval after which a restart will be forced (without the user's confirmation). This option is most suitable for workstations where users must be able to select the most convenient time for a restart.

By default, this option is selected.

- **Repeat prompt every (min)**

If this option is enabled, the application prompts the user to restart the operating system with the specified frequency.

By default, this option is enabled. The default interval is 5 minutes. Available values are between 1 and 1 440 minutes.

If this option is disabled, the prompt is displayed only once.

- **Restart after (min)**

After prompting the user, the application forces restart of the operating system upon expiration of the specified time interval.

By default, this option is enabled. The default delay is 30 minutes. Available values are between 1 and 1 440 minutes.

- **Wait time before forced closure of applications in blocked sessions (min)**

Running applications may prevent a restart of the client device. For example, if a document is being edited in a word processing application and is not saved, the application does not allow the device to restart.

If this option is enabled, such applications on a locked device are forced to close before the device restart. As a result, users may lose their unsaved changes.

If this option is disabled, a locked device is not restarted. The task status on this device states that a device restart is required. Users have to manually close all applications running on locked devices and restart these devices.

By default, this option is disabled.

1. Specify the account settings:

- **Default account**

The task will be run under the same account as the application that performs this task.

By default, this option is selected.

- **Specify account**

Fill in the **Account** and **Password** fields to specify the details of an account under which the task is run. The account must have sufficient rights for this task.

- **Account**

Account under which the task is run.

- **Password**

Password of the account under which the task will be run.

2. If you want to modify the default task settings, enable the **Open task details when creation is complete** option on the **Finish task creation** page. If you do not enable this option, the task is created with the default settings. You can modify the default settings later, at any time.
3. Click the **Finish** button.
The task is created and displayed in the list of tasks.
4. Click the name of the created task to open the task properties window.
5. In the task properties window, specify the general task settings (on page [1081](#)) according to your needs.
6. Click the **Save** button.

The task is created and configured.

Creating the Install required updates and fix vulnerabilities task

The *Install required updates and fix vulnerabilities* task is only available under the Vulnerability and Patch Management license (see section "Kaspersky Security Center licensing options" on page [320](#)). The features provided under the Vulnerability and Patch Management license are only available in MMC-based Administration Console, and Kaspersky Security Center 12.2 Web Console or later versions.

The *Install required updates and fix vulnerabilities* task is used to update and fix vulnerabilities in third-party software, including Microsoft software, installed on the managed devices. This task allows you to install multiple updates and fix multiple vulnerabilities according to certain rules.

To install updates or fix vulnerabilities by using the *Install required updates and fix vulnerabilities* task, you can do either of the following:

- Run the Update Installation Wizard (see section "Installing third-party software updates" on page [1212](#)) or the Vulnerability Fix Wizard (see section "Fixing vulnerabilities in third-party software" on page [1241](#)).
- Create a new *Install required updates and fix vulnerabilities* task.
- Add a rule for update installation (see section "Adding rules for update installation" on page [1225](#)) to an existing *Install required updates and fix vulnerabilities* task.

► *To create an Install required updates and fix vulnerabilities task:*

1. In the main application window, go to **DEVICES** → **TASKS**.

2. Click **Add**.

The Add Task Wizard starts. Proceed through the Wizard by using the **Next** button.

3. For the Kaspersky Security Center application, select the **Install required updates and fix vulnerabilities** task type.

4. Specify the name for the task that you are creating. A task name cannot be more than 100 characters long and cannot include any special characters ("* <> ? \ : |").

5. Select devices to which the task will be assigned.

6. Specify the rules for update installation (see section "Adding rules for update installation" on page [1225](#)), and then specify the following settings:

- **Start installation at device restart or shutdown**

If this option is enabled, updates are installed when the device is restarted or shut down. Otherwise, updates are installed according to a schedule.

Use this option if installing the updates might affect the device performance.

By default, this option is disabled.

- **Install required general system components**

If this option is enabled, before installing an update the application automatically installs all general system components (prerequisites) that are required to install the update. For example, these prerequisites can be operating system updates

If this option is disabled, you may have to install the prerequisites manually.

By default, this option is disabled.

- **Allow installation of new application versions during updates**

If this option is enabled, updates are allowed when they result in installation of a new version of a software application.

If this option is disabled, the software is not upgraded. You can then install new versions of the software manually or through another task. For example, you may use this option if your company infrastructure is not supported by a new software version or if you want to check an upgrade in a test infrastructure.

By default, this option is enabled.

Upgrading an application may cause malfunction of dependent applications installed on client devices.

- **Download updates to the device without installing them**

If this option is enabled, the application downloads updates to the device but does not install them automatically. You can then Install downloaded updates manually.

Microsoft updates are downloaded to the system Windows storage. Updates of third-party applications (applications made by software vendors other than Kaspersky and Microsoft) are downloaded to the folder specified in the **Folder for downloading updates** field.

If this option is disabled, the updates are installed to the device automatically.

By default, this option is disabled.

- **Folder for downloading updates**

This folder is used to download updates of third-party applications (applications made by software vendors other than Kaspersky and Microsoft).

- **Enable advanced diagnostics**

If this feature is enabled, Network Agent writes traces even if tracing is disabled for Network Agent in Kaspersky Security Center Remote Diagnostics Utility. Traces are written to two files in turn; the total size of both files is determined by the **Maximum size, in MB, of advanced diagnostics files** value. When both files are full, Network Agent starts writing to them again. The files with traces are stored in the %WINDIR%\Temp folder. These files are accessible in the remote diagnostics utility (see section "Remote diagnostics of client devices. Kaspersky Security Center remote diagnostics utility" on page [651](#)), you can download or delete them there.

If this feature is disabled, Network Agent writes traces according to the settings in Kaspersky Security Center Remote Diagnostics Utility. No additional traces are written.

When creating a task, you do not have to enable advanced diagnostics. You may want to use this feature later if, for example, a task run fails on some of the devices and you want to collect additional information during another task run.

By default, the feature is disabled.

- **Maximum size, in MB, of advanced diagnostics files**

The default value is 100 MB, and available values are between 1 MB and 2 048 MB. You may be asked to change the default value by Kaspersky Technical Support specialists when information in the advanced diagnostics files sent by you is not enough to troubleshoot the problem.

1. Specify operating system restart settings:

- **Do not restart the device**

Client devices are not restarted automatically after the operation. To complete the operation, you must restart a device (for example, manually or through a device management task). Information about the required restart is saved in the task results and in the device status. This option is suitable for tasks on servers and other devices where continuous operation is critical.

- **Restart the device**

Client devices are always restarted automatically if a restart is required for completion of the operation. This option is useful for tasks on devices that provide for regular pauses in their operation (shutdown or restart).

- **Prompt user for action**

The restart reminder is displayed on the screen of the client device, prompting the user to restart it manually. Some advanced settings can be defined for this option: text of the message for the user, the message display frequency, and the time interval after which a

restart will be forced (without the user's confirmation). This option is most suitable for workstations where users must be able to select the most convenient time for a restart.

By default, this option is selected.

- **Repeat prompt every (min)**

If this option is enabled, the application prompts the user to restart the operating system with the specified frequency.

By default, this option is enabled. The default interval is 5 minutes. Available values are between 1 and 1 440 minutes.

If this option is disabled, the prompt is displayed only once.

- **Restart after (min)**

After prompting the user, the application forces restart of the operating system upon expiration of the specified time interval.

By default, this option is enabled. The default delay is 30 minutes. Available values are between 1 and 1 440 minutes.

- **Wait time before forced closure of applications in blocked sessions (min)**

Applications are forced to close when the user's device goes locked (automatically after a specified interval of inactivity, or manually).

If this check box is selected, applications are forced to close on the locked device upon expiration of the time interval specified in the entry field.

If this check box is cleared, applications do not close on the locked device.

By default, this check box is cleared.

1. If on the **Finish task creation** page you enable the **Open task details when creation is complete** option, you can modify the default task settings. If you do not enable this option, the task is created with the default settings. You can modify the default settings later, at any time.
2. Click the **Finish** button.
The task is created and displayed in the list of tasks.
3. Click the name of the created task to open the task properties window.
4. In the task properties window, specify the general task settings (on page [1081](#)) according to your needs.
5. Click the **Save** button.
The task is created and configured.

If the task results contain a warning of the 0x80240033 "Windows Update Agent error 80240033 ("License terms could not be downloaded.")" error, you can resolve this issue through the Windows Registry (see section "Problems with tasks when using Administration Server as WSUS server" on page [886](#)).

See also:

Scenario: Updating third-party software[1208](#)

Adding rules for update installation

This feature is only available under the Vulnerability and Patch Management license (see section "Kaspersky Security Center licensing options" on page [320](#)).
The features provided under the Vulnerability and Patch Management license are only available in MMC-based Administration Console, and Kaspersky Security Center 12.2 Web Console or later versions.

When installing software updates or fixing software vulnerabilities by using the *Install required updates and fix vulnerabilities* task, you must specify rules for the update installation. These rules determine the updates to install and the vulnerabilities to fix.

The exact settings depend on whether you add a rule for all updates, for Windows Update updates, or for updates of third-party applications (applications made by software vendors other than Kaspersky and Microsoft). When adding a rule for Windows Update updates or updates of third-party applications, you can select specific applications and application versions for which you want to install updates. When adding a rule for all updates, you can select specific updates that you want to install and vulnerabilities that you want to fix by means of installing updates.

You can add a rule for update installation in the following ways:

- By adding a rule while creating a new *Install required updates and fix vulnerabilities* task (see section "Creating the *Install required updates and fix vulnerabilities* task" on page [1221](#)).
- By adding a rule on the **Application Settings** tab in the properties window of an existing *Install required updates and fix vulnerabilities* task.
- Through the Update Installation Wizard (see section "Installing third-party software updates" on page [1212](#)) or the Vulnerability Fix Wizard (see section "Fixing vulnerabilities in third-party software" on page [1241](#)).

► To add a new rule for all updates:

1. Click the **Add** button.

The Rule Creation Wizard starts. Proceed through the Wizard by using the Next button.

2. On the **Rule type** page, select **Rule for all updates**.
3. On the **General criteria** page, use the drop-down lists to specify the following settings:

- Set of updates to install

Select the updates that must be installed on client devices:

- **Install approved updates only.** This installs only approved updates.
- **Install all updates (except declined).** This installs updates with the *Approved* or *Undefined* approval status.
- **Install all updates (including declined).** This installs all updates, regardless of their approval status. Select this option with caution. For example, use this option if you

want to check installation of some declined updates in a test infrastructure.

- **Fix vulnerabilities with a severity level equal to or higher than**

Sometimes software updates may impair the user experience with the software. In such cases, you may decide to install only those updates that are critical for the software operation and to skip other updates.

If this option is enabled, the updates fix only those vulnerabilities for which the severity level set by Kaspersky is equal to or higher than the value selected in the list (**Medium**, **High**, or **Critical**). Vulnerabilities with a severity level lower than the selected value are not fixed.

If this option is disabled, the updates fix all vulnerabilities regardless of their severity level.

By default, this option is disabled.

1. On the **Updates** page, select the updates to be installed:

- **Install all suitable updates**

Install all software updates that meet the criteria specified on the **General criteria** page of the Wizard. Selected by default.

- **Install only updates from the list**

Install only software updates that you select manually from the list. This list contains all available software updates.

For example, you may want to select specific updates in the following cases: to check their installation in a test environment, to update only critical applications, or to update only specific applications.

- **Automatically install all previous application updates that are required to install the selected updates**

Keep this option enabled if you agree with the installation of interim application versions when this is required for installing the selected updates.

If this option is disabled, only the selected versions of applications are installed. Disable this option if you want to update applications in a straightforward manner, without attempting to install successive versions incrementally. If installing the selected updates is not possible without installing previous versions of applications, the updating of the application fails.

For example, you have version 3 of an application installed on a device and you want to update it to version 5, but version 5 of this application can be installed only over version 4. If this option is enabled, the software first installs version 4, and then installs version 5. If this option is disabled, the software fails to update the application.

By default, this option is enabled.

1. On the **Vulnerabilities** page, select vulnerabilities that will be fixed by installing the selected updates:

- **Fix all vulnerabilities that match other criteria**

Fix all vulnerabilities that meet the criteria specified on the **General criteria** page of the Wizard. Selected by default.

- **Fix only vulnerabilities from the list**

Fix only vulnerabilities that you select manually from the list. This list contains all detected vulnerabilities.

For example, you may want to select specific vulnerabilities in the following cases: to check their fix in a test environment, to fix vulnerabilities only in critical applications, or to fix vulnerabilities only in specific applications.

1. On the **Name** page, specify the name for the rule that you are adding. You can later change this name in the **Settings** section of the properties window of the created task.

After the Rule Creation Wizard completes its operation, the new rule is added and displayed in the rule list in the New Task Wizard or in the task properties.

► To add a new rule for Windows Update updates:

1. Click the **Add** button.

The Rule Creation Wizard starts. Proceed through the Wizard by using the Next button.

2. On the **Rule type** page, select **Rule for Windows Update**.
3. On the **General criteria** page, specify the following settings:

- Set of updates to install

Select the updates that must be installed on client devices:

- **Install approved updates only.** This installs only approved updates.
- **Install all updates (except declined).** This installs updates with the *Approved* or *Undefined* approval status.
- **Install all updates (including declined).** This installs all updates, regardless of their approval status. Select this option with caution. For example, use this option if you want to check installation of some declined updates in a test infrastructure.

- **Fix vulnerabilities with a severity level equal to or higher than**

Sometimes software updates may impair the user experience with the software. In such cases, you may decide to install only those updates that are critical for the software operation and to skip other updates.

If this option is enabled, the updates fix only those vulnerabilities for which the severity level set by Kaspersky is equal to or higher than the value selected in the list (**Medium**, **High**, or **Critical**). Vulnerabilities with a severity level lower than the selected value are not fixed.

If this option is disabled, the updates fix all vulnerabilities regardless of their severity level.

By default, this option is disabled.

- **Fix vulnerabilities with an MSRC severity level equal to or higher than**

Sometimes, software updates may impair the user experience with the software. In such cases, you may decide to install only those updates that are critical for the software operation and to skip other updates.

If this option is enabled, the updates fix only those vulnerabilities for which the severity level set by Microsoft Security Response Center (MSRC) is equal to or higher than the value selected in the list (**Low**, **Medium**, **High**, or **Critical**). Vulnerabilities with a severity level lower than the selected value are not fixed.

If this option is disabled, the updates fix all vulnerabilities regardless of their severity level.

By default, this option is disabled.

1. On the **Applications** page, select the applications and application versions for which you want to install updates. By default, all applications are selected.
2. On the **Categories of updates** page, select the categories of updates to be installed. These categories are the same as in Microsoft Update Catalog. By default, all categories are selected.

3. On the **Name** page, specify the name for the rule that you are adding. You can later change this name in the **Settings** section of the properties window of the created task.

After the Rule Creation Wizard completes its operation, the new rule is added and displayed in the rule list in the New Task Wizard or in the task properties.

► To add a new rule for updates of third-party applications:

1. Click the **Add** button.

The Rule Creation Wizard starts. Proceed through the Wizard by using the Next button.

2. On the **Rule type** page, select **Rule for third-party updates**.
3. On the **General criteria** page, specify the following settings:

- Set of updates to install

Select the updates that must be installed on client devices:

- **Install approved updates only**. This installs only approved updates.
- **Install all updates (except declined)**. This installs updates with the *Approved* or *Undefined* approval status.
- **Install all updates (including declined)**. This installs all updates, regardless of their approval status. Select this option with caution. For example, use this option if you want to check installation of some declined updates in a test infrastructure.

- **Fix vulnerabilities with a severity level equal to or higher than**

Sometimes software updates may impair the user experience with the software. In such cases, you may decide to install only those updates that are critical for the software operation and to skip other updates.

If this option is enabled, the updates fix only those vulnerabilities for which the severity level set by Kaspersky is equal to or higher than the value selected in the list (**Medium**, **High**, or **Critical**). Vulnerabilities with a severity level lower than the selected value are not fixed.

If this option is disabled, the updates fix all vulnerabilities regardless of their severity level.

By default, this option is disabled.

1. On the **Applications** page, select the applications and application versions for which you want to install updates. By default, all applications are selected.
2. On the **Name** page, specify the name for the rule that you are adding. You can later change this name in the Settings section of the properties window of the created task.

After the Rule Creation Wizard completes its operation, the new rule is added and displayed in the rule list in the New Task Wizard or in the task properties.

Selecting user fixes for vulnerabilities in third-party software

To use the *Fix vulnerabilities* task, you must manually specify the software updates to fix the vulnerabilities in third-party software listed in the task settings. The *Fix vulnerabilities* task uses recommended fixes for Microsoft software and user fixes for other third-party software. *User fixes* are software updates to fix vulnerabilities that the administrator manually specifies for installation.

► *To select user fixes for vulnerabilities in third-party software:*

1. On the **OPERATIONS** tab, in the **PATCH MANAGEMENT** drop-down list, select **Software vulnerabilities**.
The page displays the list of software vulnerabilities detected on client devices.
2. In the list of software vulnerabilities, click the link with the name of the software vulnerability for which you want to specify a user fix.
The properties window of the vulnerability opens.
3. In the left pane, select the **User fixes and other fixes** section.
The list of user fixes for the selected software vulnerability is displayed.
4. Click **Add**.
The list of available installation packages is displayed. The list of displayed installation packages corresponds to the **OPERATIONS** → **REPOSITORIES** → **INSTALLATION PACKAGES** list. If you have not created an installation package containing a user fix for selected vulnerability, you can create the package now by starting the New Package Wizard.
5. Select an installation package (or packages) containing a user fix (or user fixes) for the vulnerability in third-party software.
6. Click **Save**.

The installation packages containing user fixes for the software vulnerability are specified. When the *Fix vulnerabilities* task is started, the installation package will be installed, and the software vulnerability will be fixed.


Viewing information about software vulnerabilities detected on all managed devices

After you have scanned software on managed devices for vulnerabilities (see section "Creating the Find vulnerabilities and required updates task" on page [1216](#)), you can view the list of software vulnerabilities detected on all managed devices.

► *To view the list of software vulnerabilities detected on all managed devices,*

On the **OPERATIONS** tab, in the **PATCH MANAGEMENT** drop-down list, select **Software vulnerabilities**.
The page displays the list of software vulnerabilities detected on client devices.

You can also generate and view Report on vulnerabilities (see section "Generating and viewing a report" on page [1287](#)).

You can specify a filter to view the list of software vulnerabilities. Click the **Filter** icon () in the upper right corner of the software vulnerabilities list to manage the filter. You can also select one of preset filters from the **Preset filters** drop-down list above the software vulnerabilities list.

You can obtain detailed information about any vulnerability from the list.

► *To obtain information about a software vulnerability:*

In the list of software vulnerabilities, click the link with the name of the vulnerability.
The properties window of the software vulnerability opens.

Viewing information about software vulnerabilities detected on the selected managed device

You can view information about software vulnerabilities detected on the selected managed device running Windows.

► *To view a list of software vulnerabilities detected on the selected managed device:*

1. Select **DEVICES** → **MANAGED DEVICES**.

The list of managed devices is displayed.

2. In the list of managed devices, click the link with the name of the device for which you want to view detected software vulnerabilities.

The properties window of the selected device is displayed.

3. In the properties window of the selected device, select the **Advanced** tab.

4. In the left pane of the page, select the **Software vulnerabilities** section.

If you want to view only software vulnerabilities that can be fixed, select the **Show only vulnerabilities that can be fixed** option.

The list of software vulnerabilities detected on the selected managed device is displayed.

► *To view the properties of the selected software vulnerability,*

Click the link with the name of the software vulnerability in the list of software vulnerabilities.

The properties window of the selected software vulnerability is displayed.

Viewing statistics of vulnerabilities on managed devices

You can view statistics for each software vulnerability on managed devices. Statistics is represented as a diagram. The diagram displays the number of devices with the following statuses:

- *Ignored on: <number of devices>*. The status is assigned if, in the vulnerability properties, you have manually set the option to ignore the vulnerability.
- *Fixed on: <number of devices>*. The status is assigned if the task to fix the vulnerability has successfully completed.
- *Fix scheduled on: <number of devices>*. The status is assigned if you have created the task to fix the vulnerability but the task is not performed yet.
- *Patch applied on: <number of devices>*. The status is assigned if you have manually selected a software update to fix the vulnerability but this software updated has not fixed the vulnerability.
- *Fix required on: <number of devices>*. The status is assigned if the vulnerability was fixed only on the part of managed devices, and it is required to be fixed on the rest part of managed devices.

► *To view the statistics of a vulnerability on managed devices:*

1. On the **OPERATIONS** tab, in the **PATCH MANAGEMENT** drop-down list, select **Software vulnerabilities**.

The page displays a list of vulnerabilities in applications detected on managed devices.

2. Select the check box next to the required vulnerability.

3. Click the **Statistics of vulnerability on devices** button.

A diagram of the vulnerability statuses is displayed. Clicking a status opens a list of devices on which the vulnerability has the selected status.

Exporting the list of software vulnerabilities to a file

You can export the displayed list of vulnerabilities to the CSV or TXT files. You can use these files, for example, to send them to your information security manager or to store them for purposes of statistics.

► *To export the list of software vulnerabilities detected on all managed devices to a text file:*

1. On the **OPERATIONS** tab, in the **PATCH MANAGEMENT** drop-down list, select **Software vulnerabilities**.
The page displays a list of vulnerabilities in software detected on managed devices.
2. Click the **Export rows to TXT file** or **Export rows to CSV file** button, depending on the format prefer for export.

The file containing the list of software vulnerabilities is downloaded to the device that you use at the moment.

► *To export the list of software vulnerabilities detected on selected managed device to a text file:*

1. Open the list of software vulnerabilities detected on selected managed device (see section "Viewing information about software vulnerabilities detected on the selected managed device" on page [1255](#)).
2. Select the software vulnerabilities you want to export.

Skip this step if you want to export a complete list of software vulnerabilities detected on the managed device.

If you want to export complete list of software vulnerabilities detected on the managed device, only vulnerabilities displaying on the current page will be exported.

3. Click the **Export rows to TXT file** or the **Export rows to CSV file** button, depending on the format you prefer for export.

The file containing the list of software vulnerabilities detected on the selected managed device is downloaded to the device you are using at the moment.

Ignoring software vulnerabilities

You can ignore software vulnerabilities to be fixed. The reasons to ignore software vulnerabilities might be, for example, the following:

- You do not consider the software vulnerability critical to your organization.
- You understand that the software vulnerability fix can damage data related to the software that required the vulnerability fix.
- You are sure that the software vulnerability is not dangerous for your organization's network because you use other measures to protect your managed devices.

You can ignore a software vulnerability on all managed devices or only on selected managed devices.

► *To ignore a software vulnerability on all managed devices:*

1. On the **OPERATIONS** tab, in the **PATCH MANAGEMENT** drop-down list, select **Software vulnerabilities**.

The page displays the list of software vulnerabilities detected on managed devices.

2. In the list of software vulnerabilities, click the link with the name of the software vulnerability you want to ignore.

The properties window of the vulnerability opens.

3. On the **General** tab, enable the **Ignore vulnerability** option.

4. Click the **Save** button.

The software vulnerability properties window is closed.

The software vulnerability is ignored on all managed devices.

► *To ignore a software vulnerability on the selected managed device:*

1. On the **DEVICES** tab, select the **MANAGED DEVICES** tab.

The list of managed devices is displayed.

2. In the list of managed devices, click the link with the name of the device on which you want to ignore a software vulnerability.

The device properties window is opened.

3. In the device properties window, select the **Advanced** tab.

4. In the left pane, select the **Software vulnerabilities** section.

The list of software vulnerabilities detected on the device is displayed.

5. In the list of software vulnerabilities, select the vulnerability you want to ignore on the selected device.

The software vulnerability properties window is opened.

6. In the software vulnerability properties window, on the **General** tab, enable the **Ignore vulnerability** option.

7. Click the **Save** button.

The software vulnerability properties window is closed.

8. Close the device properties window.

The software vulnerability is ignored on the selected device.

The ignored software vulnerability will not be fixed after completion of the *Fix vulnerabilities* task or *Install required updates and fix vulnerabilities* task. You can exclude ignored software vulnerabilities from the list of vulnerabilities by means of the filter.

Managing applications run on client devices

This section describes the features of Kaspersky Security Center related to the management of applications run on client devices.

In this section

Scenario: Application Management.....	1258
About Application Control	1260
Obtaining and viewing a list of applications installed on client devices.....	1261
Obtaining and viewing a list of executable files stored on client devices	1261
Creating application category with content added manually	1262
Creating application category that includes executable files from selected devices.....	1265
Creating application category that includes executable files from selected folder	1267
Viewing the list of application categories.....	1269
Configuring Application Control in the Kaspersky Endpoint Security for Windows policy.....	1269
Adding event-related executable files to the application category	1270

Scenario: Application Management

You can manage applications startup on user devices. You can allow or block applications to be run on managed devices. This functionality is realized by the Application Control component. You can manage applications installed only on Windows devices.

Prerequisites

- Kaspersky Security Center is deployed in your organization.
- Among managed devices in your organization, there are devices running Windows.
- Kaspersky Endpoint Security for Windows policy is created and is active.

Stages

The Application Control usage scenario proceeds in stages:

a. Forming and viewing the list of applications on client devices

This stage helps you find out what applications are installed on managed devices. You can view the list of applications and decide which applications you want to allow and which you want to prohibit, according to your organization's security policies. The restrictions can be related to the information security policies in your organization. You can skip this stage if you know exactly what applications are installed on managed devices.

How-to instructions:

Administration Console: Viewing application registry (see section "Viewing the applications registry" on page [496](#))

Kaspersky Security Center 13 Web Console: Obtaining and viewing a list of applications installed on client devices (on page [1261](#))

b. Forming and viewing the list of executable files on client devices

This stage helps you find out what executable files are found on managed devices. View the list of executable files and compare it with the lists of allowed and prohibited executable files. The restrictions on

executable files usage can be related to the information security policies in your organization. You can skip this stage if you know exactly what executable files are installed on managed devices.

How-to instructions:

Administration Console: Inventory of executable files (on page [500](#))

Kaspersky Security Center 13 Web Console: Obtaining and viewing a list of executable files stored on client devices (on page [1261](#))

c. Creating application categories for the applications used in your organization

Analyze the lists of applications and executable files stored on managed devices. Basing on the analysis, create application categories. It is recommended to create a "Work applications" category that covers the standard set of applications that are used at your organization. If different user groups use different sets of applications in their work, a separate application category can be created for each user group.

Depending on the set of criteria to create an application category, you can create application categories of three types.

How-to instructions:

Administration Console: Creating application categories for Kaspersky Endpoint Security for Windows policies (on page [487](#)), Creating an application category with content added manually (on page [489](#)), Creating an application category with content added automatically (on page [491](#))

Kaspersky Security Center 13 Web Console: Creating application category with content added manually (on page [1262](#)), Creating application category that includes executable files from selected devices (on page [1265](#)), Creating application category that includes executable files from selected folder (on page [1267](#))

d. Configuring Application Control in the Kaspersky Endpoint Security for Windows policy

Configure the Application Control component in Kaspersky Endpoint Security for Windows policy using the application categories you have created on the previous stage.

How-to instructions:

Administration Console: Configuring application startup management on client devices (on page [494](#))

Kaspersky Security Center 13 Web Console: Configuring Application Control in the Kaspersky Endpoint Security for Windows policy (on page [1269](#))

e. Turning on Application Control component in test mode

To ensure that Application Control rules do not block applications required for user's work, it is recommended to enable testing of Application Control rules and analyze their operation after creating new rules. When testing is enabled, Kaspersky Endpoint Security for Windows will not block applications whose startup is forbidden by Application Control rules, but will instead send notifications about their startup to the Administration Server.

When testing Application Control rules, it is recommended to perform the following actions:

Determine the testing period. Testing period can vary from several days to two months.

Examine the events resulting from testing the operation of Application Control.

How-to instructions:

Kaspersky Security Center 13 Web Console: Configuring Application Control component in the Kaspersky Endpoint Security for Windows policy (see section "Configuring Application Control in the Kaspersky Endpoint Security for Windows policy" on page [1269](#)). Follow this instruction and enable **Test Mode** option in configuration process.

f. Changing the application categories settings of Application Control component

If necessary, make changes to the Application Control settings. Based on the test results, you can add executable files related to events of the Application Control component to an application category with content added manually.

How-to instructions:

Administration Console: Adding event-related executable files to the application category (on page [493](#))

Kaspersky Security Center 13 Web Console: Adding event-related executable files to the application category (on page [1270](#))

g. Applying the rules of Application Control in operation mode

After Application Control rules are tested and configuration of application categories is complete, you can apply the rules of Application Control in operation mode.

How-to instructions:

Kaspersky Security Center 13 Web Console: Configuring Application Control component in the Kaspersky Endpoint Security for Windows policy (see section "Configuring Application Control in the Kaspersky Endpoint Security for Windows policy" on page [1269](#)). Follow this instruction and disable **Test Mode** option in configuration process.

h. Verifying Application Control configuration

Be sure that you have done the following:

Created application categories.

Configured Application Control using the application categories.

Applied the rules of Application Control in operation mode.

Results

When the scenario is complete, applications startup on managed devices is controlled. The users can start only those applications that are allowed in your organization and cannot start applications that are prohibited in your organization.

For detailed information about Application Control, refer to Kaspersky Endpoint Security for Windows Online Help <https://support.kaspersky.com/KESWin/11.6.0/en-US/127971.htm> and to the Kaspersky Security for Virtualization Light Agent <https://help.kaspersky.com/KSVLA/5.1/en-US/145134.htm>.

About Application Control

The Application Control component monitors users' attempts to start applications and regulates the startup of applications by using Application Control rules.

Application Control component is available for Kaspersky Endpoint Security for Windows and for Kaspersky Security for Virtualization Light Agent. All the instructions in this section describe configuration of Application Control for Kaspersky Endpoint Security for Windows.

Startup of applications whose settings do not match any of the Application Control rules is regulated by the selected operating mode of the component:

- *Denylist*. The mode is used if you want to allow the startup of all applications except the applications specified in block rules. This mode is selected by default.
- *Allowlist*. The mode is used if you want to block the startup of all applications except the applications specified in allow rules.

The Application Control rules are implemented through application categories. You create application categories defining specific criteria. In Kaspersky Security Center there are three types of application categories:

- Category with content added manually (see section "Creating application category with content added manually" on page [1262](#)). You define conditions, for example, file metadata, file hashcode, file certificate, KL category, file path, to include executable files in the category.
- Category which includes executable files from selected devices (see section "Creating application category that includes executable files from selected devices" on page [1265](#)). You specify a device whose executable files are automatically included in the category.

- Category that includes executable files from selected folder (see section "Creating application category that includes executable files from selected folder" on page [1267](#)). You specify a folder from which executable files are automatically included in the category.

For detailed information about Application Control, refer to Kaspersky Endpoint Security for Windows Online Help <https://support.kaspersky.com/KESWin/11.6.0/en-US/127971.htm> and to the Kaspersky Security for Virtualization Light Agent <https://help.kaspersky.com/KSVLA/5.1/en-US/145134.htm>.

Obtaining and viewing a list of applications installed on client devices

Kaspersky Security Center inventories all software installed on managed client devices running Windows.

Network Agent compiles a list of applications installed on a device and then transmits this list to Administration Server. Network Agent automatically receives information about installed applications from the Windows registry.

To save the device resources, Network Agent by default starts receiving information about installed applications 10 minutes after the Network Agent service starts.

► *To view the list of applications installed on managed devices:*

In the **OPERATIONS** → **THIRD-PARTY APPLICATIONS** drop-down list, select **Applications registry**.

The page displays the list of applications installed on managed devices.

For detailed information about Application Control, refer to Kaspersky Endpoint Security for Windows Online Help <https://support.kaspersky.com/KESWin/11.6.0/en-US/127971.htm> and to the Kaspersky Security for Virtualization Light Agent <https://help.kaspersky.com/KSVLA/5.1/en-US/145134.htm>.

See also:

Scenario: Application Management.....[1258](#)

Obtaining and viewing a list of executable files stored on client devices

You can obtain a list of executable files stored on managed devices. To inventory executable files, you must create an inventory task.

The feature of inventorying executable files is available for Kaspersky Endpoint Security 10 for Windows and later versions, and for Kaspersky Security for Virtualization 4.0 Light Agent and later versions.

► *To create an inventory task for executable files on client devices:*

1. Go to **DEVICES** → **TASKS**.

The list of tasks is displayed.

2. Click the **Add** button.

The New Task Wizard (see section "Creating a task" on page [1080](#)) starts. Proceed through the Wizard by using the **Next** button.

3. On the **New task** page, from the **Application** drop-down list, select Kaspersky Endpoint Security for Windows.
4. From the **Task type** drop-down list, select **Inventory**.
5. On the **Finish task creation** page, click the **Finish** button.

After the New Task Wizard has finished, the **Inventory** task is created and configured. If you want, you can change the settings for the created task. The newly created task is displayed in the list of tasks.

For a detailed description of the inventory task, please refer to Kaspersky Endpoint Security for Windows Online Help <https://support.kaspersky.com/KESWin/11.6.0/en-US/127971.htm> and Kaspersky Security for Virtualization Light Agent <https://help.kaspersky.com/KSVLA/5.1/en-US/145134.htm>.

After the **Inventory** task is performed, the list of executable files stored on managed devices is formed, and you can view the list.

During inventory, executable files in the following formats are detected: MZ, COM, PE, NE, SYS, CMD, BAT, PS1, JS, VBS, REG, MSI, CPL, DLL, JAR, and HTML.

► *To view the list of executable files stored on client devices:*

In the **OPERATIONS** → **THIRD-PARTY APPLICATIONS** drop-down list, select **EXECUTABLE FILES**.

The page displays the list of executable files stored on client devices.

See also:

Scenario: Application Management [1258](#)

Creating application category with content added manually

You can specify a set of criteria as a template of executable files for which you want to allow or block a start in your organization. On the basis of executable files corresponding to the criteria, you can create an application category and use it in the Application Control component configuration.

► *To create an application category with content added manually:*

1. In the **OPERATIONS** → **THIRD-PARTY APPLICATIONS** drop-down list, select **APPLICATION CATEGORIES**.

The page with a list of application categories is displayed.

2. Click the **Add** button.

The New Category Wizard starts. Proceed through the Wizard by using the **Next** button.

3. On the **Select category creation method** page of the Wizard, select the **Category with content added manually. Data of executable files is manually added to the category** option.
4. On the **Conditions** page of the Wizard, click the **Add** button to add a condition criterion to include files in the creating category.
5. On the **Condition criteria** page, select a rule type for the creation of category from the list:

- **From KL category**

If this option is selected, you can specify a Kaspersky application category as the condition of adding applications to the user category. The applications from the specified Kaspersky category will be added to the user application category.

- **Select certificate from repository**

If this option is selected, you can specify certificates from the storage. Executable files that have been signed in accordance with the specified certificates will be added to the user category.

- **Specify path to application (masks supported)**

If this option is selected, you can specify the path to the folder on the client device containing the executable files that are to be added to the user application category.

- **Removable drive**

If this option is selected, you can specify the type of the medium (any drive or removable drive) on which the application is run. Applications that have been run on the selected drive type are added to the user application category.

- Hash, metadata, or certificate:

- **Select from list of executable files**

If this option is selected, you can use the list of executable files on the client device to select and add applications to the category.

- **Select from applications registry**

If this option is selected, application registry is displayed. You can select an application from the registry and specify the following file metadata:

- File name.
- File version. You can specify precise value of the version or describe a condition, for example "greater than 5.0".
- Application name.
- Application version. You can specify precise value of the version or describe a condition, for example "greater than 5.0".
- Vendor.

- **Specify manually**

If this option is selected, you must specify file hash, or metadata, or certificate as the condition of adding applications to the user category.

File Hash

Depending on the version of the security application installed on devices on your network, you must select an algorithm for hash value computing by Kaspersky Security Center for files in this category. Information about computed hash values is stored in the Administration Server database. Storage of hash values does not increase the database size significantly.

SHA-256 is a cryptographic hash function: no vulnerabilities have been found in its algorithm, and so it is considered the most reliable cryptographic function nowadays. Kaspersky Endpoint Security 10 Service Pack 2 for Windows and later versions support SHA-256 computing. Computing of the MD5 hash function is supported by all versions

earlier than Kaspersky Endpoint Security 10 Service Pack 2 for Windows.

Select either of the options of hash value computing by Kaspersky Security Center for files in the category:

- If all instances of security applications installed on your network are Kaspersky Endpoint Security 10 Service Pack 2 for Windows or later versions, select the **Calculate SHA-256 for files in this category (supported by Kaspersky Endpoint Security 10 Service Pack 2 for Windows and any later versions)** check box. We do not recommend that you add any categories created according to the criterion of the SHA-256 hash of an executable file for versions earlier than Kaspersky Endpoint Security 10 Service Pack 2 for Windows. This may result in failures in the security application operation. In this case, you can use the MD5 cryptographic hash function for files of the category.
- If any versions earlier than Kaspersky Endpoint Security 10 Service Pack 2 for Windows are installed on your network, select the **Calculate MD5 for files in this category (supported by versions earlier than Kaspersky Endpoint Security 10 Service Pack 2 for Windows)**. You cannot add a category that was created based on the criterion of the MD5 hash sum of an executable file for Kaspersky Endpoint Security 10 Service Pack 2 for Windows or later versions. In this case, you can use the SHA-256 cryptographic hash function for files of the category.
- If different devices on your network use both earlier and later versions of Kaspersky Endpoint Security 10, select both the **Calculate SHA-256 for files in this category** check box and the **Calculate MD5 for files in this category** check box.

Metadata

If this option is selected, you can specify file metadata as file name, file version, vendor. The metadata will be sent to Administration Server. Executable files that contain the same metadata will be added to the application category.

Certificate

If this option is selected, you can specify certificates from the storage. Executable files that have been signed in accordance with the specified certificates will be added to the user category.

- **From file or from MSI package / archived folder**

If this option is selected, you can specify an MSI installer file as the condition of adding applications to the user category. The application installer metadata will be sent to Administration Server. The applications for which the installer metadata is the same as for the specified MSI installer are added to the user application category.

The selected criterion is added to the list of conditions.

You can add as many criteria for the creating application category as you need.

1. On the **Exclusions** page of the Wizard, click the **Add** button to add an exclusive condition criterion to exclude files from the category that is being created.
2. On the **Condition criteria** page, select a rule type from the list, in the same way that you selected a rule type for category creation.

When the Wizard finishes, the application category is created. The created application category is displayed in the list of application categories. You can use the created application category when you configure Application Control.

For detailed information about Application Control, refer to Kaspersky Endpoint Security for Windows Online Help <https://support.kaspersky.com/KESWin/11.6.0/en-US/127971.htm> and to the Kaspersky Security for Virtualization Light Agent <https://help.kaspersky.com/KSVLA/5.1/en-US/145134.htm>.

See also:

Scenario: Application Management.....[1258](#)

Creating application category that includes executable files from selected devices

You can use executable files from selected devices as a template of executable files that you want to allow or block. Based on executable files from selected devices, you can create an application category and use it in the Application Control component configuration.

► *To create application category that includes executable files from selected devices:*

1. In the **OPERATIONS** → **THIRD-PARTY APPLICATIONS** drop-down list, select **APPLICATION CATEGORIES**.

The page with a list of application categories is displayed.

2. Click the **Add** button.

The New Category Wizard starts. Proceed through the Wizard by using the Next button.

3. On the **Select category creation method** page of the Wizard, specify the category name and select the **Category that includes executable files from selected devices. These executable files are processed automatically and their metrics are added to the category** option.

4. Click **Add**.

5. In the window that opens, select a device or devices whose executable files will be used to create the application category.

6. Specify the following settings:

- Hash value computing algorithm:

Depending on the version of the security application installed on devices on your network, you must select an algorithm for hash value computing by Kaspersky Security Center for files in this category. Information about computed hash values is stored in the Administration Server database. Storage of hash values does not increase the database size significantly.

SHA-256 is a cryptographic hash function: no vulnerabilities have been found in its algorithm, and so it is considered the most reliable cryptographic function nowadays. Kaspersky Endpoint Security 10 Service Pack 2 for Windows and later versions support SHA-256 computing. Computing of the MD5 hash function is supported by all versions earlier than Kaspersky Endpoint Security 10 Service Pack 2 for Windows.

Select either of the options of hash value computing by Kaspersky Security Center for files in the category:

- If all instances of security applications installed on your network are Kaspersky Endpoint Security 10 Service Pack 2 for Windows or later versions, select the **Calculate SHA-256 for files in this category (supported by Kaspersky Endpoint Security 10 Service Pack 2 for Windows and any later versions)** check box. We do not recommend that you add any categories created according to the criterion of the SHA-256 hash of an executable file for versions earlier than Kaspersky Endpoint Security 10 Service Pack 2 for Windows. This may result in failures in the security application operation. In this case, you can use the MD5 cryptographic hash function

for files of the category.

- If any versions earlier than Kaspersky Endpoint Security 10 Service Pack 2 for Windows are installed on your network, select the **Calculate MD5 for files in this category (supported by versions earlier than Kaspersky Endpoint Security 10 Service Pack 2 for Windows)**. You cannot add a category that was created based on the criterion of the MD5 hash sum of an executable file for Kaspersky Endpoint Security 10 Service Pack 2 for Windows or later versions. In this case, you can use the SHA-256 cryptographic hash function for files of the category.

If different devices on your network use both earlier and later versions of Kaspersky Endpoint Security 10, select both the **Calculate SHA-256 for files in this category** check box and the **Calculate MD5 for files in this category** check box.

The **Calculate SHA-256 for files in this category (supported by Kaspersky Endpoint Security 10 Service Pack 2 for Windows and any later versions)** check box is selected by default.

The **Calculate MD5 for files in this category (supported by versions earlier than Kaspersky Endpoint Security 10 Service Pack 2 for Windows)** is cleared by default.

- **Calculate SHA-256 for files in this category (supported by Kaspersky Endpoint Security 10 Service Pack 2 for Windows and later versions)**
- **Calculate MD5 for files in this category (supported by versions earlier than Kaspersky Endpoint Security 10 Service Pack 2 for Windows)**
- **Synchronize data with Administration Server repository**

Select this option if you want that Administration Server periodically to check changes in the specified folder (or folders).

By default, this option is disabled.

If you enable this option, specify the period (in hours) to check changes in the specified folder (folders). By default, scan interval is 24 hours.

- **File type**

In this section, you can specify file type that is used to create the application category.

All files. All files are taken into consideration when creating the category. By default, this option is selected.

Only files outside the application categories. Only files outside the application categories are taken into consideration when creating the category.

- **Folders**

In this section you can specify which folders from the selected device (devices) contain files that are used to create the application category.

All folders. All folders are taken into consideration for the creating category. By default, this option is selected.

Specified folder. Only specified folder is taken into consideration for the creating category. If you select this option you must specify path to the folder.

When the Wizard finishes, the application category is created. The created application category is displayed in the list of application categories. You can use the created application category when you configure Application Control.

See also:

Scenario: Application Management [1258](#)

Creating application category that includes executable files from selected folder

You can use executable files from a selected folder as a standard of executable files that you want to allow or block in your organization. On the basis of executable files from the selected folder, you can create an application category and use it in the Application Control component configuration.

► *To create an application category that includes executable files from the selected folder:*

1. In the **OPERATIONS** → **THIRD-PARTY APPLICATIONS** drop-down list, select **APPLICATION CATEGORIES**.

The page with a list of application categories is displayed.

2. Click the **Add** button.

The New Category Wizard starts. Proceed through the Wizard by using the Next button.

3. On the **Select category creation method** page of the Wizard, specify category name and select the **Category that includes executable files from a specific folder. Executable files of applications copied to the specified folder are automatically processed and their metrics are added to the category** option.

4. Specify the folder whose executable files will be used to create the application category.

5. Configure the following settings:

- **Include dynamic-link libraries (DLL) in this category**

The application category includes dynamic-link libraries (files in DLL format), and the Application Control component logs the actions of such libraries running in the system. Including DLL files in the category may lower the performance of Kaspersky Security Center.

By default, this check box is cleared.

- **Include script data in this category**

The application category includes data on scripts, and scripts are not blocked by Web Threat Protection. Including the script data in the category may lower the performance of Kaspersky Security Center.

By default, this check box is cleared.

- Hash value computing algorithm: **Calculate SHA-256 for files in this category (supported by Kaspersky Endpoint Security 10 Service Pack 2 for Windows and later versions) / Calculate MD5 for files in this category (supported by versions earlier than Kaspersky Endpoint Security 10 Service Pack 2 for Windows)**

Depending on the version of the security application installed on devices on your network, you must select an algorithm for hash value computing by Kaspersky Security Center for files in this category. Information about computed hash values is stored in the Administration Server database. Storage of hash values does not increase the database size significantly.

SHA-256 is a cryptographic hash function: no vulnerabilities have been found in its algorithm, and so it is considered the most reliable cryptographic function nowadays. Kaspersky Endpoint Security 10 Service Pack 2 for Windows and later versions support SHA-256 computing. Computing of the MD5 hash function is supported by all versions earlier than Kaspersky Endpoint Security 10 Service Pack 2 for Windows.

Select either of the options of hash value computing by Kaspersky Security Center for files in the category:

- If all instances of security applications installed on your network are Kaspersky Endpoint Security 10 Service Pack 2 for Windows or later versions, select the **Calculate SHA-256 for files in this category (supported by Kaspersky Endpoint Security 10 Service Pack 2 for Windows and any later versions)** check box. We do not recommend that you add any categories created according to the criterion of the SHA-256 hash of an executable file for versions earlier than Kaspersky Endpoint Security 10 Service Pack 2 for Windows. This may result in failures in the security application operation. In this case, you can use the MD5 cryptographic hash function for files of the category.
- If any versions earlier than Kaspersky Endpoint Security 10 Service Pack 2 for Windows are installed on your network, select the **Calculate MD5 for files in this category (supported by versions earlier than Kaspersky Endpoint Security 10 Service Pack 2 for Windows)**. You cannot add a category that was created based on the criterion of the MD5 hash sum of an executable file for Kaspersky Endpoint Security 10 Service Pack 2 for Windows or later versions. In this case, you can use the SHA-256 cryptographic hash function for files of the category.

If different devices on your network use both earlier and later versions of Kaspersky Endpoint Security 10, select both the **Calculate SHA-256 for files in this category** check box and the **Calculate MD5 for files in this category** check box.

The **Calculate SHA-256 for files in this category (supported by Kaspersky Endpoint Security 10 Service Pack 2 for Windows and any later versions)** check box is selected by default.

The **Calculate MD5 for files in this category (supported by versions earlier than Kaspersky Endpoint Security 10 Service Pack 2 for Windows)** is cleared by default.

- **Force folder scan for changes**

If this check box is selected, the application regularly checks the folder of category content addition for changes. You can specify the frequency of checks (in hours) in the entry field next to the check box. By default, the time interval between forced checks is 24 hours.

If this check box is cleared, the application does not force any checks of the folder. The Server attempts to access files if they have been modified, added, or deleted.

By default, this check box is cleared.

When the Wizard finishes, the application category is created. Created application category is displayed in the list of application categories. You can use the application category at Application Control configuration.

For detailed information about Application Control, refer to Kaspersky Endpoint Security for Windows Online Help <https://support.kaspersky.com/KESWin/11.6.0/en-US/127971.htm> and to the Kaspersky Security for Virtualization Light Agent <https://help.kaspersky.com/KSVLA/5.1/en-US/145134.htm>.

See also:

Scenario: Application Management.....[1258](#)

Viewing the list of application categories

You can view the list of configured application categories and the settings of each application category.

► *To view the list of application categories,*

On the **OPERATIONS** tab, in the **THIRD-PARTY APPLICATIONS** drop-down list, select **APPLICATION CATEGORIES**.

The page with a list of application categories is displayed.

► *To view properties of an application category,*

Click the name of the application category.

The properties window of the application category is displayed. The properties are grouped on several tabs.

Configuring Application Control in the Kaspersky Endpoint Security for Windows policy

After you create Application Control categories, you can use them for configuring Application Control in Kaspersky Endpoint Security for Windows policies.

► *To configure Application Control in Kaspersky Endpoint Security for Windows policy:*

1. Go to **DEVICES** → **POLICIES & PROFILES**.

A page with a list of policies is displayed.

2. Click **Kaspersky Endpoint Security for Windows** policy.

The policy settings window opens.

3. Select the **Application settings** tab, **Security Controls** section, **Application Control** subsection.

The **Application Control** window with Application Control settings is displayed.

4. Switch the toggle button to enable the **Application Control** option.

5. If you want to test Application Control rules, switch the toggle button to enable the **Test Mode** option.

If you want to apply Application Control rules, switch the toggle button to disable the **Test Mode** option.

6. Enable the **Control DLL and drivers** option if you want Kaspersky Endpoint Security for Windows to monitor the loading of DLL modules when applications are started by users.

Information about the module and the application that loaded the module will be saved to a report.

Kaspersky Endpoint Security for Windows monitors only the DLL modules and drivers loaded after the **Control DLL and drivers** option is selected. Restart the computer after selecting the **Control DLL and drivers** option if you want Kaspersky Endpoint Security for Windows to monitor all DLL modules and drivers, including those loaded before Kaspersky Endpoint Security for Windows is started.

7. (Optional) In the **Message templates** block, change the template of the message that is displayed when an application is blocked from starting and the template of the email message that is sent to you.
8. In the **Application Control Mode** block settings, select **Denylist** or **Allowlist** mode.
By default, **Denylist** mode is selected.
9. Click the **Rules Lists Settings** link.
The **Denylists and allowlists** window opens to let you add an application category. By default, the **Denylist** tab is selected if the **Denylist** mode is selected, and the **Allowlist** tab is selected if the **Allowlist** mode is selected.
10. In the **Denylists and allowlists** window, click the **Add** button.
The **Application Control rule** window opens.
11. Click the **Category is not defined** link.
The **Application Category** window opens.
12. Add the application category (or categories) that you created earlier.
You can edit the settings of a created category by clicking the **Edit** button.
You can create a new category by clicking the **Add** button.
You can delete a category from the list by clicking the **Delete** button.
13. After the list of application categories is complete, click the **OK** button.
The **Application Category** window closes.
14. In the **Application Control** rule window, in the **Subjects and their rights** section, create the list of users and groups of users to apply the Application Control rule.
15. Click the **OK** button to save the settings and to close the **Application Control rule** window.
16. Click the **OK** button to save the settings and to close the **Denylists and allowlists** window.
17. Click the **OK** button to save the settings and to close the **Application Control** window.
18. Click the **Close** button (X) to close the window with the Kaspersky Endpoint Security for Windows policy settings.

Application Control is configured. After the policy is propagated to the client devices, the startup of executable files is managed.

For detailed information about Application Control, refer to Kaspersky Endpoint Security for Windows Online Help <https://support.kaspersky.com/KESWin/11.6.0/en-US/127971.htm> and to the Kaspersky Security for Virtualization Light Agent <https://help.kaspersky.com/KSVLA/5.1/en-US/145134.htm>.

See also:

Scenario: Application Management.....[1258](#)

Adding event-related executable files to the application category

After you configure Application Control in the Kaspersky Endpoint Security for Windows policies, the following events will be displayed in the list of events:

- **Application startup prohibited** (*Critical* event). This event is displayed if you have configured Application Control to apply rules.
- **Application startup prohibited in test mode** (*Info* event). This event is displayed if you have configured Application Control to test rules.
- **Application startup blockage message to administrator** (*Warning* event). This event is displayed if you have configured Application Control to apply rules and a user has requested access to the application that is blocked at startup.

It is recommended to create event selections (see section "Creating an event selection" on page [1290](#)) to view events related to Application Control operation.

You can add executable files related to Application Control events to an existing application category or to a new application category. You can add executable files only to an application category with content added manually.

► *To add executable files related to Application Control events to an application category:*

1. Go to **MONITORING & REPORTING** → **EVENT SELECTIONS**.

The list of event selections is displayed.

2. Select the event selection to view events related to Application Control and start this event selection (see section "Viewing a list of an event selection" on page [1291](#)).

If you have not created event selection related to Application Control, you can select and start a predefined selection, for example, **Recent events**.

The list of events is displayed.

3. Select the events whose associated executable files you want to add to the application category, and then click the **Assign to category** button.

The New Category Wizard starts. Proceed through the Wizard by using the **Next** button.

4. On the Wizard page, specify the relevant settings:

- In the **Action on executable file related to the event** section, select one of the following options:
 - **Add to a new application category**

Select this option if you want to create a new application category based on event-related executable files.

By default, this option is selected.

If you have selected this option, specify a new category name.

- **Add to an existing application category**

Select this option if you want to add event-related executable files to an existing application category.

By default, this option is not selected.

If you have selected this option, select the application category with content added manually to which you want to add executable files.

- In the **Rule type** section, select one of the following options:
 - **Rules for adding to inclusions**

- **Rules for adding to exclusions**
- In the **Parameter used as a condition** section, select one of the following options:
 - **Certificate details (or SHA-256 hashes for files without a certificate)**

Files may be signed with a certificate. Multiple files may be signed with the same certificate. For example, different versions of the same application may be signed with the same certificate, or several different applications from the same vendor may be signed with the same certificate. When you select a certificate, several versions of an application or several applications from the same vendor may end up in the category.

Each file has its own unique SHA-256 hash function. When you select an SHA-256 hash function, only one corresponding file, for example, the defined application version, ends up in the category.

Select this option if you want to add to the category rules the certificate details of an executable file (or the SHA-256 hash function for files without a certificate).

By default, this option is selected.
 - **Certificate details (files without a certificate will be skipped)**

Files may be signed with a certificate. Multiple files may be signed with the same certificate. For example, different versions of the same application may be signed with the same certificate, or several different applications from the same vendor may be signed with the same certificate. When you select a certificate, several versions of an application or several applications from the same vendor may end up in the category.

Select this option if you want to add the certificate details of an executable file to the category rules. If the executable file has no certificate, this file will be skipped. No information about this file will be added to the category.
 - **Only SHA-256 (files without a hash will be skipped)**

Each file has its own unique SHA-256 hash function. When you select an SHA-256 hash function, only one corresponding file, for example, the defined application version, ends up in the category.

Select this option if you want to add only the details of the SHA-256 hash function of the executable file.
 - **Only MD5 (discontinued mode, only for Kaspersky Endpoint Security 10 Service Pack 1 version)**

Each file has its own unique MD5 hash function. When you select an MD5 hash function, only one corresponding file, for example, the defined application version, ends up in the category.

Select this option if you want to add only the details of the MD5 hash function of the executable file. Computing of the MD5 hash function is supported by Kaspersky Endpoint Security 10 Service Pack 1 for Windows and all earlier versions.

1. Click **OK**.

When the Wizard finishes, executable files related to the Application Control events are added to the existing application category or to a new application category. You can view settings of the application category that you have modified or created.

For detailed information about Application Control, refer to Kaspersky Endpoint Security for Windows Online Help <https://support.kaspersky.com/KESWin/11.6.0/en-US/127971.htm> and to the Kaspersky Security for Virtualization Light Agent <https://help.kaspersky.com/KSVLA/5.1/en-US/145134.htm>.

See also:

Scenario: Application Management.....[1258](#)

Creating an installation package of a third-party application from the Kaspersky database

The features provided under the Vulnerability and Patch Management license are only available in MMC-based Administration Console, and Kaspersky Security Center 12.2 Web Console or later versions.

Kaspersky Security Center Web Console allows you to perform remote installation of third-party applications by using installation packages (on page [775](#)). Such third-party applications are included in a dedicated Kaspersky database. This database is created automatically when you run the *Download updates to the repository of the Administration Server* task (see section "Creating the task for downloading updates to the repository of the Administration Server" on page [1184](#)) for the first time.

► *To create an installation package of a third-party application from the Kaspersky database:*

1. In Kaspersky Security Center Web Console, open **DISCOVERY & DEPLOYMENT** → **DEPLOYMENT & ASSIGNMENT** → **INSTALLATION PACKAGES**.
2. Click the **Add** button.
3. On the New Package Wizard page that opens, select the **Select an application from the Kaspersky database to create an installation package** option, and then click **Next**.
4. In the list of applications that opens, select the relevant application, and then click **Next**.
5. Select the relevant localization language in the drop-down list, and then click **Next**.

This step is only displayed if the application offers multiple language options.

6. If you are prompted to accept a License Agreement for the installation, on the **End User License Agreement** page that opens, click the link to read the License Agreement on the vendor's website, and then select the **I confirm that I have fully read, understand, and accept the terms and conditions of this End User License Agreement** check box.
7. On the **Name of the new installation package** page that opens, in the **Package name** field, enter the name for the installation package, and then click **Next**.

Wait until the newly created installation package is uploaded to Administration Server. When the New Package Wizard displays the message informing you the package creation process was successful, click **Finish**.

The newly created installation package appears on the list of installation packages. You can select this package when creating or reconfiguring the *Install application remotely* task.

Viewing and modifying the settings of an installation package of a third-party application from the Kaspersky database

The features provided under the Vulnerability and Patch Management license are only available in MMC-based Administration Console, and Kaspersky Security Center 12.2 Web Console or later versions.

If you have previously created any installation packages of third-party applications listed in the Kaspersky database (see section "Creating an installation package of a third-party application from the Kaspersky database" on page [1273](#)), you can subsequently view and modify the settings (see section "Settings of an installation package of a third-party application from the Kaspersky database" on page [1274](#)) of these packages.

Modifying the settings of an installation package of a third-party application from the Kaspersky database is only available under the Vulnerability and Patch Management license.

To view and modify the settings of an installation package of a third-party application from the Kaspersky database:

1. In Kaspersky Security Center Web Console, open **DISCOVERY & DEPLOYMENT** → **DEPLOYMENT & ASSIGNMENT** → **INSTALLATION PACKAGES**.
2. In the list of installation packages that opens, click the name of the relevant package.
3. On the properties page that opens, modify the settings, if necessary.
4. Click the **Save** button.

The settings that you modified are saved.

Settings of an installation package of a third-party application from the Kaspersky database

The settings of an installation package of a third-party application are grouped on the following tabs:

Only a part of the settings listed below are displayed by default so you can add the corresponding columns by clicking the **Filter** button and selecting relevant column names from the list.

- **General** tab:
 - Entry field containing the name of the installation package that can be edited manually
 - **Application**
 - **Version**
 - **Size**
 - **Created**
 - **Path**
- **Installation procedure** tab:

- **Install required general system components**
- Table displaying the update properties and containing the following columns:
 - **Name**
 - **Description**
 - **Source**
 - **Type**
 - **Category**
 - **Importance level according to MSRC**
 - **Importance level**
 - **Patch importance level (for patches intended for Kaspersky applications)**
 - **Article**
 - **Bulletin**
 - **Not assigned for installation (new version)**
 - **To be installed**
 - **Installing**
 - **Installed**
 - **Failed**
 - **Restart is required**
 - **Registered**
 - **Installed in interactive mode**
 - **Revoked**
 - **Update approval status**
 - **Revision**
 - **Update ID**
 - **Application version**
 - **Superseded**
 - **Superseding**
 - **You must accept the terms of the License Agreement**
 - **Description URL**
 - **Application family**
 - **Application**
 - **Localization language**
 - **Not assigned for installation (new version)**
 - **Requires prerequisites installation**
 - **Download mode**

- **Is a patch**
- **Not installed**
- **Settings** tab:
 - Table displaying the installation package settings—with their names, descriptions, and values—used as command-line parameters during installation. If the package provides no such settings, the corresponding message is displayed. You can modify the values of these settings.
- **Revision history** tab displaying the installation package revisions and containing the following columns:
 - **Revision**
 - **Time**
 - **User**
 - **Action**
 - **Description**

Monitoring and reporting

This section describes the monitoring and reporting capabilities of Kaspersky Security Center. These capabilities give you an overview of your infrastructure, protection statuses, and statistics.

After Kaspersky Security Center deployment or during the operation, you can configure the monitoring and reporting features to best suit your needs.

In this chapter

Scenario: Monitoring and reporting	1279
About types of monitoring and reporting.....	1280
Using the dashboard.....	1281
Adding widgets to the dashboard	1281
Hiding a widget from the dashboard.....	1282
Moving a widget on the dashboard.....	1282
Changing the widget size or appearance	1282
Changing widget settings.....	1283
Using reports	1283
Creating a report template	1284
Viewing and editing report template properties	1284
Exporting a report to a file.....	1287
Generating and viewing a report	1287
Creating a report delivery task.....	1288
Deleting report templates.....	1289
Using event selections.....	1289
Creating an event selection	1290
Editing an event selection.....	1290
Viewing a list of an event selection.....	1291
Viewing details of an event.....	1291
Exporting events to a file	1292
Viewing an object history from an event.....	1292
Deleting events	1292
Deleting event selections.....	1292
Using notifications.....	1293
Viewing onscreen notifications	1293
About device statuses.....	1296
Configuring the switching of device statuses	1301
Configuring notification delivery.....	1303
Setting the storage term for an event	1305
Event types	1306
Blocking frequent events	1351
Device selections.....	1353
About Kaspersky announcements.....	1365

Specifying Kaspersky announcements settings	1366
Disabling Kaspersky announcements	1367

Scenario: Monitoring and reporting

This section provides a scenario for configuring the monitoring and reporting feature in Kaspersky Security Center.

Prerequisites

After you deploy Kaspersky Security Center in an organization's network you can start to monitor it and generate reports on its functioning.

Monitoring and reporting in an organization's network proceeds in stages:

a. Configuring the switching of device statuses

Get acquainted with the settings for device statuses depending on specific conditions. By changing these settings (see section "Configuring the switching of device statuses" on page [1301](#)), you can change the number of events with *Critical* or *Warning* importance levels. When configuring the switching of device statuses, be sure of the following:

New settings do not conflict with the information security policies of your organization.

You are able to react to important security events in your organization's network in a timely manner.

b. Configuring notifications about events on client devices

How-to instructions:

Configure notification (by email, by SMS, or by running an executable file) of events on client devices (see section "Configuring notification delivery" on page [1303](#))

c. Changing the response of your security network to the Virus outbreak event

You can change the specific thresholds (on page [611](#)) in the Administration Server properties. You can also create a stricter policy (see section "Activating a policy automatically at the Virus outbreak event" on page [1125](#)) that will be activated or create a task (see section "Creating a task" on page [1080](#)) that will be run at the occurrence of this event.

d. Performing recommended actions for Critical and Warning notifications

How-to instructions:

Perform recommended actions for your organization's network (see section "Viewing onscreen notifications" on page [1293](#))

e. Reviewing the security status of your organization's network

How-to instructions:

Review the Protection status widget (see section "Using the dashboard" on page [1281](#))

Generate and review the Report on protection status (see section "Generating and viewing a report" on page [1287](#))

Generate and review the Report on errors (see section "Generating and viewing a report" on page [1287](#))

f. Locating client devices that are not protected

How-to instructions:

Review the New devices widget (see section "Using the dashboard" on page [1281](#))

Generate and review the Report on protection deployment (see section "Generating and viewing a report" on page [1287](#))

g. Checking protection of client devices

How-to instructions:

Generate and review reports from the Protection status and Threat statistics categories (see section "Generating and viewing a report" on page [1287](#))

Start and review the Critical event selection (see section "Viewing a list of an event selection" on page [1291](#))

h. Evaluating and limiting the event load on the database

Information about events that occur during operation of managed applications is transferred from a client device and registered in the Administration Server database. To reduce the load on the Administration Server, evaluate and limit the maximum number of events that can be stored in the database.

How-to instructions:

Limiting the maximum number of events (see section "Setting the maximum number of events in the event repository" on page [1008](#))

i. Reviewing license information

How-to instructions:

Add the License key usage widget to the dashboard and review it (see section "Using the dashboard" on page [1281](#))

Generate and review the Report on usage of license keys (see section "Generating and viewing a report" on page [1287](#))

Results

Upon completion of the scenario, you are informed about protection of your organization's network and, thus, can plan actions for further protection.

About types of monitoring and reporting

Information on security events in an organization's network is stored in the Administration Server database. Based on the events, Kaspersky Security Center 13 Web Console provides the following types of monitoring and reporting in your organization's network:

- Dashboard
- Reports
- Event selections
- Notifications

Dashboard

The dashboard allows you to monitor security trends on your organization's network by providing you with a graphical display of information.

Reports

The Reports feature allows you to get detailed numerical information about the security of your organization's network, save this information to a file, send it by email, and print it.

Event selections

Event selections provide an onscreen view of named sets of events that are selected from the Administration Server database. These sets of events are grouped according to the following categories:

- By importance level—**Critical events**, **Functional failures**, **Warnings**, and **Info events**
- By time—**Recent events**
- By type—**User requests** and **Audit events**

You can create and view user-defined event selections based on the settings available, in the Kaspersky Security Center 13 Web Console interface, for configuration.

Notifications

Notifications alert you about events and help you to speed up your responses to these events by performing recommended actions or actions you consider as appropriate.

Using the dashboard

The dashboard allows you to monitor security trends on your organization's network by providing you with a graphical display of information.

The dashboard is available in the Kaspersky Security Center 13 Web Console, in the **MONITORING & REPORTING** section, by clicking **DASHBOARD**.

The dashboard provides widgets that can be customized. You can choose a large number of different widgets, presented as pie charts or donut charts, tables, graphs, bar charts, and lists. The information displayed in widgets is updated every 1 to 2 minutes. The interval between updates varies for different widgets. You can refresh data on a widget manually at any time by means of the settings menu.

By default, widgets include information about all events stored in the database of Administration Server.

Kaspersky Security Center 13 Web Console has a default set of widgets for the following categories:

- **Protection status**
- **Deployment**
- **Update**
- **Threat statistics**
- **Other**

Some widgets have text information with links. You can view detailed information by clicking a link.

When configuring the dashboard, you can add widgets (see section "Adding widgets to the dashboard" on page [1281](#)) that you need, hide widgets (see section "Hiding a widget from the dashboard" on page [1282](#)) that you do not need, change the size or appearance (see section "Changing the widget size or appearance" on page [1282](#)) of widgets, move (see section "Moving a widget on the dashboard" on page [1282](#)) widgets, and change their settings (see section "Changing widget settings" on page [1283](#)).


See also:

Scenario: Installation and initial setup of Kaspersky Security Center 13 Web Console[962](#)

Adding widgets to the dashboard

► *To add widgets to the dashboard:*

1. Go to **MONITORING & REPORTING** → **DASHBOARD**.


2. Click the **Add or restore web widget** button.
3. In the list of available widgets, select the widgets that you want to add to the dashboard.
Widgets are grouped by category. To view the list of widgets included in a category, click the chevron icon () next to the category name.
4. Click the **Add** button.

The selected widgets are added at the end of the dashboard.

You can now edit the representation (see section "Changing the widget size or appearance" on page [1282](#)) and parameters (see section "Changing widget settings" on page [1283](#)) of the added widgets.

Hiding a widget from the dashboard


► *To hide a displayed widget from the dashboard:*

1. Go to **MONITORING & REPORTING** → **DASHBOARD**.
2. Click the **Settings** icon () next to the widget that you want to hide.
3. Select **Hide web widget**.
4. In the **Warning** window that opens, click **OK**.

The selected widget is hidden. Later, you can add this widget to the dashboard (see section "Adding widgets to the dashboard" on page [1281](#)) again.

Moving a widget on the dashboard

► *To move a widget on the dashboard:*


1. Go to **MONITORING & REPORTING** → **DASHBOARD**.
2. Click the **Settings** icon () next to the widget that you want to move.
3. Select **Move**.
4. Click the place to which you want to move the widget. You can select only another widget.

The places of the selected widgets are swapped.

Changing the widget size or appearance

For widgets that display a graph, you can change its representation—a bar chart or a line chart. For some widgets, you can change their size: compact, medium, or maximum.

► *To change the widget representation:*

1. Go to **MONITORING & REPORTING** → **DASHBOARD**.
2. Click the **Settings** icon () next to the widget that you want to edit.
3. Do one of the following:

- To display the widget as a bar chart, select **Chart type: Bars**.
- To display the widget as a line chart, select **Chart type: Lines**.
- To change the area occupied by the widget, select one of the values: **Compact**, **Compact (bar only)**, **Medium (donut chart)**, **Medium (bar chart)**, or **Maximum**.

The representation of the selected widget is changed.

Changing widget settings

► *To change settings of a widget:*

1. Go to **MONITORING & REPORTING** → **DASHBOARD**.
2. Click the **Settings** icon (⚙️) next to the widget that you want to change.
3. Select **Show settings**.
4. In the widget settings window that opens, change the widget settings as required.
5. Click **Save** to save the changes.

The settings of the selected widget are changed.

The set of settings depends on the specific widget. Below are some of the common settings:

- **Web widget scope** (the set of objects for which the widget displays information)—For example, an administration group or device selection.
- **Select task** (the task for which the widget displays information).
- **Time interval** (the time interval during which the information is displayed in the widget)—Between the two specified dates; from the specified date to the current day; or from the current day minus the specified number of days to the current day.
- **Set to Critical if these are specified** and **Set to Warning if these are specified** (the rules that determine the color of a traffic light).

Using reports

The Reports feature allows you to get detailed numerical information about the security of your organization's network, save this information to a file, send it by email, and print it.

Reports are available in the Kaspersky Security Center 13 Web Console, in the **MONITORING & REPORTING** section, by clicking **REPORTS**.

By default, reports include information for the last 30 days.

Kaspersky Security Center has a default set of reports for the following categories:

- **Protection status**
- **Deployment**
- **Updating**
- **Statistics of threats**
- **Others**

You can create custom report templates (see section "Creating a report template" on page [1284](#)), edit report templates (see section "Viewing and editing report template properties" on page [1284](#)), and delete them (see section "Deleting report templates" on page [1289](#)).

You can create reports (see section "Generating and viewing a report" on page [1287](#)) that are based on existing templates, export reports to files (see section "Exporting a report to a file" on page [1287](#)), and create tasks for report delivery (see section "Creating a report delivery task" on page [1288](#)).

See also:

Scenario: Installation and initial setup of Kaspersky Security Center 13 Web Console[962](#)

Creating a report template

► *To create a report template:*

1. Go to **MONITORING & REPORTING** → **REPORTS**.
2. Click **Add**.
The New Report Template Wizard starts. Proceed through the Wizard by using the **Next** button.
3. On the first page of the Wizard, enter the report name and select the report type.
4. On the **Scope** page of the Wizard, select the set of client devices (administration group, device selection, selected devices, or all networked devices) whose data will be displayed in reports that are based on this report template.
5. On the **Reporting period** page of the Wizard, specify the report period. Available values are as follows:
 - Between the two specified dates
 - From the specified date to the report creation date
 - From the report creation date, minus the specified number of days, to the report creation dateThis page may not appear for some reports.
6. Click **OK** to close the Wizard.
7. Do one of the following:
 - Click the **Save and run** button to save the new report template and to run a report based on it.
The report template is saved. The report is generated.
 - Click the **Save** button to save the new report template.
The report template is saved.

You can use the new template for generating and viewing reports.

Viewing and editing report template properties

You can view and edit basic properties of a report template, for example, the report template name or the fields displayed in the report.

► *To view and edit properties of a report template:*

1. Go to **MONITORING & REPORTING** → **REPORTS**.

2. Select the check box next to the report template whose properties you want to view and edit.

As an alternative, you can first generate the report (see section "Generating and viewing a report" on page [1287](#)), and then click the **Edit** button.

3. Click the **Open report template properties** button.

The **Editing report <Report name>** window opens with the **General** tab selected.

4. Edit the report template properties:

- **General** tab:
 - Report template name
 - **Maximum number of entries to display**

If this option is enabled, the number of entries displayed in the table with detailed report data does not exceed the specified value.

Report entries are first sorted according to the rules specified in the **Fields** → **Details fields** section of the report template properties, and then only the first of the resulting entries are kept. The heading of the table with detailed report data shows the displayed number of entries and the total available number of entries that match other report template settings.

If this option is disabled, the table with detailed report data displays all available entries. We do not recommend that you disable this option. Limiting the number of displayed report entries reduces the load on the database management system (DBMS) and reduces the time required for generating and exporting the report. Some of the reports contain too many entries. If this is the case, you may find it difficult to read and analyze them all. Also, your device may run out of memory while generating such a report and, consequently, you will not be able to view the report.

By default, this option is enabled. The default value is 1000.

- **Group**

Click the **Settings** button to change the set of client devices for which the report is created. For some types of the reports, the button may be unavailable. The actual settings depend on the settings specified during creation of the report template.

- **Time interval**

Click the **Settings** button to modify the report period. For some types of reports, the button may be unavailable. Available values are as follows:

- Between the two specified dates
- From the specified date to the report creation date
- From the report creation date, minus the specified number of days, to the report creation date

- **Include data from secondary and virtual Administration Servers**

If this option is enabled, the report includes the information from the secondary and virtual Administration Servers that are subordinate to the Administration Server for which the report template is created.

Disable this option if you want to view data only from the current Administration Server.

By default, this option is enabled.

- **Up to nesting level**

The report includes data from secondary and virtual Administration Servers that are located under the current Administration Server on a nesting level that is less than or equal to the specified value.

The default value is 1. You may want to change this value if you have to retrieve information from secondary Administration Servers located at lower levels in the tree.

- **Data wait interval (min)**

Before generating the report, the Administration Server for which the report template is created waits for data from secondary Administration Servers during the specified number of minutes. If no data is received from a secondary Administration Server at the end of this period, the report runs anyway. Instead of the actual data, the report shows data taken from the cache (if the **Cache data from secondary Administration Servers** option is enabled), or **N/A** (not available) otherwise.

The default value is 5 (minutes).

- **Cache data from secondary Administration Servers**

Secondary Administration Servers regularly transfer data to the Administration Server for which the report template is created. There, the transferred data is stored in the cache.

If the current Administration Server cannot receive data from a secondary Administration Server while generating the report, the report shows data taken from the cache. The date when the data was transferred to the cache is also displayed.

Enabling this option allows you to view the information from secondary Administration Servers even if the up-to-date data cannot be retrieved. However, the displayed data can be obsolete.

By default, this option is disabled.

- **Cache update frequency (h)**

Secondary Administration Servers at regular intervals transfer data to the Administration Server for which the report template is created. You can specify this period in hours. If you specify 0 hours, data is transferred only when the report is generated.

The default value is 0.

- **Transfer detailed information from secondary Administration Servers**

In the generated report, the table with detailed report data includes data from secondary Administration Servers of the Administration Server for which the report template is created.

Enabling this option slows the report generation and increases traffic between Administration Servers. However, you can view all data in one report.

Instead of enabling this option, you may want to analyze detailed report data to detect a faulty secondary Administration Server, and then generate the same report only for that faulty Administration Server.

By default, this option is disabled.

- **Fields tab**

Select the fields that will be displayed in the report, and use the **Move up** button and **Move down** button to change the order of these fields. Use the **Add** button or **Edit** button to specify whether the information in the report must be sorted and filtered by each of the fields.

In the **Filters of Details fields** section, you can also click the **Convert filters** button to start using the extended filtering format. This format enables you to combine filtering conditions specified in various fields by using the logical OR operation. After you click the button, the **Convert filters** panel opens on the right. Click the **Convert filters** button to confirm conversion. You can now define a converted filter with conditions from the **Details fields** section that are applied by using the logical OR operation.

Conversion of a report to the format supporting complex filtering conditions will make the report incompatible with the previous versions of Kaspersky Security Center (11 and earlier). Also, the converted report will not contain any data from secondary Administration Servers running such incompatible versions.

1. Click **Save** to save the changes.
2. Click the **Close** button (✕) to close the **Editing report <Report name>** window.

The updated report template appears in the list of report templates.

Exporting a report to a file

You can export a report to an XML, HTML, or PDF file.

► *To export a report to a file:*

1. Go to **MONITORING & REPORTING** → **REPORTS**.
2. Select the check box next to the report that you want to export to a file.
3. Click the **Export report** button.
4. In the window that opens, change the report file name in the **Name** field. By default, the file name coincides with the name of the selected report template.
5. Select the report file type: XML, HTML, or PDF.
6. Click the **Export report** button.

The report in selected format will be downloaded to your device—to the default folder of your device—or a standard **Save as** window in your browser will open to let you save the file where you want.

The report is saved to the file.



Generating and viewing a report

► *To create and view a report:*

1. Go to **MONITORING & REPORTING** → **REPORTS**.
2. Click the name of the report template that you want to use to create a report.

A report using the selected template is generated and displayed.

The report displays the following data:

- On the **Summary** tab:
 - The name and type of report, a brief description and the reporting period, as well as information about the group of devices for which the report is generated.
 - Graph chart showing the most representative report data.
 - Consolidated table with calculated report indicators.
- On the **Details** tab, a table with detailed report data is displayed.

See also:

Scenario: Updating third-party software[1208](#)

Creating a report delivery task

You can create a task that will deliver selected reports.

► *To create a report delivery task:*

1. Go to **MONITORING & REPORTING** → **REPORTS**.
2. [Optional] Select the check boxes next to the report templates for which you want to create a report delivery task.
3. Click the **New report delivery task** button.
4. The New Task Wizard starts. Proceed through the Wizard by using the **Next** button.
5. On the first page of the Wizard, enter the task name. The default name is **Deliver reports (<N>)**, where <N> is the sequence number of the task.
6. On the task settings page of the Wizard, specify the following settings:
 - a. Report templates to be delivered by the task. If you selected them at step 2, skip this step.
 - b. The report format: HTML, XLS, or PDF.
 - c. Whether the reports are to be sent by email, together with email notification settings.
 - d. Whether the reports are to be saved to a folder, whether previously saved reports in this folder are to be overwritten, and whether a specific account is to be used to access the folder (for a shared folder).
7. If you want to modify other task settings after the task is created, on the **Finish task creation** page of the Wizard enable the **Open task details when creation is complete** option.
8. Click the **Create** button to create the task and close the Wizard.

The report delivery task is created. If you enabled the **Open task details when creation is complete** option, the task settings window opens.

Deleting report templates

► *To delete one or several report templates:*

1. Go to **MONITORING & REPORTING** → **REPORTS**.
2. Select check boxes next to the report templates that you want to delete.
3. Click the **Delete** button.
4. In the confirmation window that opens, click **OK**.

The selected report templates are deleted. If these report templates were included in the report delivery tasks, they are also removed from the tasks.

Using event selections

Event selections provide an onscreen view of named sets of events that are selected from the Administration Server database. These sets of events are grouped according to the following categories:

- By importance level—**Critical events**, **Functional failures**, **Warnings**, and **Info events**
- By time—**Recent events**
- By type—**User requests** and **Audit events**

You can create and view user-defined event selections based on the settings available, in the Kaspersky Security Center 13 Web Console interface, for configuration.

Event selections are available in the Kaspersky Security Center 13 Web Console, in the **MONITORING & REPORTING** section, by clicking **EVENT SELECTIONS**.

By default, event selections include information for the last seven days.

Kaspersky Security Center has a default set of event (predefined) selections:

- Events with different importance levels:
 - **Critical events**
 - **Functional failures**
 - **Warnings**
 - **Informational messages**
- **User requests** (events of managed applications)
- **Recent events** (over the last week)
- **Audit events** (see section "**Administration Server informational events**" on page [566](#)).

You can also create and configure additional user-defined selections (see section "Creating an event selection" on page [1290](#)). In user-defined selections, you can filter events by the properties of the devices they originated from (device names, IP ranges, and administration groups), by event types and severity levels, by application and component name, and by time interval. It is also possible to include task results in the search scope. You can also use a simple search field where a word or several words can be typed. All events that contain any of the typed words anywhere in their attributes (such as event name, description, component name) are displayed.

Both for predefined and user-defined selections, you can limit the number of displayed events or the number of records to search. Both options affect the time it takes Kaspersky Security Center to display the events. The larger the database is, the more time-consuming the process can be.

You can edit properties of event selections (see section "Editing an event selection" on page [1290](#)), generate event selections (see section "Viewing a list of an event selection" on page [1291](#)), view details of event selections (see section "Viewing details of an event" on page [1291](#)), delete event selections (see section "Deleting event selections" on page [1292](#)), and delete events from the Administration Server database (see section "Deleting events" on page [1292](#)).

See also:

Device selections	1037
Scenario: Installation and initial setup of Kaspersky Security Center 13 Web Console	962

Creating an event selection

► To create an event selection:

1. Go to **MONITORING & REPORTING** → **EVENT SELECTIONS**.
2. Click **Add**.
3. In the **New event selection** window that opens, specify the settings of the new event selection. Do this in one or more of the sections in the window.
4. Click **Save** to save the changes.
The confirmation window opens.
5. To view the event selection result, keep the **Go to selection result** check box selected.
6. Click **Save** to confirm the event selection creation.

If you kept the **Go to selection result** check box selected, the event selection result is displayed. Otherwise, the new event selection appears in the list of event selections.

Editing an event selection

► To edit an event selection:

1. Go to **MONITORING & REPORTING** → **EVENT SELECTIONS**.
2. Select the check box next to the event selection that you want to edit.
3. Click the **Properties** button.
An event selection settings window opens.
4. Edit the properties of the event selection.

For predefined event selections, you can edit only the properties on the following tabs: **General** (except for the selection name), **Time**, and **Access rights**.

For user-defined selections, you can edit all properties.

5. Click **Save** to save the changes.

The edited event selection is shown in the list.

Viewing a list of an event selection

► *To start an event selection:*

1. Go to **MONITORING & REPORTING** → **EVENT SELECTIONS**.
2. Select the check box next to the event selection that you want to start.
3. Do one of the following:
 - If you want to configure sorting in the event selection result, do the following:
 - a. Click the **Reconfigure sorting and start** button.
 - b. In the displayed **Reconfigure sorting for event selection** window, specify the sorting settings.
 - c. Click the name of the selection.
 - Otherwise, if you want to view the list of events as they are sorted on the Administration Server, click the name of the selection.

The event selection result is displayed.

Viewing details of an event

► *To view details of an event:*

1. Start an event selection (see section "Viewing a list of an event selection" on page [1291](#)).
2. Click the time of the required event.
The **Event properties** window opens.
3. In the displayed window, you can do the following:
 - View the information about the selected event.
 - Go to the next event and the previous event in the event selection result.
 - Go to the device on which the event occurred.
 - Go to the administration group that includes the device on which the event occurred.
 - For an event related to a task, go to the task properties.

Exporting events to a file

► *To export events to a file:*

1. Start an event selection (see section "Viewing a list of an event selection" on page [1291](#)).
2. Select the check box next to the required event.
3. Click the **Export to file** button.

The selected event is exported to a file.

Viewing an object history from an event

From an event of creation or modification of an object that supports revision management (see section "Managing object revisions" on page [719](#)), you can switch to the revision history of the object.

► *To view an object history from an event:*

1. Start an event selection (see section "Viewing a list of an event selection" on page [1291](#)).
2. Select the check box next to the required event.
3. Click the **Revision history** button.

The revision history of the object is opened.

Deleting events

► *To delete one or several events:*

1. Start an event selection (see section "Viewing a list of an event selection" on page [1291](#)).
2. Select the check boxes next to the required events.
3. Click the **Delete** button.

The selected events are deleted and cannot be restored.

Deleting event selections

You can delete only user-defined event selections. Predefined event selections cannot be deleted.

► *To delete one or several event selections:*

1. Go to **MONITORING & REPORTING** → **EVENT SELECTIONS**.
2. Select the check boxes next to the event selections that you want to delete.
3. Click **Delete**.
4. In the window that opens, click **OK**.

The event selection is deleted.

Using notifications

Notifications alert you about events and help you to speed up your responses to these events by performing recommended actions or actions you consider as appropriate.

Depending on the notification method chosen, the following types of notifications are available:

- Onscreen notifications
- Notifications by SMS
- Notifications by email
- Notifications by executable file or script

Onscreen notifications

Onscreen notifications alert you to events grouped by importance levels (*Critical*, *Warning*, and *Informational*).

Onscreen notification can have one of two statuses:

- *Reviewed*. It means you have performed recommended action for the notification or you have assigned this status for the notification manually.
- *Not Reviewed*. It means you have not performed recommended action for the notification or you have not assigned this status for the notification manually.

By default, the list of notifications include notifications in the *Not Reviewed* status.

You can monitor your organization's network viewing onscreen notifications (on page [1293](#)) and responding to them in a real time.

Notifications by email, by SMS, and by executable file or a script

Kaspersky Security Center provides the capability to monitor your organization's network by sending notifications about any event that you consider important. For any event you can configure notifications by email, by SMS, or by running an executable file or a script (see section "Configuring notification delivery" on page [1303](#)).

Upon receiving notifications by email or by SMS, you can decide on your response to an event. This response has to be the one that is most appropriate for your organization's network. By running an executable file or a script, you predefine a response to an event. You can also consider running an executable file or a script as a primary response to an event. After the executable file runs, you can take other steps to respond to the event.

Viewing onscreen notifications

You can view notifications onscreen in three ways:

- In the **MONITORING & REPORTING** → **NOTIFICATIONS** section. Here you can view notifications relating to predefined categories.
- In a separate window that can be opened no matter which section you are using at the moment. In this case you can mark notifications as reviewed.

- In the **Notifications by selected severity level** widget on the **MONITORING & REPORTING** → **DASHBOARD** section. In the widget, you can view only notifications of events that are at the *Critical* and *Warning* severity levels.

You can perform actions, for example, you can respond to an event.

► *To view notifications from predefined categories:*

1. Go to **MONITORING & REPORTING** → **NOTIFICATIONS**.

The **All notifications** category is selected in the left pane, and in the right pane all the notifications are displayed.

2. In the left pane, select one of the categories:

- **Deployment**
- **Devices**
- **Protection**
- **Updates** (this includes notifications about Kaspersky applications available for download and notifications about anti-virus database updates that have been downloaded)
- **Exploit Prevention**
- **Administration Server** (this includes events concerning only Administration Server)
- **Useful links** (this includes links to Kaspersky resources, for example, Kaspersky Technical Support, Kaspersky forum, license renewal page, or the Kaspersky IT Encyclopedia)
- **Kaspersky news** (this includes information about releases of Kaspersky applications)

A list of notifications of the selected category is displayed. The list contains the following:

- Icon related to the topic of the notification: deployment (📦), protection (🛡️), updates (🔄), device management (📱), Exploit Prevention (🛡️), Administration Server (🖨️).
- Notification severity level. Notifications of the following severity levels are displayed: **Critical notifications** (🔴), **Warning notifications** (🟡), **Info notifications**. Notifications in the list are grouped by severity levels.
- **Notification**. This contains a description of the notification.
- **Action**. This contains a link to a quick action that we recommend you perform. For example, by clicking this link, you can proceed to the repository (see section "Downloading and creating installation packages for Kaspersky applications" on page [1025](#)) and install security applications on devices, or view a list of devices or a list of events. After you perform the recommended action for the notification, this notification is assigned the *Reviewed* status.
- **Status registered**. This contains the number of days or hours that have passed from the moment when the notification was registered on the Administration Server.

► *To view onscreen notifications in a separate window by severity level:*

1. In the upper-right corner of Kaspersky Security Center 13 Web Console, click the **Flag** icon (🚩).

If the **Flag** icon has a red dot, there are notifications that have not been reviewed.

A window opens listing the notifications. By default, the **All notifications** tab is selected and the notifications are grouped by severity level: *Critical*, *Warning*, and *Info*.

2. Select the **System** tab.

The list of *Critical* (🔴) and *Warning* (🟡) severity level notifications is displayed. The notification list includes the following:

- Color marker. Critical notifications are marked in red. Warning notifications are marked in yellow.
- Icon indicating the topic of the notification: deployment (🔧), protection (🛡️), updates (🔄), device management (📱), Exploit Prevention (🛡️), Administration Server (🖥️).
- Description of the notification.
- **Flag** icon. The **Flag** icon is gray if notifications have been assigned the *Not Reviewed* status. When you select the gray **Flag** icon and assign the *Reviewed* status to a notification, the icon changes color to white.
- Link to the recommended action. When you perform the recommended action after clicking the link, the notification gets the *Reviewed* status.
- Number of days that have passed since the date when the notification was registered on the Administration Server.

3. Select the **More** tab.

The list of *Info* severity level notifications is displayed.

The organization of the list is the same as for the list on the **System** tab (see the description above). The only difference is the absence of a color marker.

You can filter notifications by the date interval when they were registered on Administration Server. Use the **Show filter** check box to manage the filter.

► *To view onscreen notifications in the widget:*

1. In the **DASHBOARD** section, select **Add or restore web widget**.
2. In the window that opens, click the **Other** category, select the **Notifications by selected severity level** widget, and click **Add** (see section "Adding widgets to the dashboard" on page [1281](#)).

The widget now appears on the **DASHBOARD** tab. By default, the notifications of *Critical* severity level are displayed on the widget.

You can click the **Settings** button on the widget and change the widget settings (see section "Changing widget settings" on page [1283](#)) to view notifications of the *Warning* severity level. Or, you can add another widget: **Notifications by selected severity level**, with a *Warning* severity level.

The list of notifications on the widget is limited by its size and includes two notifications. These two notifications relate to the latest events.

The notification list in the widget includes the following:

- Icon related to the topic of the notification: deployment (🔧), protection (🛡️), updates (🔄), device management (📱), Exploit Prevention (🛡️), Administration Server (🖥️).
- Description of the notification with a link to the recommended action. When you perform a recommended action by clicking the link, the notification is assigned the *Reviewed* status.
- Number of days or number of hours that have passed since the date when the notification was registered on the Administration Server.
- Link to other notifications. Upon clicking this link, you are transferred to the view of notifications in the **NOTIFICATIONS** section of the **MONITORING & REPORTING** section.

About device statuses

Kaspersky Security Center assigns a status to each managed device. The particular status depends on whether the conditions defined by the user are met. In some cases, when assigning a status to a device, Kaspersky Security Center takes into consideration the device's visibility flag on the network (see the table below). If Kaspersky Security Center does not find a device on the network within two hours, the visibility flag of the device is set to *Not Visible*.

The statuses are the following:

- *Critical* or *Critical / Visible*
- *Warning* or *Warning / Visible*
- *OK* or *OK / Visible*

The table below lists the default conditions that must be met to assign the *Critical* or *Warning* status to a device, with all possible values.

Table 86. Conditions for assigning a status to a device

Condition	Condition description	Available values
Security application is not installed	Network Agent is installed on the device, but a security application is not installed.	<ul style="list-style-type: none"> • Toggle button is on. • Toggle button is off.
Too many viruses detected	Some viruses have been found on the device by a task for virus detection, for example, the Virus scan task, and the number of viruses found exceeds the specified value.	More than 0.
Real-time protection level differs from the level set by the Administrator	The device is visible on the network, but the real-time protection level differs from the level set (in the condition) by the administrator for the device status.	<ul style="list-style-type: none"> • Stopped. • Paused. • Running.
Virus scan has not been performed in a long time	The device is visible on the network and a security application is installed on the device, but the Virus scan task has not been run within the specified time interval. The condition is applicable only to devices that were added to the Administration Server database 7 days ago or earlier.	More than 1 day.
Databases are outdated	The device is visible on the network and a security application is installed on the device, but the anti-virus databases have not been updated on this device within the specified time interval. The condition is applicable only to devices that were added to the Administration Server database 1 day ago or earlier.	More than 1 day.
Not connected in a long time	Network Agent is installed on the device, but the device has not connected to an Administration Server within the specified time interval, because the device was turned off.	More than 1 day.
Active threats are detected	The number of unprocessed objects in the ACTIVE THREATS folder exceeds the specified value.	More than 0 items.

Condition	Condition description	Available values
Restart is required	The device is visible on the network, but an application requires the device restart longer than the specified time interval and for one of the selected reasons.	More than 0 minutes.
Incompatible applications are installed	The device is visible on the network, but software inventory performed through Network Agent has detected incompatible applications installed on the device.	<ul style="list-style-type: none"> • Toggle button is off. • Toggle button is on.
Software vulnerabilities have been detected	The device is visible on the network and Network Agent is installed on the device, but the <i>Find vulnerabilities and required updates</i> task has detected vulnerabilities with the specified severity level in applications installed on the device.	<ul style="list-style-type: none"> • Critical. • High. • Medium. • Ignore if the vulnerability cannot be fixed. • Ignore if an update is assigned for installation.
License expired	The device is visible on the network, but the license has expired.	<ul style="list-style-type: none"> • Toggle button is off. • Toggle button is on.
License expires soon	The device is visible on the network, but the license will expire on the device in less than the specified number of days.	More than 0 days.

Condition	Condition description	Available values
Check for Windows Update updates has not been performed in a long time	The device is visible on the network, but the Perform Windows Update synchronization task has not been run within the specified time interval.	More than 1 day.
Invalid encryption status	Network Agent is installed on the device, but the device encryption result is equal to the specified value.	<ul style="list-style-type: none"> • Does not comply with the policy due to the user's refusal (for external devices only). • Does not comply with the policy due to an error. • Restart is required when applying the policy. • No encryption policy is specified. • Not supported. • When applying the policy.
Mobile device settings do not comply with the policy	The mobile device settings are other than the settings that were specified in the Kaspersky Endpoint Security for Android policy during the check of compliance rules.	<ul style="list-style-type: none"> • Toggle button is off. • Toggle button is on.
Unprocessed incidents detected	Some unprocessed incidents have been found on the device. Incidents can be created either automatically, through managed Kaspersky applications installed on the client device, or manually by the administrator.	<ul style="list-style-type: none"> • Toggle button is off. • Toggle button is on.
Device status defined by application	The status of the device is defined by the managed application.	<ul style="list-style-type: none"> • Toggle button is off. • Toggle button is on.
Device is out of disk space	Free disk space on the device is less than the specified value or the device could not be synchronized with the Administration Server. The <i>Critical</i> or <i>Warning</i> status is changed to the <i>OK</i> status when the device is successfully synchronized with the Administration Server and free space on the device is greater than or equal to the specified value.	More than 0 MB

Condition	Condition description	Available values
Device has become unmanaged	During device discovery, the device was recognized as visible on the network, but more than three attempts to synchronize with the Administration Server failed.	<ul style="list-style-type: none"> Toggle button is off. Toggle button is on.
Protection is disabled	The device is visible on the network, but the security application on the device has been disabled for longer than the specified time interval.	More than 0 minutes.
Security application is not running	The device is visible on the network and a security application is installed on the device but is not running.	<ul style="list-style-type: none"> Toggle button is off. Toggle button is on.

Kaspersky Security Center allows you to set up automatic switching of the status of a device in an administration group when specified conditions are met. When specified conditions are met, the client device is assigned one of the following statuses: *Critical* or *Warning*. When specified conditions are not met, the client device is assigned the *OK* status.

Different statuses may correspond to different values of one condition. For example, by default, if the **Databases are outdated** condition has the **More than 3 days** value, the client device is assigned the *Warning* status; if the value is **More than 7 days**, the *Critical* status is assigned.

If you upgrade the Kaspersky Security Center from the previous version, the values of the **Databases are outdated** condition for assigning the status to *Critical* or *Warning* do not change.

When Kaspersky Security Center assigns a status to a device, for some conditions (see the Condition description column) the visibility flag is taken into consideration. For example, if a managed device was assigned the *Critical* status because the Databases are outdated condition was met, and later the visibility flag was set for the device, then the device is assigned the *OK* status.

See also:

Configuring the switching of device statuses[1301](#)

Configuring the switching of device statuses

You can change conditions to assign the *Critical* or *Warning* status to a device.

► *To enable changing the device status to Critical:*

1. Go to **DEVICES** → **HIERARCHY OF GROUPS**.

2. In the list of groups that opens, click the link with the name of a group for which you want to change switching the device statuses.
3. In the properties window that opens, select the **Device status** tab.
4. In the left pane, select **Critical**.
5. In the right pane, in the **Set to Critical if these are specified** section, enable the condition to switch a device to the *Critical* status.

You can change only settings that are not locked in the parent policy.

6. Select the radio button next to the condition in the list.
7. In the upper-left corner of the list, click the **Edit** button.
8. Set the required value for the selected condition.
Values cannot be set for every condition.
9. Click **OK**.

When specified conditions are met, the managed device is assigned the *Critical* status.

► *To enable changing the device status to Warning:*

1. Go to **DEVICES** → **HIERARCHY OF GROUPS**.
2. In the list of groups that opens, click the link with the name of a group for which you want to change switching the device statuses.
3. In the properties window that opens, select the **Device status** tab.
4. In the left pane, select **Warning**.
5. In the right pane, in the **Set to Warning if these are specified** section, enable the condition to switch a device to the *Warning* status.

You can change only settings that are not locked in the parent policy.

6. Select the radio button next to the condition in the list.
7. In the upper-left corner of the list, click the **Edit** button.
8. Set the required value for the selected condition.
Values cannot be set for every condition.
9. Click **OK**.

When specified conditions are met, the managed device is assigned the *Warning* status.

See also:

About device statuses	1099
Scenario: Monitoring and reporting	1279

Configuring notification delivery

You can configure notification about events occurring in Kaspersky Security Center. Depending on the notification method chosen, the following types of notifications are available:

- **Email**—When an event occurs, Kaspersky Security Center sends a notification to the email addresses specified.
- **SMS**—When an event occurs, Kaspersky Security Center sends a notification to the phone numbers specified.
- **Executable file**—When an event occurs, the executable file is run on the Administration Server.

► *To configure notification delivery of events occurring in Kaspersky Security Center:*

1. At the top of the screen, click the **Settings** icon () next to the name of the required Administration Server.

The Administration Server properties window opens with the **General** tab is selected.

2. Click the **Notification** section, and in the right pane select the tab for the notification method you want:
 - **Email**

The **Email** tab allows you to configure event notification by email.

In the **Recipients (email addresses)** field, specify the email addresses to which the application will send notifications. You can specify multiple addresses in this field, separating them with semicolons.

In the **SMTP servers** field, specify mail server addresses, separating them with semicolons. You can use the IP address or the Windows network name (NetBIOS name) of the device as the address.

In the **SMTP server port** field, specify the number of an SMTP server communication port. The default port number is 25.

If the **Use DNS MX lookup** option is enabled, the **SMTP servers** field is interpreted as a DNS name to be resolved. The same DNS name may have several MX records with different priorities. Attempts to send email notification are made in ascending order of priority. By default, this option is disabled.

In the **Subject** field, specify the email subject. You can leave this field empty.

In the **Subject template** drop-down list, select the template for your subject. A variable determined by the selected template is placed automatically in the **Subject** field. You can construct an email subject selecting several subject templates.

In the **Sender email address: If this setting is not specified, the recipient address will be used instead.**

Warning: We do not recommend using a fictitious email address field, specify the sender email address. If you leave this field empty, by default, the recipient address is used. It is not recommended to use fictitious email addresses.

If the **Use ESMTP authentication** option is enabled, in the **User name** and **Password** fields you can specify the ESMTP authentication settings. By default, the option is disabled, and the ESMTP authentication settings are not available.

Clicking the **Specify certificate** link allows you to specify a certificate file for authentication on the SMTP server.

The **Notification message** field contains standard text with information about the event that the application sends when an event occurs. This text includes substitute parameters, such as event name, device name, and domain name. You can edit the

message text by adding other substitute parameters (see section "Event notifications displayed by running an executable file" on page [300](#)) with more relevant details about the event.

If the notification text contains a percent sign (%), you have to type it twice in a row to allow message sending. For example, "CPU load is 100%%".

Clicking the **Configure numeric limit of notifications** link allows you to specify the maximum number of notifications that the application can send over the specified time interval.

Clicking the **Send test message** button allows you to check whether you configured notifications properly: the application sends a test notification to the email addresses that you specified.

- SMS

The **SMS** tab allows you to configure the transmission of SMS notifications about various events to a cell phone. SMS messages is sent through a mail gateway.

In the **Recipients (email addresses)** field, specify the email addresses to which the application will send notifications. You can specify multiple addresses in this field, separating them with semicolons. The notifications will be delivered to the phone numbers associated with the specified email addresses.

In the **SMTP servers** field, specify mail server addresses, separating them with semicolons. You can use the IP address or the Windows network name (NetBIOS name) of the device as the address.

In the **SMTP server port** field, specify the number of an SMTP server communication port. The default port number is 25.

In the **Subject** field, specify the email subject.

In the **Subject template** drop-down list, select the template for your subject. A variable according to the selected template is put in the **Subject** field. You can construct an email subject selecting several subject templates.

In the **Sender email address: If this setting is not specified, the recipient address will be used instead. Warning: We do not recommend using a fictitious email address** field, specify the sender email address. If you leave this field empty, by default, the recipient address is used. It is not recommended to use fictitious email addresses.

If the **Use ESMTP authentication** option is enabled, in the **User name** and **Password** fields you can specify the ESMTP authentication settings. By default, the option is disabled, and the ESMTP authentication settings are not available.

In the **Notification message** field, specify a text with information about the event that the application sends when an event occurs. This text can include substitute parameters (see section "Event notifications displayed by running an executable file" on page [300](#)), such as event name, device name, and domain name.

If the notification text contains a percent sign (%), you have to type it twice in a row to allow message sending. For example, "CPU load is 100%%".

Clicking the **Configure numeric limit of notifications** link allows you to specify the maximum number of notifications that the application can send during the specified time interval.

Clicking the **Send test message** allows you to check whether you configured notifications properly: the application sends a test notification to the recipient that you specified.

- Executable file to run

If this notification method is selected, in the entry field you can specify the application that will start when an event occurs.

In the **Executable file to be run on the Administration Server when an event occurs** field, specify the folder and the name of the file to be run. The folder and the file that you specify must be located on the Administration Server.

Clicking the **Configure numeric limit of notifications** link allows you to specify the maximum number of notifications that the application can send during the specified time interval.

1. On the tab, define the notification settings.
2. Click the **OK** button to close Administration Server properties window.

The saved notification delivery settings are applied to all events that occur in Kaspersky Security Center.

You can override notification delivery settings for certain events in the **Event configuration** section of the Administration Server settings, of a policy's settings, or of an application's settings (see section "Modifying a policy" on page [1119](#)).

See also:

| Scenario: Monitoring and reporting[1279](#)

Setting the storage term for an event

Kaspersky Security Center allows you to receive information about events that occur during the operation of Administration Server and Kaspersky applications installed on managed devices. Information about events is saved in the Administration Server database. You might need to store some events for a longer or shorter period of time than specified by default values. You can change the default settings of the storage term for an event.

If you are not interested in storing some events in the database of Administration Server, you can disable the appropriate setting in the Administration Server policy and Kaspersky application policy, or in the Administration Server properties (only for Administration Server events). This will reduce the number of event types in the database.

The longer the storage term for an event, the faster the database reaches its maximum capacity. However, a longer storage term for an event lets you perform monitoring and reporting tasks for a longer period of time.

► *To set the storage term for an event in the database of Administration Server:*

1. Select **DEVICES** → **POLICIES & PROFILES**.
2. Do one of the following:

- To configure the storage term of the events of Network Agent or of a managed Kaspersky application, click the name of the corresponding policy.
The policy properties page opens.
- To configure Administration Server events, at the top of the screen, click the **Settings** icon (🔧) next to the name of the required Administration Server.
If you have a policy for the Administration Server, you can click the name of this policy instead.
The Administration Server properties page (or the Administration Server policy properties page) opens.

3. Select the **Event configuration** tab.

A list of event types related to the **Critical** section is displayed.

4. Select the **Functional failure**, **Warning**, or **Info** section.

5. In the list of event types in the right pane, click the link for the event whose storage term you want to change.

In the **Event registration** section of the window that opens, the **Store in the Administration Server database for (days)** option is enabled.

6. In the edit box below this toggle button, enter the number of days to store the event.

7. If you do not want to store an event in the Administration Server database, disable the **Store in the Administration Server database for (days)** option.

If you configure Administration Server events in Administration Server properties window and if event settings are locked in the Kaspersky Security Center Administration Server policy, you cannot redefine the storage term value for an event.

8. Click **OK**.

The properties window of the policy is closed.

The new storage term for the event you selected now takes effect.

Event types

Each Kaspersky Security Center component has its own set of event types. This section lists types of events that occur in Kaspersky Security Center Administration Server, Network Agent, iOS MDM Server, and Exchange Mobile Device Server. Types of events that occur in Kaspersky applications are not listed in this section.

In this section

Data structure of event type description	1307
Administration Server events.....	1307
Network Agent events.....	1340
iOS MDM Server events	1344
Exchange Mobile Device Server events.....	1350

Data structure of event type description

For each event type, its display name, identifier (ID), alphabetic code, description, and the default storage term are provided.

- **Event type display name.** This text is displayed in Kaspersky Security Center when you configure events and when they occur.
- **Event type ID.** This numerical code is used when you process events by using third-party tools for event analysis.
- **Event type** (alphabetic code). This code is used when you browse and process events by using public views that are provided in the Kaspersky Security Center database and when events are exported to a SIEM system.
- **Description.** This text contains the situations when an event occurs and what you can do in such a case.
- **Default storage term.** This is the number of days during which the event is stored in the Administration Server database and is displayed in the list of events on Administration Server. After this period elapses, the event is deleted. If the event storage term value is 0, such events are detected but are not displayed in the list of events on Administration Server. If you configured to save such events to the operating system event log, you can find them there.

You can change the storage term for events:

- Administration Console: Setting the storage term for an event (see section "Event processing and storage on the Administration Server" on page [610](#))
- Kaspersky Security Center 13 Web Console: Setting the storage term for an event (on page [1305](#))

Administration Server events

This section contains information about the events related to the Administration Server.

In this section

Administration Server critical events	1308
Administration Server functional failure events	1317
Administration Server warning events	1323
Administration Server informational events	1338

Administration Server critical events

The table below shows the events of Kaspersky Security Center Administration Server that have the **Critical** severity level.

Table 87. Administration Server critical events

Event type display name	Event type ID	Event type	Description	Default storage term
<p>License limit has been exceeded</p>	<p>4099</p>	<p>KLSRV_EV_LICENSE_CHECK_MORE_110</p>	<p>Once a day Kaspersky Security Center checks whether a licensing restriction is exceeded.</p> <p>Events of this type occur when Administration Server detects that some licensing limits are exceeded by Kaspersky applications installed on client devices and if the number of currently used licensing units (see section "About the license certificate" on page 319) covered by a single license exceeds 110% of the total number of units covered by the license.</p> <p>Even when this event occurs, client devices are protected.</p> <p>You can respond to the event in the following ways:</p> <ul style="list-style-type: none"> • Look through the managed devices list. Delete devices that are not in use. • Provide a license for more devices (add a valid activation code or a key file to Administration Server). <p>Kaspersky Security Center determines the rules to generate events (see section "Events of the licensing limit exceeded" on page 329) when a licensing restriction is exceeded.</p>	<p>180 days</p>

Event type display name	Event type ID	Event type	Description	Default storage term
Virus outbreak	26 (for File Threat Protection)	GNRL_EV_VIRUS_OUTBREAK	<p>Events of this type occur when the number of malicious objects detected on several managed devices exceeds the threshold within a short period of time.</p> <p>You can respond to the event in the following ways:</p> <ul style="list-style-type: none"> • Configure the threshold in the Administration Server properties (on page 611). • Create a stricter policy (see section "Activating a policy automatically at the Virus outbreak event" on page 390) that will be activated, or create a task (see section "Creating a task" on page 374) that will be run, at the occurrence of this event. 	180 days

Event type display name	Event type ID	Event type	Description	Default storage term
Virus outbreak	27 (for Mail Threat Protection)	GNRL_EV_VIRUS_OUTBREAK	<p>Events of this type occur when the number of malicious objects detected on several managed devices exceeds the threshold within a short period of time.</p> <p>You can respond to the event in the following ways:</p> <ul style="list-style-type: none"> • Configure the threshold in the Administration Server properties (on page 611). • Create a stricter policy (see section "Activating a policy automatically at the Virus outbreak event" on page 390) that will be activated, or create a task (see section "Creating a task" on page 374) that will be run, at the occurrence of this event. 	180 days

Event type display name	Event type ID	Event type	Description	Default storage term
Virus outbreak	28 (for firewall)	GNRL_EV_VIRUS_OUTBREAK	<p>Events of this type occur when the number of malicious objects detected on several managed devices exceeds the threshold within a short period of time.</p> <p>You can respond to the event in the following ways:</p> <ul style="list-style-type: none"> • Configure the threshold in the Administration Server properties (on page 611). • Create a stricter policy (see section "Activating a policy automatically at the Virus outbreak event" on page 390) that will be activated, or create a task (see section "Creating a task" on page 374) that will be run, at the occurrence of this event. 	180 days
Device has become unmanaged	4111	KLSRV_HOST_OUT_CONTROL	<p>Events of this type occur if a managed device is visible on the network but has not connected to Administration Server for a specific period of time.</p> <p>Find out what prevents the proper functioning of Network Agent on the device. Possible causes include network issues and removal of Network Agent from the device.</p>	180 days

Event type display name	Event type ID	Event type	Description	Default storage term
Device status is Critical	4113	KLSRV_HOST_STATUS_CRITICAL	Events of this type occur when a managed device is assigned the <i>Critical</i> status. You can configure the conditions (see section "Configuring the switching of device statuses" on page 647) under which the device status is changed to <i>Critical</i> .	180 days
The key file has been added to the denylist	4124	KLSRV_LICENSE_BLACKLISTED	Events of this type occur when Kaspersky has added the activation code or key file that you use to the denylist. Contact Technical Support (on page 1401) for more detail.	180 days

Event type display name	Event type ID	Event type	Description	Default storage term
Limited functionality mode	4130	KLSRV_EV_LICENSE_SRV_LIMITED_MODE	<p>Events of this type occur when Kaspersky Security Center starts to operate with basic functionality (see section "About restrictions on the main functionality" on page 322), without Vulnerability and Patch Management and without Mobile Device Management features.</p> <p>Following are causes of, and appropriate responses to, the event:</p> <ul style="list-style-type: none"> • License term has expired. Provide a license to use the full functionality mode of Kaspersky Security Center (add a valid activation code or a key file to Administration Server). • Administration Server manages more devices than specified by the license limit. Move devices from the administration groups of an Administration Server to those of another Administration Server (if the license limit of the other Administration Server allows). 	180 days

Event type display name	Event type ID	Event type	Description	Default storage term
License expires soon	4129	KLSRV_EV_LICENSE_SRV_EXPIRE_SOON	<p>Events of this type occur when the commercial license (see section "About the license" on page 319) expiration date is approaching.</p> <p>When the commercial license expires, Kaspersky Security Center provides only basic functionality (see section "About restrictions on the main functionality" on page 322).</p> <p>You can respond to the event in the following ways:</p> <ul style="list-style-type: none"> • Make sure that a reserve license key (see section "About the license key" on page 320) is added to Administration Server. • If you use a subscription (see section "About the subscription" on page 328), make sure to renew it. An unlimited subscription is renewed automatically if it has been prepaid to the service provider by the due date. 	180 days

Event type display name	Event type ID	Event type	Description	Default storage term
Certificate has expired	4132	KLSRV_CERTIFICATE_EXPIRED	<p>Events of this type occur when the Administration Server certificate for Mobile Device Management expires.</p> <p>You need to update the expired certificate (see section "Working with certificates" on page 737).</p> <p>You can configure automatic updates of certificates by selecting the Reissue certificate automatically if possible check box in the certificate issuance settings (see section "Configuring certificate issuance rules" on page 742).</p>	180 days
Updates for Kaspersky software modules have been revoked	4142	KLSRV_SEAMLESS_UPDATE_REVOKED	<p>Events of this type occur if seamless updates (see section "Approving and declining software updates" on page 1197) have been revoked (<i>Revoked</i> status is displayed for these updates) by Kaspersky technical specialists; for example, they must be updated to a newer version. The event concerns Kaspersky Security Center patches and does not concern modules of managed Kaspersky applications. The event provides the reason that the seamless updates are not installed.</p>	180 days

See also:

Administration Server functional failure events	543
Administration Server informational events	566
Administration Server warning events	552
Events in Kaspersky Security Center	792

Administration Server functional failure events

The table below shows the events of Kaspersky Security Center Administration Server that have the **Functional failure** severity level.

Table 88. Administration Server functional failure events

Event type display name	Event type ID	Event type	Description	Default storage term
Runtime error	4125	KLSRV_RUNTIME_ERROR	<p>Events of this type occur because of unknown issues.</p> <p>Most often these are DBMS issues, network issues, and other software and hardware issues.</p> <p>Details of the event can be found in the event description.</p>	180 days
Limit of installations has been exceeded for one of the licensed applications groups	4126	KLSRV_INVLICPRO D_EXCEDED	<p>Administration Server generates events of this type periodically (every hour). Events of this type occur if in Kaspersky Security Center you manage license keys of third-party applications and if the number of installations has exceeded the limit set by the license key of the third-party application.</p> <p>You can respond to the event in the following ways:</p> <ul style="list-style-type: none"> • Look through the managed devices list. Delete the third-party application from devices on which the application is not in use. • Use a third-party license for more devices. <p>You can manage license keys of third-party applications (see section "Managing license keys for licensed applications groups" on page 499) using the functionality of licensed applications groups. A licensed applications group includes third-party applications that meet criteria set by you.</p>	180 days

Event type display name	Event type ID	Event type	Description	Default storage term
Failed to poll the cloud segment	4143	KLSRV_KLCLLOUD_SCAN_ERROR	<p>Events of this type occur when Administration Server fails to poll a network segment in a cloud environment (see section "Network segment polling" on page 865).</p> <p>Read the details in the event description and respond accordingly.</p>	Not stored
Failed to copy the updates to the specified folder	4123	KLSRV_UPD_REPL_FAIL	<p>Events of this type occur when software updates are copied to an additional shared folder(s). You can respond to the event in the following ways:</p> <ul style="list-style-type: none"> • Check whether the user account that is employed to gain access to the folder(s) has write permission. • Check whether a user name and/or a password to the folder(s) changed. • Check the Internet connection, as it might be the cause of the event. Follow the instructions to update databases and software modules (see section "Creating the task for downloading updates to the repository of the Administration Server" on page 413). 	180 days
No free disk space	4107	KLSRV_DISK_FULL	<p>Events of this type occur when the hard drive of the device on which Administration Server is installed runs out of free space.</p> <p>Free up disk space on the device.</p>	180 days

Event type display name	Event type ID	Event type	Description	Default storage term
Shared folder is not available	4108	KLSRV_SHARED_FOLDER_UNAVAILABLE	<p>Events of this type occur if the shared folder of Administration Server (see section "Defining a shared folder" on page 224) is not available.</p> <p>You can respond to the event in the following ways:</p> <ul style="list-style-type: none"> • Check whether the Administration Server (where the shared folder is located) is turned on and available. • Check whether a user name and/or a password to the folder is/are changed. • Check the network connection. 	180 days
The Administration Server database is unavailable	4109	KLSRV_DATABASE_UNAVAILABLE	<p>Events of this type occur if the Administration Server database becomes unavailable.</p> <p>You can respond to the event in the following ways:</p> <ul style="list-style-type: none"> • Check whether the remote server that has SQL Server installed is available. • View the DBMS logs to discover the reason for Administration Server database unavailability. For example, because of preventive maintenance a remote server with SQL Server installed might be unavailable. 	180 days

<p>No free space in the Administration Server database</p>	<p>411 0</p>	<p>KLSRV_DATABASE _FULL</p>	<p>Events of this type occur when there is no free space in the Administration Server database. Administration Server does not function when its database has reached its capacity and when further recording to the database is not possible.</p> <p>Following are the causes of this event, depending on the DBMS that you use, and appropriate responses to the event:</p> <ul style="list-style-type: none"> • You use the SQL Server Express Edition DBMS: <ul style="list-style-type: none"> • In the SQL Server Express documentation, review the database size limit for the version you use. Probably your Administration Server database has exceeded the database size limit. • Limit the number of events to store in the Administration Server database (see section "Setting the maximum number of events in the event repository" on page 1008). • In the Administration Server database there are too many events sent by the Application Control component. You can change the settings of the Kaspersky Endpoint Security for Windows policy relating to Application Control event storage in the Administration Server database. • You use a DBMS other than SQL Server Express Edition: <ul style="list-style-type: none"> • Do not limit the number of events to store in the Administration Server database (see section 	<p>180 days</p>
---	------------------	---------------------------------	--	---------------------

Event type display name	Event type ID	Event type	Description	Default storage term
			<p>"Setting the maximum number of events in the event repository" on page 1008.</p> <ul style="list-style-type: none"> Reduce the list of events to store in the Administration Server database (see section "Setting the storage term for an event" on page 1305). <p>Review the information on DBMS selection (see section "Selecting a DBMS" on page 129).</p>	

See also:

Administration Server critical events	538
Administration Server informational events	566
Administration Server warning events	552
Events in Kaspersky Security Center	792

Administration Server warning events

The table below shows the events of Kaspersky Security Center Administration Server that have the **Warning** severity level.

Table 89. Administration Server warning events

Event type display name	Event type ID	Event type	Description	Default storage term
<p>License limit has been exceeded</p>	<p>4098</p>	<p>KLSRV_EV_LICENSE_CHECK_100_110</p>	<p>Once a day Kaspersky Security Center checks whether a licensing restriction is exceeded.</p> <p>Events of this type occur when Administration Server detects that some licensing limits are exceeded by Kaspersky applications installed on client devices and if the number of currently used licensing units (see section "About the license certificate" on page 319) covered by a single license constitute 100% to 110% of the total number of units covered by the license.</p> <p>Even when this event occurs, client devices are protected.</p> <p>You can respond to the event in the following ways:</p> <ul style="list-style-type: none"> • Look through the managed devices list. Delete devices that are not in use. • Provide a license for more devices (add a valid activation code or a key file to Administration Server). <p>Kaspersky Security Center determines the rules to generate events (see section "Events of the licensing limit exceeded" on page 329) when a licensing restriction is exceeded.</p>	<p>90 days</p>

Event type display name	Event type ID	Event type	Description	Default storage term
<p>Device has remained inactive on the network for a long time</p>	<p>4103</p>	<p>KLSRV_EVENT_HOSTS_NOT_VISIBLE</p>	<p>Events of this type occur when a managed device shows inactivity for some time.</p> <p>Most often, this happens when a managed device is decommissioned.</p> <p>You can respond to the event in the following ways:</p> <ul style="list-style-type: none"> • Manually remove the device from the list of managed devices. • Specify the time interval after which the Device has remained inactive on the network for a long time event is created by using Administration Console (see section "Viewing and configuring the actions when devices show inactivity" on page 586) or by using Kaspersky Security Center 13 Web Console (see section "Viewing and configuring the actions when devices show inactivity" on page 1098). • Specify the time interval after which the device is automatically removed from the group by using Administration Console (see section "Viewing and configuring the actions when devices show inactivity" on page 586) or by using Kaspersky Security Center 13 Web Console (see section "Viewing and configuring the actions when devices show inactivity" on page 1098). 	<p>90 days</p>

Event type display name	Event type ID	Event type	Description	Default storage term
Conflict of device names	4102	KLSRV_EVENT_HOSTS_CONFLICT	<p>Events of this type occur when Administration Server considers two or more managed devices as a single device.</p> <p>Most often this happens when a cloned hard drive was used for software deployment on managed devices and without switching the Network Agent to the dedicated disk cloning mode on a reference device.</p> <p>To avoid this issue, switch Network Agent to the disk cloning mode (see section "Network Agent disk cloning mode" on page 889) on a reference device before cloning the hard drive of this device.</p>	90 days
Device status is Warning	4114	KLSRV_HOST_STATUS_WARNING	<p>Events of this type occur when a managed device is assigned the <i>Warning</i> status. You can configure the conditions (see section "Configuring the switching of device statuses" on page 647) under which the device status is changed to <i>Warning</i>.</p>	90 days

Event type display name	Event type ID	Event type	Description	Default storage term
<p>Limit of installations will soon be exceeded for one of the licensed applications groups</p>	<p>4127</p>	<p>KLSRV_INVLICPROD_FILLED</p>	<p>Events of this type occur when the number of installations for third-party applications included in a licensed applications group (see section "Groups of applications" on page 485) reaches 90% of the maximum allowed value specified in the license key properties (see section "Managing license keys for licensed applications groups" on page 499).</p> <p>You can respond to the event in the following ways:</p> <ul style="list-style-type: none"> • If the third-party application is not in use on some of the managed devices, delete the application from these devices. • If you expect that the number of installations for the third-party application will exceed the allowed maximum in the near future, consider obtaining a third-party license for a greater number of devices in advance. <p>You can manage license keys of third-party applications (see section "Managing license keys for licensed applications groups" on page 499) using the functionality of licensed applications groups.</p>	<p>90 days</p>

Event type display name	Event type ID	Event type	Description	Default storage term
<p>Certificate has been requested</p>	<p>4133</p>	<p>KLSRV_CERTIFICATE_REQUESTED</p>	<p>Events of this type occur when a certificate for Mobile Device Management fails to be automatically reissued.</p> <p>Following might be the causes and appropriate responses to the event:</p> <ul style="list-style-type: none"> • Automatic reissue was initiated for a certificate for which the Reissue certificate automatically if possible option (see section "Configuring certificate issuance rules" on page 742) is disabled. This might be due to an error that occurred during creation of the certificate. Manual reissue of the certificate might be required. • If you use an integration with a public key infrastructure (see section "Integration with public key infrastructure" on page 743), the cause might be a missing SAM-Account-Name attribute of the account used for integration with PKI and for issuance of the certificate. Review the account properties. 	<p>90 days</p>

Event type display name	Event type ID	Event type	Description	Default storage term
Certificate has been removed	4134	KLSRV_CERTIFICATE_REMOVED	<p>Events of this type occur when an administrator removes any type of certificate (General, Mail, VPN) for Mobile Device Management.</p> <p>After removing a certificate, mobile devices connected via this certificate will fail to connect to Administration Server.</p> <p>This event might be helpful when investigating malfunctions associated with the management of mobile devices.</p>	90 days
APNs certificate has expired	4135	KLSRV_APN_CERTIFICATE_EXPIRED	<p>Events of this type occur when an APNs certificate expires.</p> <p>You need to manually renew the APNs certificate (see section "Renewing an APNs certificate" on page 203) and install it on an iOS MDM Server (see section "Installing an APNs certificate on an iOS MDM Server" on page 205).</p>	Not stored
APNs certificate expires soon	4136	KLSRV_APN_CERTIFICATE_EXPIRES_SOON	<p>Events of this type occur when there are fewer than 14 days left before the APNs certificate expires.</p> <p>When the APNs certificate expires, you need to manually renew the APNs certificate (see section "Renewing an APNs certificate" on page 203) and install it on an iOS MDM Server (see section "Installing an APNs certificate on an iOS MDM Server" on page 205).</p> <p>We recommend that you schedule the APNs certificate renewal in advance of the expiration date.</p>	Not stored

Event type display name	Event type ID	Event type	Description	Default storage term
Failed to send the FCM message to the mobile device	4138	KLSRV_GCM_DEVICE_ERROR	<p>Events of this type occur when Mobile Device Management is configured to use Google Firebase Cloud Messaging (FCM) (see section "Using Google Firebase Cloud Messaging" on page 735) for connecting to managed mobile devices with an Android operating system and FCM Server fails to handle some of the requests received from Administration Server. It means that some of the managed mobile devices will not receive a push notification.</p> <p>Read the HTTP code in the details of the event description and respond accordingly. For more information on the HTTP codes received from FCM Server and related errors, please refer to the Google Firebase service documentation https://firebase.google.com/docs/cloud-messaging/http-server-ref (see chapter "Downstream message error response codes").</p>	90 days

Event type display name	Event type ID	Event type	Description	Default storage term
HTTP error sending the FCM message to the FCM server	4139	KLSRV_GCM_HTTP_ERROR	<p>Events of this type occur when Mobile Device Management is configured to use Google Firebase Cloud Messaging (FCM) (see section "Using Google Firebase Cloud Messaging" on page 735) for connecting managed mobile devices with the Android operating system and FCM Server reverts to the Administration Server a request with a HTTP code other than 200 (OK).</p> <p>Following might be the causes and appropriate responses to the event:</p> <ul style="list-style-type: none"> • Problems on the FCM server side. Read the HTTP code in the details of the event description and respond accordingly. For more information on the HTTP codes received from FCM Server and related errors, please refer to the Google Firebase service documentation https://firebase.google.com/docs/cloud-messaging/http-server-ref (see chapter "Downstream message error response codes"). • Problems on the proxy server side (if you use proxy server). Read the HTTP code in the details of the event and respond accordingly. 	90 days

Event type display name	Event type ID	Event type	Description	Default storage term
Failed to send the FCM message to the FCM server	4140	KLSRV_GCM_GENERAL_ERROR	<p>Events of this type occur due to unexpected errors on the Administration Server side when working with the Google Firebase Cloud Messaging HTTP protocol.</p> <p>Read the details in the event description and respond accordingly.</p> <p>If you cannot find the solution to an issue on your own, we recommend that you contact Kaspersky Technical Support.</p>	90 days
Little free space on the hard drive	4105	KLSRV_NO_SPACE_ON_VOLUMES	<p>Events of this type occur when the hard drive of the device on which Administration Server is installed almost runs out of free space.</p> <p>Free up disk space on the device.</p>	90 days

<p>Little free space in the Administration Server database</p>	<p>41 06</p>	<p>KLSRV_NO_SPACE_IN_DATABASE</p>	<p>Events of this type occur if space in the Administration Server database is too limited. If you do not remedy the situation, soon the Administration Server database will reach its capacity and Administration Server will not function.</p> <p>Following are the causes of this event, depending on the DBMS that you use, and the appropriate responses to the event.</p> <p>You use the SQL Server Express Edition DBMS:</p> <ul style="list-style-type: none"> • In SQL Server Express documentation, review the database size limit for the version you use. Probably your Administration Server database is about to reach the database size limit. • Limit the number of events to store in the Administration Server database (see section "Setting the maximum number of events in the event repository" on page 1008). • In the Administration Server database there are too many events sent by the Application Control component. You can change the settings of the Kaspersky Endpoint Security for Windows policy relating to Application Control event storage in the Administration Server database. <p>You use a DBMS other than SQL Server Express Edition:</p> <ul style="list-style-type: none"> • Do not limit the number of events to store in the Administration Server database (see section "Setting the maximum number of events in the 	<p>90 days</p>
---	------------------	-----------------------------------	---	--------------------

Event type display name	Event type ID	Event type	Description	Default storage term
			<p>event repository" on page 1008)</p> <ul style="list-style-type: none"> • Reduce the list of events to store in the Administration Server database (see section "Setting the storage term for an event" on page 1305) <p>Review the information on DBMS selection (see section "Selecting a DBMS" on page 129).</p>	
<p>Connection to the secondary Administration Server has been interrupted</p>	<p>4116</p>	<p>KLSRV_EV_SLAVE_SRV_DISCONNECTED</p>	<p>Events of this type occur when a connection to the secondary Administration Server is interrupted.</p> <p>Read the Kaspersky Event Log on the device where the secondary Administration Server is installed and respond accordingly.</p>	<p>90 days</p>
<p>Connection to the primary Administration Server has been interrupted</p>	<p>4118</p>	<p>KLSRV_EV_MASTER_SRV_DISCONNECTED</p>	<p>Events of this type occur when a connection to the primary Administration Server is interrupted.</p> <p>Read the Kaspersky Event Log on the device where the primary Administration Server is installed and respond accordingly.</p>	<p>90 days</p>

Event type display name	Event type ID	Event type	Description	Default storage term
New updates for Kaspersky software modules have been registered	41 41	KLSRV_SEAMLESS_UPDATE_REGISTERED	<p>Events of this type occur when Administration Server registers new updates for the Kaspersky software installed on managed devices that require approval to be installed.</p> <p>Approve or decline the updates by using Administration Console (see section "Approving and declining software updates" on page 435) or using Kaspersky Security Center Web Console (see section "Approving and declining software updates" on page 1197).</p>	90 days
Deletion of events from the database has started because the limit on the number of events was exceeded	41 45	KLSRV_EVP_DB_TRUNCATING	<p>Events of this type occur when deletion of old events from the Administration Server database has started after the Administration Server database capacity is reached (see section "Event processing and storage on the Administration Server" on page 610).</p> <p>You can respond to the event in the following ways:</p> <ul style="list-style-type: none"> • Change the maximum number of events stored in the Administration Server database (see section "Setting the maximum number of events in the event repository" on page 1008) • Reduce the list of events to store in the Administration Server database (see section "Setting the storage term for an event" on page 1305) 	Not stored

Event type display name	Event type ID	Event type	Description	Default storage term
Events have been deleted from the database because the limit on the number of events was exceeded	41 46	KLSRV_EVP_DB_TRUNCATED	<p>Events of this type occur when old events have been deleted from the Administration Server database after the Administration Server database capacity is reached (see section "Event processing and storage on the Administration Server" on page 610).</p> <p>You can respond to the event in the following ways:</p> <ul style="list-style-type: none"> • Change the allowed maximum number of events to be stored in the Administration Server database (see section "Setting the maximum number of events in the event repository" on page 1008) • Reduce the list of events to store in the Administration Server database (see section "Setting the storage term for an event" on page 1305) 	Not stored

See also:

Administration Server critical events	538
Administration Server functional failure events	543
Administration Server informational events	566
Events in Kaspersky Security Center	792

Administration Server informational events

The table below shows the events of Kaspersky Security Center Administration Server that have the **Info** severity level.

Table 90. Administration Server informational events

Event type display name	Event type ID	Event type	Default storage term
Over 90% of the license key is used up	4097	KLSRV_EV_LICENSE_CHECK_90	30 days
New device has been detected	4100	KLSRV_EVENT_HOSTS_NEW_DETECTED	30 days
Device has been automatically added to the group	4101	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	30 days
Device has been removed from the group: inactive on the network for a long time	4104	KLSRV_INVISIBLE_HOSTS_REMOVED	30 days
Limit of installations will soon be exceeded (more than 95% is used up) for one of the licensed applications groups	4128	KLSRV_INVLICPROD_EXPIRED_SOON	30 days
Files have been found to send to Kaspersky for analysis	4131	KLSRV_APS_FILE_APPEARED	30 days
FCM Instance ID has changed on this mobile device	4137	KLSRV_GCM_DEVICE_REGID_CHANGED	30 days
Updates have been successfully copied to the specified folder	4122	KLSRV_UPD_REPL_OK	30 days
Connection to the secondary Administration Server has been established	4115	KLSRV_EV_SLAVE_SRV_CONNECTED	30 days
Connection to the primary Administration Server has been established	4117	KLSRV_EV_MASTER_SRV_CONNECTED	30 days
Databases have been updated	4144	KLSRV_UPD_BASES_UPDATED	30 days
Audit: Connection to the Administration Server has been established	4147	KLAUD_EV_SERVERCONNECT	30 days
Audit: Object has been modified	4148	KLAUD_EV_OBJECTMODIFY	30 days
Audit: Object status has changed	4150	KLAUD_EV_TASK_STATE_CHANGED	30 days
Audit: Group settings have been modified	4149	KLAUD_EV_ADMGROUP_CHANGED	30 days
Audit: Connection to Administration Server has been terminated	4151	KLAUD_EV_SERVERDISCONNECT	30 days
Audit: Object properties have been modified	4152	KLAUD_EV_OBJECTPROPMODIFIED	30 days
Audit: User permissions have been modified	4153	KLAUD_EV_OBJECTACLMODIFIED	30 days

Network Agent events

This section contains information about the events related to Network Agent.

In this section

Network Agent functional failure events	1340
Network Agent warning events	1342
Network Agent informational events	1342

Network Agent functional failure events

The table below shows the events of Kaspersky Security Center Network Agent that have the **Functional failure** severity level.

Table 91. Network Agent functional failure events

Event type display name	Event type ID	Event type	Description	Default storage term
Update installation error	7702	KLNAG_EV_PATCH_INSTALL_ERROR	<p>Events of this type occur if automatic updating and patching for Kaspersky Security Center components (on page 457) was not successful. The event does not concern updates of the managed Kaspersky applications.</p> <p>Read the event description. A Windows issue on the Administration Server might be a reason for this event. If the description mentions any issue of Windows configuration, resolve this issue.</p>	30 days
Failed to install the third-party software update	7697	KLNAG_EV_3P_PATCH_INSTALL_ERROR	<p>Events of this type occur if Vulnerability and Patch Management and Mobile Device Management features (see section "Kaspersky Security Center licensing options" on page 320) are in use, and if update of third-party software (see section "Installation of third-party software updates" on page 432) was not successful.</p> <p>Check whether the link to the third-party software is valid. Read the event description.</p>	30 days
Failed to install the Windows Update updates	7717	KLNAG_EV_WUA_INSTALL_ERROR	<p>Events of this type occur if Windows Updates were not successful. Configure Windows Updates in a Network Agent policy (see section "Configuring Windows updates in a Network Agent policy" on page 455).</p> <p>Read the event description. Look for the error in the Microsoft Knowledge Base. Contact Microsoft Technical Support if you cannot resolve the issue yourself.</p>	30 days

See also:

Network Agent warning events.....	571
Network Agent informational events.....	572

Network Agent warning events

The table below shows the events of Kaspersky Security Center Network Agent that have the **Warning** severity level.

Table 92. Network Agent warning events

Event type display name	Event type ID	Event type	Default storage term
Warning has been returned during installation of the software module update	7701	KLNAG_EV_PATCH_INSTALL_WARNING	30 days
Third-party software update installation has completed with a warning	7696	KLNAG_EV_3P_PATCH_INSTALL_WARNING	30 days
Third-party software update installation has been postponed	7698	KLNAG_EV_3P_PATCH_INSTALL_SLIPPED	30 days
Incident has occurred	549	GNRL_EV_APP_INCIDENT_OCURED	30 days
KSN Proxy has started. Failed to check KSN for availability	7718	KSNPROXY_STARTED_CON_CHK_FAILED	30 days

See also:

Network Agent functional failure events	568
Network Agent informational events.....	572

Network Agent informational events

The table below shows the events of Kaspersky Security Center Network Agent that have the **Info** severity level.

Table 93. Network Agent informational events

Event type display name	Event type ID	Event type	Default storage term
Update for software modules has been installed successfully	7699	KLNAG_EV_PATCH_INSTALLED_SUCCESSFULLY	30 days
Installation of the software module update has started	7700	KLNAG_EV_PATCH_INSTALL_STARTING	30 days
Application has been installed	7703	KLNAG_EV_INV_APP_INSTALLED	30 days
Application has been uninstalled	7704	KLNAG_EV_INV_APP_UNINSTALLED	30 days
Monitored application has been installed	7705	KLNAG_EV_INV_OBS_APP_INSTALLED	30 days
Monitored application has been uninstalled	7706	KLNAG_EV_INV_OBS_APP_UNINSTALLED	30 days
Third-party application has been installed	7707	KLNAG_EV_INV_CMPTR_APP_INSTALLED	30 days
New device has been added	7708	KLNAG_EV_DEVICE_ARRIVAL	30 days
Device has been removed	7709	KLNAG_EV_DEVICE_REMOVE	30 days
New device has been detected	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30 days
Device has been authorized	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	30 days
Windows Desktop Sharing: File has been read	7712	KLUSRLOG_EV_FILE_READ	30 days
Windows Desktop Sharing: File has been modified	7713	KLUSRLOG_EV_FILE_MODIFIED	30 days
Windows Desktop Sharing: Application has been started	7714	KLUSRLOG_EV_PROCESS_LAUNCHED	30 days
Windows Desktop Sharing: Started	7715	KLUSRLOG_EV_WDS_BEGIN	30 days
Windows Desktop Sharing: Stopped	7716	KLUSRLOG_EV_WDS_END	30 days
Third-party software update has been installed successfully	7694	KLNAG_EV_3P_PATCH_INSTALLED_SUCCESSFULLY	30 days
Third-party software update installation has started	7695	KLNAG_EV_3P_PATCH_INSTALL_STARTING	30 days
KSN Proxy has started. KSN availability check has completed successfully	7719	KSNPROXY_STARTED_CON_CHK_OK	30 days
KSN Proxy has stopped	7720	KSNPROXY_STOPPED	30 days

See also:

Network Agent functional failure events	568
Network Agent warning events	571

iOS MDM Server events

This section contains information about the events related to iOS MDM Server.

In this section

iOS MDM Server functional failure events.....	1344
iOS MDM Server warning events	1347
iOS MDM Server informational events	1347

iOS MDM Server functional failure events

The table below shows the events of Kaspersky Security Center iOS MDM Server that have the **Functional failure** severity level.

Table 94. *iOS MDM Server functional failure events*

Event type display name	Event type ID	Event type	Default storage term
Failed to request the list of profiles.		PROFILELIST_COMMAND_FAILED	30 days
Failed to install the profile.		INSTALLPROFILE_COMMAND_FAILED	30 days
Failed to remove the profile.		REMOVEPROFILE_COMMAND_FAILED	30 days
Failed to request the list of provisioning profiles.		PROVISIONINGPROFILELIST_COMMAND_FAILED	30 days
Failed to install provisioning profile.		INSTALLPROVISIONINGPROFILE_COMMAND_FAILED	30 days
Failed to remove the provisioning profile.		REMOVEPROVISIONINGPROFILE_COMMAND_FAILED	30 days
Failed to request the list of digital certificates.		CERTIFICATELIST_COMMAND_FAILED	30 days
Failed to request the list of installed applications.		INSTALLEDAPPLICATIONLIST_COMMAND_FAILED	30 days
Failed to request general information about the mobile device.		DEVICEINFORMATION_COMMAND_FAILED	30 days
Failed to request security information.		SECURITYINFO_COMMAND_FAILED	30 days
Failed to lock the mobile device.		DEVICELOCK_COMMAND_FAILED	30 days
Failed to reset the password.		CLEARPASSCODE_COMMAND_FAILED	30 days
Failed to wipe data from the mobile device.		ERASEDEVICE_COMMAND_FAILED	30 days
Failed to install the app.		INSTALLAPPLICATION_COMMAND_FAILED	30 days
Failed to set the redemption code for the app.		APPLYREDEMPTIONCODE_COMMAND_FAILED	30 days
Failed to request the list of managed apps.		MANAGEDAPPLICATIONLIST_COMMAND_FAILED	30 days
Failed to remove the managed app.		REMOVEAPPLICATION_COMMAND_FAILED	30 days
Roaming settings have been rejected.		SETROAMINGSETTINGS_COMMAND_FAILED	30 days
Error has occurred in the app operation.		PRODUCT_FAILURE	30 days

Event type display name	Event type ID	Event type	Default storage term
Command result contains invalid data.		MALFORMED_COMMAND	30 days
Failed to send the push notification.		SEND_PUSH_NOTIFICATION_FAILED	30 days
Failed to send the command.		SEND_COMMAND_FAILED	30 days
Device not found.		DEVICE_NOT_FOUND	30 days

iOS MDM Server warning events

The table below shows the events of Kaspersky Security Center iOS MDM Server that have the **Warning** severity level.

Table 95. iOS MDM Server warning events

Event type display name	Event type ID	Event type	Default storage term
Attempt to connect a locked mobile device has been detected.		INACTICE_DEVICE_TRY_CONNECTED	30 days
Profile has been removed.		MDM_PROFILE_WAS_REMOVED	30 days
Attempt to re-use a client certificate has been detected.		CLIENT_CERT_ALREADY_IN_USE	30 days
Inactive device has been detected.		FOUND_INACTIVE_DEVICE	30 days
Redemption code is required.		NEED_REDEMPTION_CODE	30 days
Profile has been included in a policy removed from the device.		UMDM_PROFILE_WAS_REMOVED	30 days

iOS MDM Server informational events

The table below shows the events of Kaspersky Security Center iOS MDM Server that have the **Info** severity level.

Table 96. *iOS MDM Server informational events*

Event type display name	Event type ID	Event type	Default storage term
New mobile device has been connected.		NEW_DEVICE_CONNECTED	30 days
List of profiles has been successfully requested.		PROFILELIST_COMMAND_SUCCESSFULL	30 days
Profile has been successfully installed.		INSTALLPROFILE_COMMAND_SUCCESSFULL	30 days
Profile has been successfully removed.		REMOVEPROFILE_COMMAND_SUCCESSFULL	30 days
List of provisioning profiles has been successfully requested.		PROVISIONINGPROFILELIST_COMMAND_SUCCESSFULL	30 days
Provisioning profile has been successfully installed.		INSTALLPROVISIONINGPROFILE_COMMAND_SUCCESSFULL	30 days
Provisioning profile has been successfully removed.		REMOVEPROVISIONINGPROFILE_COMMAND_SUCCESSFULL	30 days
List of digital certificates has been successfully requested.		CERTIFICATELIST_COMMAND_SUCCESSFULL	30 days
List of installed applications has been successfully requested.		INSTALLEDAPPLICATIONLIST_COMMAND_SUCCESSFULL	30 days
General information about the mobile device has been successfully requested.		DEVICEINFORMATION_COMMAND_SUCCESSFULL	30 days
Security information has been successfully requested.		SECURITYINFO_COMMAND_SUCCESSFULL	30 days
Mobile device has been successfully locked.		DEVICELOCK_COMMAND_SUCCESSFULL	30 days
The password has been successfully reset.		CLEARPASSCODE_COMMAND_SUCCESSFULL	30 days
Data has been wiped from the mobile device.		ERASEDEVICE_COMMAND_SUCCESSFULL	30 days
App has been successfully installed.		INSTALLAPPLICATION_COMMAND_SUCCESSFULL	30 days
Redemption code has been successfully set for the app.		APPLYREDEMPTIONCODE_COMMAND_SUCCESSFULL	30 days
The list of managed apps has been successfully requested.		MANAGEDAPPLICATIONLIST_COMMAND_SUCCESSFULL	30 days
Managed app has been removed successfully.		REMOVEAPPLICATION_COMMAND_SUCCESSFULL	30 days

Event type display name	Event type ID	Event type	Default storage term
Roaming settings have been successfully applied.		SETROAMINGSETTINGS_COM MAND_SUCCESSFUL	30 days

Exchange Mobile Device Server events

This section contains information about the events related to Exchange Mobile Device Server.

In this section

Exchange Mobile Device Server functional failure events	1350
Exchange Mobile Device Server informational events	1351

Exchange Mobile Device Server functional failure events

The table below shows the events of Kaspersky Security Center Exchange Mobile Device Server that have the **Functional failure** severity level.

Table 97. Exchange Mobile Device Server functional failure events

Event type display name	Event type ID	Event type	Default storage term
Failed to wipe data from the mobile device.		WIPE_FAILED	30 days
Cannot delete information about mobile device connection to mailbox.		DEVICE_REMOVE_FAILED	30 days
Failed to apply the ActiveSync policy to the mailbox.		POLICY_APPLY_FAILED	30 days
Application operation error.		PRODUCT_FAILURE	30 days
Failed to modify the state of ActiveSync functionality.		CHANGE_ACTIVE_SYNC_STATE_FAILED	30 days

Exchange Mobile Device Server informational events

The table below shows the events of Kaspersky Security Center Exchange Mobile Device Server that have the **Info** severity level.

Table 98. Exchange Mobile Device Server informational events

Event type display name	Event type ID	Event type	Default storage term
New mobile device has connected.		NEW_DEVICE_CONNECTED	30 days
Data has been wiped from the mobile device.		WIPE_SUCCESSFULL	30 days

Blocking frequent events

This section provides information about managing frequent events blocking and about removing blocking of frequent events.

In this section

About blocking frequent events	1351
Managing frequent events blocking	1352
Removing blocking of frequent events	1352

About blocking frequent events

A managed application, for example, Kaspersky Endpoint Security for Windows, installed on a single or several managed devices can send a lot of events of the same type to the Administration Server. Receiving frequent events may overload the Administration Server database and overwrite other events. Administration Server starts blocking the most frequent events when the number of all the received events exceeds the specified limit for the database (see section "Setting the maximum number of events in the event repository" on page [1008](#)).

Administration Server blocks the frequent events from receiving automatically. You cannot block the frequent events yourself, or choose which events to block.

If you want to find out if an event is blocked, you can view the notification list or you can see if this event is present in the **Blocking frequent events** section of the Administration Server properties. If the event is blocked, you can do the following:


- If you want to prevent overwriting the database, you can continue blocking (see section "Managing frequent events blocking" on page [1352](#)) such type of events from receiving.

- If you want, for example, to find the reason of sending the frequent events to the Administration Server you can unblock (see section "Managing frequent events blocking" on page [1352](#)) frequent events and continue receiving the events of this type anyway.
- If you want to continue receiving the frequent events until they become blocked again, you can remove from blocking (see section "Removing blocking of frequent events" on page [1352](#)) the frequent events.

Managing frequent events blocking

Administration Server blocks the automatic receiving of frequent events, but you can unblock and continue to receive frequent events. You can also block receiving frequent events that you unblocked before.

► *To manage frequent events blocking:*


1. In the main application window, click the **Settings** icon () next to the name of the required Administration Server.
The Administration Server properties window opens.
2. On the **General** tab, select the **Blocking frequent events** section.
3. In the **Blocking frequent events** section:
 - If you want to unblock the receiving of frequent events:
 - a. Select the frequent events you want to unblock, and then click the **Exclude** button.
 - b. Click the **Save** button.
 - If you want to block receiving frequent events:
 - a. Select the frequent events you want to block, and then click the **Block** button.
 - b. Click the **Save** button.

Administration Server receives the unblocked frequent events and does not receive the blocked frequent events.

Removing blocking of frequent events

You can remove blocking for frequent events and start receiving them until Administration Server blocks these frequent events again.

► *To remove blocking for frequent events:*

1. In the main application window, click the **Settings** icon () next to the name of the required Administration Server.
The Administration Server properties window opens.
2. On the **General** tab, select the **Blocking frequent events** section.
3. In the **Blocking frequent events** section, select the frequent event types for which you want to remove blocking.
4. Click the **Remove from blocking** button.

The frequent event is removed from the list of frequent events. Administration Server will receive events of this type.

Device selections

Device selections are a tool for filtering devices according to specific conditions. You can use device selections to manage several devices: for example, to view a report about only these devices or to move all of these devices to another group.

Kaspersky Security Center provides a broad range of *predefined selections* (for example, **Devices with Critical status, Protection is disabled, Active threats are detected**). Predefined selections cannot be deleted. You can also create and configure additional *user-defined selections*.

In user-defined selections, you can set the search scope and select all devices, managed devices, or unassigned devices. Search parameters are specified in the conditions. In the device selection you can create several conditions with different search parameters. For example, you can create two conditions and specify different IP ranges in each of them. If several conditions are specified, a selection displays the devices that meet any of the conditions. By contrast, search parameters within a condition are superimposed. If both an IP range and the name of an installed application are specified in a condition, only those devices will be displayed where both the application is installed and the IP address belongs to the specified range.

► *To view the device selection:*

1. Go to **DEVICES** → **DEVICE SELECTIONS** or **DISCOVERY & DEPLOYMENT** → **DEVICE SELECTIONS** section.
2. In the selection list, click the name of the relevant selection.

The device selection result is displayed.

See also:

Using event selections.....	1289
Scenario: Installation and initial setup of Kaspersky Security Center 13 Web Console	962

Creating a device selection

► *To create a device selection:*

1. Go to **DEVICES** → **DEVICE SELECTIONS**.
A page with a list of device selections is displayed.
2. Click the **Add** button.
The **Device selection settings** window opens.
3. Enter the name of the new selection.
4. Specify the type of the devices that you want to include in the device selection.
5. Click the **Add** button.
6. In the window that opens, specify conditions (see section "Configuring a device selection" on page [1354](#)) that must be met for including devices in this selection, and then click the **OK** button.
7. Click the **Save** button.

The device selection is created and added to the list of device selections.

Configuring a device selection

► *To configure a device selection:*

1. Go to **DEVICES** → **DEVICE SELECTIONS**.
A page with a list of device selections is displayed.
2. Click the relevant user-defined device selection.
The **Device selection settings** window opens.
3. On the **General** tab, specify conditions that must be met for including devices in this selection.
4. Click the **Save** button.

The settings are applied and saved.

Below are descriptions of the conditions for assigning devices to a selection. Conditions are combined by using the OR logical operator: the selection will contain devices that comply with at least one of the listed conditions.

General

In the **General** section, you can change the name of the selection condition and specify whether that condition must be inverted:

- **Invert selection condition**

If this check box is selected, the specified selection condition will be inverted. The selection will include all devices that do not meet the condition.

By default, this check box is cleared.

Network

In the **Network** section, you can specify the criteria that will be used to include devices in the selection according to their network data:

- **Device name or IP address**

Name of the device in the Windows network (NetBIOS name).

- **Windows domain**

Displays all devices included in the specified Windows domain.

- **Administration group**

Displays devices included in the specified administration group.

- **Description**

Text in the device properties window: In the **Description** field of the **General** section.

To describe text in the **Description** field, you can use the following characters:

- Within a word:
 - *. Replaces any string with any number of characters.

Example:

To describe words such as **Server** or **Server's**, you can enter **Server***.

- ?. Replaces any single character.

Example:

To describe words such as **Window** or **Windows**, you can enter **Windo?**.

Asterisk (*) or question mark (?) cannot be used as the first character in the query.

- To find several words:
 - Space. You will see all devices whose descriptions contain any of the listed words.

Example:

To find a phrase that contains **Secondary** or **Virtual** words, you can include **Secondary Virtual** line in your query.

- +. When a plus sign precedes a word, all search results will contain this word.

Example:

To find a phrase that contains both **Secondary** and **Virtual**, enter the **+Secondary+Virtual** query.

- -. When a minus sign precedes a word, no search results will contain this word.

Example:

To find a phrase that contains **Secondary** and does not contain **Virtual**, enter the **+Secondary-Virtual** query.

- "<some text>". Text enclosed in quotation marks must be present in the text.

Example:

To find a phrase that contains **Secondary Server** word combination, you can enter "**Secondary Server**" in the query.

- **IP range**

If this check box is selected, you can enter the initial and final IP addresses of the IP range in which the relevant devices must be included.

By default, this check box is cleared.

Tags

In the **Tags** section, you can configure criteria for including devices into a selection based on key words (tags) that were previously added to the descriptions of managed devices:

- **Apply if at least one specified tag matches**

If this check box is selected, the search results will show devices with descriptions that contain at least one of the selected tags.

If this check box is cleared, the search results will only show devices with descriptions that contain all the selected tags.

By default, this check box is cleared.

- **Tag must be included**

If this option is selected, the search results will display the devices whose descriptions contain the selected tag. To find devices, you can use the asterisk, which stands for any string with any number of characters.

By default, this option is selected.

- **Tag must be excluded**

If this option is selected, the search results will display the devices whose descriptions do not contain the selected tag. To find devices, you can use the asterisk, which stands for any string with any number of characters.

Active Directory

In the **Active Directory** section, you can configure criteria for including devices into a selection based on their Active Directory data:

- **Device is in an Active Directory organizational unit**

If this check box is selected, the selection includes devices from the Active Directory unit specified in the entry field.

By default, this check box is cleared.

- **Include child organizational units**

If this check box is selected, the selection includes devices from all child OUs of the specified Active Directory OU.

By default, this check box is cleared.

- **This device is a member of an Active Directory group**

If this check box is selected, the selection includes devices from the Active Directory group specified in the entry field.

By default, this check box is cleared.

Network activity

In the **Network activity** section, you can specify the criteria that will be used to include devices in the selection according to their network activity:

- **This device is a distribution point**

In the drop-down list, you can set up the criterion for including devices in the selection when performing search:

- **Yes.** The selection includes devices that act as distribution points.
- **No.** Devices that act as distribution points are not included in the selection.
- **No value is selected.** The criterion will not be applied.

- **Do not disconnect from the Administration Server**

In the drop-down list, you can set up the criterion for including devices in the selection when performing search:

- **Enabled.** The selection will include devices on which the **Do not disconnect from the Administration Server** check box is selected.
- **Disabled.** The selection will include devices on which the **Do not disconnect from**

the **Administration Server** check box is cleared.

- **No value is selected.** The criterion will not be applied.

- **Connection profile switched**

In the drop-down list, you can set up the criterion for including devices in the selection when performing search:

- **Yes.** The selection will include devices that connected to the Administration Server after the connection profile was switched.
- **No.** The selection will not include devices that connected to the Administration Server after the connection profile was switched.
- **No value is selected.** The criterion will not be applied.

- **Last connected to Administration Server**

You can use this check box to set a search criterion for devices according to the time they last connected to the Administration Server.

If this check box is selected, in the entry fields you can specify the time interval (date and time) during which the last connection was established between Network Agent installed on the client device and the Administration Server. The selection will include devices that fall within the specified interval.

If this check box is cleared, the criterion will not be applied.

By default, this check box is cleared.

- **New devices detected by network poll**

Searches for new devices that have been detected by network polling over the last few days.

If this check box is selected, the selection only includes new devices that have been detected by device discovery over the number of days specified in the **Detection period (days)** field.

If this check box is cleared, the selection includes all devices that have been detected by device discovery.

By default, this check box is cleared.

- **Device is visible**

In the drop-down list, you can set up the criterion for including devices in the selection when performing search:

- **Yes.** The application includes in the selection devices that are currently visible in the network.
- **No.** The application includes in the selection devices that are currently invisible in the network.
- **No value is selected.** The criterion will not be applied.

Application

In the **Application** section, you can configure criteria for including devices in a selection based on the selected managed application:

- **Application name**

In the drop-down list, you can set a criterion for including devices in a selection when search is performed by the name of a Kaspersky application.

The list provides only the names of applications with management plug-ins installed on the administrator's workstation.

If no application is selected, the criterion will not be applied.

- **Application version**

In the entry field, you can set a criterion for including devices in a selection when search is performed by the version number of a Kaspersky application.

If no version number is specified, the criterion will not be applied.

- **Critical update name**

In the entry field, you can set a criterion for including devices in a selection when search is performed by application name or by update package number.

If the field is left blank, the criterion will not be applied.

- **Modules last updated**

You can use this setting to set a criterion for searching devices by time of the last update of modules of applications installed on those devices.

If this check box is selected, in the entry fields you can specify the time interval (date and time) during which the last update of modules of applications installed on those devices was performed.

If this check box is cleared, the criterion will not be applied.

By default, this check box is cleared.

- **Device is managed through Kaspersky Security Center 13**

In the drop-down list, you can include in the selection the devices managed through Kaspersky Security Center:

- **Yes.** The application includes in the selection devices managed through Kaspersky Security Center.
- **No.** The application includes devices in the selection if they are not managed through Kaspersky Security Center.
- **No value is selected.** The criterion will not be applied.

- **Security application is installed**

In the drop-down list, you can include in the selection all devices with the security application installed:

- **Yes.** The application includes in the selection all devices with the security application installed.
- **No.** The application includes in the selection all devices with no security application installed.
- **No value is selected.** The criterion will not be applied.

Operating system

In the **Operating system** section, you can specify the criteria that will be used to include devices in the selection according to their operating system type.

- **Operating system version**

If the check box is selected, you can select an operating system from the list. Devices with the specified operating systems installed are included in the search results.

- **Operating system bit size**

In the drop-down list, you can select the architecture for the operating system, which will determine how the moving rule is applied to the device (**Unknown**, **x86**, **AMD64**, or **IA64**). By default, no option is selected in the list so that the operating system's architecture is not defined.

- **Operating system service pack version**

In this field, you can specify the package version of the operating system (in X.Y format), which will determine how the moving rule is applied to the device. By default, no version value is specified.

- **Operating system build**

This setting is applicable to Windows operating systems only.

The build number of the operating system. You can specify whether the selected operating system must have an equal, earlier, or later build number. You can also configure searching for all build numbers except the specified one.

- **Operating system release ID**

This setting is applicable to Windows operating systems only.

The release identifier (ID) of the operating system. You can specify whether the selected operating system must have an equal, earlier, or later release ID. You can also configure searching for all release ID numbers except the specified one.

Device status

In the **Device status** section, you can configure criteria for including devices into a selection based on the description of the devices status from a managed application:

- **Device status**

Drop-down list in which you can select one of the device statuses: *OK*, *Critical*, or *Warning*.

- **Device status description**

In this field, you can select the check boxes next to conditions that, if met, assign one of the following statuses to the device: *OK*, *Critical*, or *Warning*.

- **Device status defined by application**

Drop-down list, in which you can select the real-time protection status. Devices with the specified real-time protection status are included in the selection.

Protection components

In the **Protection components** section, you can set up the criteria for including devices in a selection based on their protection status:

- **Databases released**

If this check box is selected, you can search for client devices by anti-virus database release date. In the entry fields you can set the time interval, on the basis of which the search is performed.

By default, this check box is cleared.

- **Database records count**

If this check box is selected, you can search for client devices by number of database records. In the entry fields you can set the lower and upper threshold values for anti-virus database records.

By default, this check box is cleared.

- **Last scanned**

If this check box is selected, you can search for client devices by time of the last virus scan. In the entry fields you can specify the time period within which the last virus scan was performed.

By default, this check box is cleared.

- **Total number of threats detected**

If this check box is selected, you can search for client devices by number of viruses detected. In the entry fields you can set the lower and upper threshold values for the number of viruses found.

By default, this check box is cleared.

Applications registry

In the **Applications registry** section, you can set up the criteria to search for devices according to applications installed on them:

- **Application name**

Drop-down list in which you can select an application. Devices on which the specified application is installed, are included in the selection.

- **Application version**

Entry field in which you can specify the version of selected application.

- **Vendor**

Drop-down list in which you can select the manufacturer of an application installed on the device.

- **Application status**

A drop-down list in which you can select the status of an application (*Installed, Not installed*). Devices on which the specified application is installed or not installed, depending on the selected status, will be included in the selection.

- **Find by update**

If this check box is selected, search will be performed using the details of updates for applications installed on the relevant devices. After you select the check box, the **Application name**, **Application version**, and **Application status** fields change to **Update name**, **Update version**, and **Status** respectively.

By default, this check box is cleared.

- **Incompatible security application name**

Drop-down list in which you can select third-party security applications. During the search, devices on which the specified application is installed, are included in the selection.

- **Application tag**

In the drop-down list, you can select the application tag. All devices that have installed applications with the selected tag in the description are included in the device selection.

- **Apply to devices without the specified tags**

If this check box is selected, the selection includes devices with descriptions that contain none of the selected tags.

If this check box is cleared, the criterion is not applied.

By default, this check box is cleared.

Hardware registry

In the **Hardware registry** section, you can configure criteria for including devices into a selection based on their installed hardware:

- **Device**

In the drop-down list, you can select a unit type. All devices with this unit are included in the search results.

The field supports the full-text search.

- **Vendor**

In the drop-down list, you can select the name of a unit manufacturer. All devices with this unit are included in the search results.

The field supports the full-text search.

- **Device name**

Name of the device in the Windows network. The device with the specified name is included in the selection.

- **Description**

Description of the device or hardware unit. Devices with the description specified in this field are included in the selection.

A device's description in any format can be entered in the properties window of that device. The field supports the full-text search.

- **Device vendor**

Name of the device manufacturer. Devices produced by the manufacturer specified in this field are included in the selection.

You can enter the manufacturer's name in the properties window of a device.

- **Serial number**

All hardware units with the serial number specified in this field will be included in the selection.

- **Inventory number**

Equipment with the inventory number specified in this field will be included in the selection.

- **User**

All hardware units of the user specified in this field will be included in the selection.

- **Location**

Location of the device or hardware unit (for example, at the HQ or a branch office). Computers or other devices that are deployed at the location specified in this field will be included in the selection.

You can describe the location of a device in any format in the properties window of that device.

- **CPU frequency, in MHz**

The frequency range of a CPU. Devices with CPUs that match the frequency range in these fields (inclusive) will be included in the selection.

- **Virtual CPU cores**

Range of the number of virtual cores in a CPU. Devices with CPUs that match the range in these fields (inclusive) will be included in the selection.

- **Hard drive volume, in GB**

Range of values for the size of the hard drive on the device. Devices with hard drives that match the range in these entry fields (inclusive) will be included in the selection.

- **RAM size, in MB**

Range of values for the size of the device RAM. Devices with RAMs that match the range in these entry fields (inclusive) will be included in the selection.

Virtual machines

In the **Virtual machines** section, you can set up the criteria to include devices in the selection according to whether these are virtual machines or part of virtual desktop infrastructure (VDI):

- **This is a virtual machine**

In the drop-down list you can select the following options:

- **Not important.**

- **No.** Find devices that are not virtual machines.
- **Yes.** Find devices that are virtual machines.

- **Virtual machine type**

In the drop-down list, you can select the virtual machine manufacturer.

This drop-down list is available if the **Yes** or **Not important** value is selected in the **This is a virtual machine** drop-down list.

- **Part of Virtual Desktop Infrastructure**

In the drop-down list you can select the following options:

- **Not important.**

- **No.** Find devices that are not part of Virtual Desktop Infrastructure.
- **Yes.** Find devices that are part of the Virtual Desktop Infrastructure (VDI).

Vulnerabilities and updates

In the **Vulnerabilities and updates** section, you can specify the criteria that will be used to include devices in the selection according to their Windows Update source:

- **WUA is switched to Administration Server**

You can select one of the following search options from the drop-down list:

- **Yes.** If this option is selected, the search results will include devices that receive updates through Windows Update from the Administration Server.
- **No.** If this option is selected, the results will include devices that receive updates through Windows Update from another sources.

Users

In the **Users** section, you can set up the criteria to include devices in the selection according to the accounts of users who have logged in to the operating system.

- **Last user who logged in to the system**

If this check box is selected, click the **Browse** button to specify a user account. The search results include devices on which the specified user performed the last login to the system.

- **User who logged in to the system at least once**

If this check box is selected, click the **Browse** button to specify a user account. The search results include devices on which the specified user logged in to the system at least once.

Status-affecting problems in managed applications

In the **Status-affecting problems in managed applications** section, you can specify the criteria that will be used to include devices in the selection according to the list of possible problems detected by a managed application. If at least one problem that you select exists on a device, the device will be included in the selection. When you select a problem listed for several applications, you have the option to select this problem in all of the lists automatically.

- **Device status description**

You can select check boxes for descriptions of statuses from the managed application; upon receipt of these statuses, the devices will be included in the selection. When you select a status listed for several applications, you have the option to select this status in all of the lists automatically.

Statuses of components in managed applications

In the **Statuses of components in managed applications** section, you can configure criteria for including devices in a selection according to the statuses of components in managed applications:

- **Data Leakage Prevention status**

Search for devices by the status of Data Leakage Prevention (*No data from device, Stopped, Starting, Paused, Running, Failed*).

- **Collaboration servers protection status**

Search for devices by the status of server collaboration protection (*No data from device, Stopped, Starting, Paused, Running, Failed*).

- **Anti-virus protection status of mail servers**

Search for devices by the status of Mail Server protection (*No data from device, Stopped, Starting, Paused, Running, Failed*).

- **Endpoint Sensor status**

Search for devices by the status of the Endpoint Sensor component (*No data from device, Stopped, Starting, Paused, Running, Failed*).

Encryption

- **Encryption algorithm**

Advanced Encryption Standard (AES) symmetrical block cipher algorithm. In the drop-down list, you can select the encryption key size (56-bit, 128-bit, 192-bit, or 256-bit).

Available values: *AES56, AES128, AES192, and AES256*.

Cloud segments

In the **Cloud segments** section, you can configure criteria for including devices in a selection according to their respective cloud segments:

- **Device is in a cloud segment**

If this check box is selected, you can click the **Browse** button to specify the segment to search.

If the **Include child objects** check box is also selected, the search is run on all child objects of the specified segment.

Search results include only devices from the selected segment.

- **Device discovered by using the API**

In the drop-down list, you can select whether a device is detected by API tools.

- **AWS.** The device is discovered by using AWS API, that is, the device definitely is in the AWS cloud environment.
- **Azure.** The device is discovered by using Azure API, that is, the device definitely is in the Azure cloud environment.
- **Google Cloud.** The device is discovered by using Google API, that is, the device definitely is in the Google cloud environment.
- **No.** The device cannot be detected by using AWS, Azure or Google API, that is, it is either outside the cloud environment, or it is in the cloud environment but it cannot be detected by using an API for some reason.
- **No value.** This criterion cannot be applied.

Application components

This section contains the list of components of those applications that have corresponding management plugins installed in Administration Console.

In the **Application components** section, you can specify criteria for including devices in a selection according to the statuses and version numbers of the components that refer to the application that you select:

- **Status**

Search for devices according to the component status sent by an application to the Administration Server. You can select one of the following statuses: *No data from device*, *Stopped*, *Starting*, *Paused*, *Running*, *Malfunction*, or *Not installed*. If the selected component of the application installed on a managed device has the specified status, the device is included in the device selection.

Statuses sent by applications:

- *Starting*—The component is currently in the process of initialization.
- *Running*—The component is enabled and working properly.
- *Paused*—The component is suspended, for example, after the user has paused protection in the managed application.
- *Malfunction*—An error has occurred during the component operation.
- *Stopped*—The component is disabled and not working at the moment.
- *Not installed*—The user did not select the component for installation when configuring custom installation of the application.

Unlike other statuses, the *No data from device* status is not sent by applications. This option shows that the applications have no information about the selected component status. For example, this can happen when the selected component does not belong to any of the applications installed on the device, or when the device is turned off.

- **Version**

Search for devices according to the version number of the component that you select in the list. You can type a version number, for example `3.4.1.0`, and then specify whether the selected component must have an equal, earlier, or later version. You can also configure searching for all versions except the specified one.

About Kaspersky announcements

The Kaspersky announcements section (**MONITORING & REPORTING** → **Kaspersky announcements**) keeps you informed by providing information related to your version of Kaspersky Security Center and the managed applications installed on the managed devices. Kaspersky Security Center periodically updates the information in the section by removing outdated announcements and adding new information.

Administration Server must have an Internet connection to receive Kaspersky announcements.

The announcements include information of the following types:

- Security-related announcements

Security-related announcements are intended to keep the Kaspersky applications installed in your network up-to-date and fully functional. The announcements may include information about critical updates for Kaspersky applications, fixes for found vulnerabilities, and ways to fix other issues in Kaspersky applications. Security-related announcements are enabled by default. If you do not want to receive the announcements, you can disable this feature.

To show you the information that corresponds to your network protection configuration, Kaspersky Security Center sends data to Kaspersky cloud servers and receives only those announcements that relate to the Kaspersky applications installed in your network. The data set that can be sent to the servers is described in the End User License Agreement (see section "About the End User License Agreement" on page [318](#)) that you accept when you install Kaspersky Security Center Administration Server.

- Marketing announcements

Marketing announcements include information about special offers for your Kaspersky applications, advertisements, and news from Kaspersky. Marketing announcements are disabled by default. You receive this type of announcements only if you enabled Kaspersky Security Network (KSN). You can disable marketing announcements by disabling KSN.

To show you only relevant information that might be helpful in protecting your network devices and in your everyday tasks, Kaspersky Security Center sends data to Kaspersky cloud servers and receives the appropriate announcements. The data set that can be sent to the servers is described in the Processed Data section of the KSN Statement (see section "About KSN" on page [785](#)).

New information is divided into the following categories, according to importance:

1. Critical info
2. Important news
3. Warning
4. Info

When new information appears in the Kaspersky announcements section, Kaspersky Security Center 13 Web Console displays a notification label that corresponds to the importance level of the announcements. You can click the label to view this announcement in the Kaspersky announcements section.

You can specify the Kaspersky announcements settings (see section "Specifying Kaspersky announcements settings" on page [1366](#)), including the announcement categories that you want to view and where to display the notification label.

See also:

Specifying Kaspersky announcements settings	1366
Disabling Kaspersky announcements	1367
About KSN	785

Specifying Kaspersky announcements settings

In the Kaspersky announcements section, you can specify the Kaspersky announcements settings, including the categories of the announcements that you want to view and where to display the notification label.

► *To configure Kaspersky announcements:*

1. Go to **MONITORING & REPORTING** → **Kaspersky announcements**.

2. Click the **Settings** link.

The Kaspersky announcement settings window opens.

3. Specify the following settings:

- Select the importance level of the announcements that you want to view. The announcements of other categories will not be displayed.
- Select where you want to see the notification label. The label can be displayed in all console sections, or in the **MONITORING & REPORTING** section and its subsections.

4. Click the **OK** button.

The Kaspersky announcement settings are specified.

See also:


About Kaspersky announcements	1365
Disabling Kaspersky announcements	1367

Disabling Kaspersky announcements

The Kaspersky announcements section (**MONITORING & REPORTING** → **Kaspersky announcements**) keeps you informed by providing information related to your version of Kaspersky Security Center and managed applications installed on the managed devices. If you do not want to receive Kaspersky announcements, you can disable this feature.

The Kaspersky announcements include two types of information: security-related announcements and marketing announcements. You can disable the announcements of each type separately.

► *To disable security-related announcements:*

1. In the main application window, click the **Settings** icon () next to the name of the required Administration Server.


The Administration Server properties window opens.

2. On the **General** tab, select the **Kaspersky announcements** section.
3. Switch the toggle button to the **Security-related announcements are disabled** position.
4. Click the **Save** button.

Kaspersky announcements are disabled.

Marketing announcements are disabled by default. You receive marketing announcements only if you enabled Kaspersky Security Network (KSN). You can disable this type of announcement by disabling KSN.

► *To disable marketing announcements:*

1. In the main application window, click the **Settings** icon () next to the name of the required Administration Server.
The Administration Server properties window opens.
2. On the **General** tab, select the **KSN Proxy settings** section.
3. Disable the **I agree to use Kaspersky Security Network** option.
4. Click the **Save** button.

Marketing announcements are disabled.

See also:

About Kaspersky announcements	1365
Specifying Kaspersky announcements settings	1366

Kaspersky Security Center 13 Web Console activity logging

Kaspersky Security Center 13 Web Console activity logging can help to investigate the causes of a software malfunction. When you contact Kaspersky Technical Support about a Kaspersky Security Center 13 Web Console malfunction, Kaspersky Technical Support specialists can request Kaspersky Security Center 13 Web Console log files from you. Kaspersky Security Center 13 Web Console log files are stored in the <Kaspersky Security Center 13 Web Console installation folder>/logs folder the entire time you use the application. Log files are not sent to Kaspersky Technical Support specialists automatically.

► *To enable Kaspersky Security Center 13 Web Console activity logging,*

Select the **Enable logging of Kaspersky Security Center 13 Web Console activities** check box in the **Kaspersky Security Center 13 Web Console connection settings** window of the Kaspersky Security Center 13 Web Console Setup Wizard (see section "Installing Kaspersky Security Center 13 Web Console" on page [967](#)).

The log files are in text format.

The log file names are in the format logs-<component name>.<device name>-<file revision number>.YYYY-MM-DD, where

- <component name> is the name of the Kaspersky Security Center component or is the Kaspersky Security Center 13 Web Console management plug-in name.
- <device name> is the name of the device on which the <component name> is running.
- <file revision number> is the number of the log file created for the <component name> that is in operation on the <device name>. Within one day, several log files for the same <component name> and <device name> can be created. The maximum size of a log file is 50 megabytes (MB). When the maximum file size is reached, a new log file is created. A new log file <file revision number> is incremented by 1.
- YYYY, MM, and DD are the year, month, and day when the log was first created. When a new day starts a new log file is created.

Integration between Kaspersky Security Center Web Console and other Kaspersky solutions

This section describes how to configure access from Kaspersky Security Center Web Console to another Kaspersky application, such as Kaspersky Endpoint Detection and Response, and Kaspersky Managed Detection and Response.

In this section

Configuring access to KATA/KEDR Web Console	1369
Establishing a background connection for cross-service integration	1369

Configuring access to KATA/KEDR Web Console

This section describes features applicable only to Kaspersky Security Center 11.1 Web Console or a later version.

Kaspersky Anti Targeted Attack (KATA) and Kaspersky Endpoint Detection and Response (KEDR) are two functional blocks of Kaspersky Anti Targeted Attack Platform <https://help.kaspersky.com/KATA/3.7.2/en-US/>. You can manage these functional blocks through Web Console for Kaspersky Anti Targeted Attack Platform (KATA/KEDR Web Console). If you use both Kaspersky Security Center 13 Web Console and KATA/KEDR Web Console, you can configure access to KATA/KEDR Web Console directly from the interface of Kaspersky Security Center 13 Web Console.

► *To configure access to KATA/KEDR Web Console:*

1. In the **Console settings** drop-down list, select **Integration**.
The **Console settings** window opens.
2. Select the **Integration** tab.
3. On the **Integration** tab, select the **KATA** section.
4. Enter the URL of KATA/KEDR Web Console in the **URL to KATA / KEDR Web Console** field.
5. Click the **Save** button.

The **Advanced management** drop-down list is added to the main application window. You can use this menu to open KATA/KEDR Web Console. After you click **Advanced Cybersecurity**, a new tab opens in your browser with the URL that you specified.

Establishing a background connection for cross-service integration

In order to configure interaction between Kaspersky Security Center and another Kaspersky application or solution, for example, Kaspersky Managed Detection and Response (also referred to as MDR), you have to establish a background connection between Kaspersky Security Center Web Console and Administration Server for cross-

service integration. You can establish this connection only if your account has the rights of the Main Administrator (see section "Predefined user roles" on page [1155](#)) role.

► *To establish a background connection for cross-service integration:*

1. In the **Console settings** drop-down list, select **Integration**.
The **Console settings** window opens.
2. Select the **Integration** tab.
3. On the **Integration** tab, select the **Cross-service integration** section.
4. Switch the toggle button of establishing a background connection to the to position: **Establish a background connection for cross-service integration ENABLED**.
5. In the opened **Establish a background connection** section, click the **OK** button.

The background connection between Kaspersky Security Center Web Console and Administration Server is established. Administration Server creates an account for the background connection and this account is used as a service account to maintain interaction between Kaspersky Security Center and another Kaspersky application or solution. The name of this service account contains the NWCSvcUser prefix. You cannot delete this account manually. Administration Server deletes this account automatically when you disable a cross-service connection. Administration Server creates a single service account for each Administration Console and assigns all the service accounts to the security group with the name ServiceNwcGroup. Administration Server creates this security group automatically during the Kaspersky Security Center installation process and you cannot delete this group manually.

Working with Kaspersky Security Center 13 Web Console in a cloud environment

This section describes features applicable only to Kaspersky Security Center 12.1 or a later version.

This section provides information about Kaspersky Security Center 13 Web Console features related to deployment and maintenance of Kaspersky Security Center in cloud environments, such as Amazon Web Services, Microsoft Azure, or Google Cloud.

To work within a cloud environment, you need a special license (see section "Licensing options in a cloud environment" on page [826](#)). If you do not have such a license, the interface elements related to cloud devices are not displayed.

In this section

Kaspersky Security Center 13 Web Console Cloud Environment Configuration Wizard.....	1371
Network segment polling via Kaspersky Security Center 13 Web Console	1377
Synchronization with Cloud: configuring the moving rule.....	1383
Creating Backup of the Administration Server data task by using a cloud DBMS	1385

Kaspersky Security Center 13 Web Console Cloud Environment Configuration Wizard

This section describes features applicable only to Kaspersky Security Center 12.1 or a later version.

To configure Kaspersky Security Center using this Wizard, you must have the following:

- Specific credentials for a cloud environment:
 - An IAM role that has been granted the right to poll the cloud segment (see section "Creating an IAM role for the Administration Server" on page [830](#)) or an IAM user account that has been granted the right to poll the cloud segment (see section "Creating an IAM user account for work with Kaspersky Security Center" on page [833](#)) (for work with Amazon Web Services)
 - Azure Application ID, password, and subscription (see section "Creating a subscription, Application ID, and password" on page [843](#)) (for work with Microsoft Azure)
 - Google client email, Project ID, and private key (see section "Working in Google Cloud" on page [849](#)) (for work with Google Cloud)
- Plug-in for Kaspersky Endpoint Security for Linux (Web Console plug-in)
- Plug-in for Kaspersky Endpoint Security for Windows (Web Console plug-in)
- Network Agent for Windows
- Network Agent for Linux
- Installation package for Kaspersky Endpoint Security for Linux
- Installation package for Kaspersky Security for Windows Server

The Cloud Environment Configuration Wizard starts automatically at the first connection to Administration Server through Administration Console if you deploy Kaspersky Security Center from a ready-to-use image. You can also start the Cloud Environment Configuration Wizard manually at any time.

► *To start the Cloud Environment Configuration Wizard manually,*

Go to **DISCOVERY & DEPLOYMENT** → **DEPLOYMENT & ASSIGNMENT** → **Cloud Environment Configuration Wizard**.

The Wizard starts.

An average work session with this Wizard lasts about 15 minutes.

In this section

Step 1. Reading information about the Wizard.....	1372
Step 2. Licensing the application.....	1372
Step 3. Selecting the cloud environment and authorization	1372
Step 4. Segment polling, configuring synchronization with Cloud and choosing further actions	1374
Step 5. Configuring Kaspersky Security Network for Kaspersky Security Center.....	1376
Step 6. Creating an initial configuration of protection	1376

Step 1. Reading information about the Wizard

This section describes features applicable only to Kaspersky Security Center 12.1 or a later version.

Read about the Cloud Environment Configuration Wizard on the Welcome page and click **Next** to proceed.

Step 2. Licensing the application

This section describes features applicable only to Kaspersky Security Center 12.1 or a later version.
This step is displayed only if you are using a BYOL AMI and you have not activated the application with a Kaspersky Security for Virtualization license or a Kaspersky Hybrid Cloud Security license.

Specify the license key and click **Next** to proceed.

The license key is added to the Administration Server storage.

If you run the Wizard again, this step is not displayed.

Step 3. Selecting the cloud environment and authorization

This section describes features applicable only to Kaspersky Security Center 12.1 or a later version.

Specify the following data:

- **Cloud environment**
- **Connection name**

Enter a name for the connection. The name cannot contain more than 256 characters. Only Unicode characters are permitted.

This name will also be used as the name for the administration group for the cloud devices.

If you plan to work with more than one cloud environment, you might want to include the name of the environment in the connection name, for example, "Azure Segment," "AWS Segment," or "Google Segment."

Enter your credentials to receive authorization in the cloud environment that you specified.

AWS

If you selected AWS as the cloud segment type, you need an IAM role or an AWS IAM access key for further polling of the cloud segment.

- **AWS IAM role assigned to an EC2 instance**

Select this option if you have an IAM role with the required rights (see section "Creating an IAM role for the Administration Server" on page [830](#)) for the Administration Server.

- **AWS IAM user**

Select this option if you have an AWS IAM access key (see section "Creating an IAM user account for work with Kaspersky Security Center" on page [833](#)). Enter your key data:

- **Access key ID**

The IAM access key ID is a sequence of alphanumeric characters. You received the key ID when you created the IAM user account (see section "Creating an IAM user account for work with Kaspersky Security Center" on page [833](#)).

The field is available if you selected an AWS IAM access key for authorization instead of an IAM role.

- **Secret key**

The secret key that you received with the access key ID when you created the IAM user account (see section "Creating an IAM user account for work with Kaspersky Security Center" on page [833](#)).

The characters of the secret key are displayed as asterisks. After you begin entering the secret key, the **Show** button is displayed. Click and hold this button for the necessary amount of time to view the characters you entered.

The field is available if you selected an AWS IAM access key for authorization instead of an IAM role.

To see the characters that you entered, click and hold the **Show** button.

Azure

If you selected Azure as the cloud segment type, specify the following settings for the connection that will be used for further polling of the cloud segment:

- **Azure Application ID**

You created (see section "Creating a subscription, Application ID, and password" on page [843](#)) this application ID on the Azure portal.

You can provide only one Azure Application ID for polling and other purposes. If you want to poll another Azure segment, you must first delete the existing Azure connection.

- **Azure Subscription ID**

You created (see section "Creating a subscription, Application ID, and password" on page

[843](#)) the subscription on the Azure portal.

- **Azure Application password**

You received the password of the Application ID when you created the Application ID (see section "Creating a subscription, Application ID, and password" on page [843](#)).

The characters of the password are displayed as asterisks. After you begin entering the password, the **Show** button becomes available. Click and hold this button to view the characters you entered.

To see the characters that you entered, click and hold the **Show** button.

- **Azure storage account name**

You created the name of the Azure storage account (see section "Creating Azure storage account" on page [846](#)) for working with Kaspersky Security Center.

- **Azure storage access key**

You received a password (key) when you created Azure storage account for working with Kaspersky Security Center.

The key is available in section "Overview of the Azure storage account", in subsection "Keys".

To see the characters that you entered, click and hold the **Show** button.

Google Cloud

If you selected Google Cloud as the cloud segment type, specify the following settings for the connection that will be used for further polling the cloud segment:

- **Client email address**
- **Project ID**
- **Private key**

To see the characters that you entered, click and hold the **Show** button.

The connection that you specified is saved in the application settings.

The Cloud Environment Configuration Wizard allows you to specify only one segment. Later, you can specify more connections to manage other cloud segments.

Click **Next** to proceed.

See also:

| Adding connections for cloud segment polling[1378](#)

Step 4. Segment polling, configuring synchronization with Cloud and choosing further actions

This section describes features applicable only to Kaspersky Security Center 12.1 or a later version.

At this step, cloud segment polling starts, and a special administration group for cloud devices is automatically created. The devices found during polling are placed into this group. The cloud segment polling schedule is

configured (every 5 minutes by default; you can change this setting (see section "Configuring the polling schedule via Kaspersky Security Center 13 Web Console" on page [1381](#)) later).

A **Synchronize with Cloud** (see section "**Synchronization with Cloud: configuring the moving rule**" on page [1383](#)) automatic moving rule is also created. For each subsequent scan of the cloud network, virtual devices detected will be moved to the corresponding subgroup within the **Managed devices\Cloud** group.

Define the following settings:

- **Synchronize administration groups with cloud structure**

If this option is enabled, the **Cloud** group is automatically created within the **Managed devices** group and a cloud device discovery is started. The instances and virtual machines detected during each cloud network scan are placed into the Cloud group. The structure of the administration subgroups within this group matches the structure of your cloud segment (in AWS, availability zones and placement groups are not represented in the structure; in Azure, subnets are not represented in the structure). Devices that have not been identified as instances in the cloud environment are in the **Unassigned devices** group. This group structure allows you to use group installation tasks to install anti-virus applications on instances, as well as set up different policies for different groups.

If this option is disabled, the **Cloud** group is also created and the cloud device discovery is also started; however, subgroups matching the cloud segment structure are not created within the group. All detected instances are in the **Cloud** administration group so they are displayed in a single list. If your work with Kaspersky Security Center requires synchronization, you can modify the properties of the **Synchronize with Cloud** rule and enforce it (see section "Synchronization with cloud" on page [873](#)). Enforcing this rule alters the structure of subgroups in the Cloud group so that it matches the structure of your cloud segment.

By default, this option is disabled.

- **Deploy protection**

If this option is selected, the Wizard creates a task to install security applications on instances. After the Wizard finishes, the Protection Deployment Wizard automatically starts on the devices in your cloud segments, and you will be able to install Network Agent and security applications on those devices.

Kaspersky Security Center can perform the deployment with its native tools. If you do not have permissions to install the applications on EC2 instances or Azure virtual machines, you can configure the **Remote installation** task manually (see section "Installing applications on devices in a cloud environment" on page [870](#)) and specify an account with the required permissions. In this case, the Remote installation task will not work for the devices discovered using AWS API or Azure. This task will only work for the devices discovered using Active Directory polling, Windows domains polling, or IP range polling.

If this option is not selected, the Protection Deployment Wizard is not started and tasks for installing security applications on instances are not created. You can manually perform both actions later.

If you select the Deploy protection option, the **Restarting devices** section becomes available. In this section, you must choose what to do when the operating system of a target device has to be restarted. Select whether to restart instances if the device operating system has to be restarted during installation of applications:

- **Do not restart**

If this option is selected, the device will not be restarted after the security application

installation.

- **Restart**

If this option is selected, the device will be restarted after the security application installation.

Click **Next** to proceed.

For Google Cloud, you can only perform deployment with Kaspersky Security Center native tools. If you selected Google Cloud, the **Deploy protection** option is not available.

See also:

| Synchronization with Cloud: configuring the moving rule[1383](#)

Step 5. Configuring Kaspersky Security Network for Kaspersky Security Center

This section describes features applicable only to Kaspersky Security Center 12.1 or a later version.

Specify the settings for relaying information about Kaspersky Security Center operations to the Kaspersky Security Network (KSN) knowledge base. Select one of the following options:

- **I agree to use Kaspersky Security Network**

Kaspersky Security Center and managed applications installed on client devices will automatically transfer their operation details to Kaspersky Security Network (see section "About KSN" on page [785](#)). Participation in Kaspersky Security Network ensures faster updates of databases containing information about viruses and other threats, which ensures a faster response to emergent security threats.

- **I do not agree to use Kaspersky Security Network**

Kaspersky Security Center and managed applications will provide no information to Kaspersky Security Network.

If you select this option, the use of Kaspersky Security Network will be disabled.

Kaspersky recommends participation in Kaspersky Security Network.

KSN agreements for managed applications may also be displayed. If you agree to use Kaspersky Security Network, the managed application will send data to Kaspersky. If you do not agree to participate in Kaspersky Security Network, the managed application will not send data to Kaspersky. (You can change this setting later in the application policy.)

Click **Next** to proceed.

Step 6. Creating an initial configuration of protection

This section describes features applicable only to Kaspersky Security Center 12.1 or a later version.

You can check a list of policies and tasks that are created.

Wait for the creation of policies and tasks to complete, and then click **Next** to proceed. On the last page of the Wizard, click the **Finish** button to exit.

Network segment polling via Kaspersky Security Center 13 Web Console

This section describes features applicable only to Kaspersky Security Center 12.1 or a later version.

Information about the structure of the network (and devices in it) is received by Administration Server through regular polling of cloud segments by using AWS API, Azure API, or Google API tools. Kaspersky Security Center uses this information to update the contents of the Unassigned devices and Managed devices folders. If you have configured devices to be moved to administration groups automatically, detected devices are included in administration groups.

To allow the Administration Server to poll cloud segments, you must have the corresponding rights that are provided with an IAM role or IAM user account (in AWS), or with Application ID and password (in Azure), or with a Google client email, Google project ID, and private key (in Google Cloud).

You can add and delete connections, as well as set the polling schedule, for each cloud segment.

In this section

Adding connections for cloud segment polling	1378
Deleting a connection for cloud segment polling	1380
Configuring the polling schedule via Kaspersky Security Center 13 Web Console	1381
Viewing the results of cloud segment polling via Kaspersky Security Center 13 Web Console	1382
Viewing the properties of cloud devices via Kaspersky Security Center 13 Web Console	1382

Adding connections for cloud segment polling

This section describes features applicable only to Kaspersky Security Center 12.1 or a later version.

► *To add a connection for cloud segment polling to the list of available connections:*

1. Go to **DISCOVERY & DEPLOYMENT** → **DISCOVERY** → **Cloud**.
2. In the window that opens, click **Properties**.
3. In the **Settings** window that opens, click **Add**.

The **Cloud segment settings** window opens.

4. Specify the name of the cloud environment for the connection that will be used for further polling of the cloud segment:
 - **Cloud environment**
 - **Connection name**

Enter a name for the connection. The name cannot contain more than 256 characters. Only Unicode characters are permitted.

This name will also be used as the name for the administration group for the cloud devices.

If you plan to work with more than one cloud environment, you might want to include the name of the environment in the connection name, for example, "Azure Segment," "AWS Segment," or "Google Segment."

1. Enter your credentials to receive authorization in the cloud environment that you specified.
 - If you selected AWS, specify the following settings:

- **Use AWS IAM role**

Select this option if you have already created an IAM role for the Administration Server to use AWS services (see section "Creating an IAM role for the Administration Server" on page [830](#)).

- **Use AWS IAM user account**

Select this option if you have an IAM user account with the necessary permissions (see section "Creating an IAM user account for work with Kaspersky Security Center" on page [833](#)) and you can enter a key ID and secret key.

If you specified that you have Use AWS IAM user account, specify the following:

- **Access key ID**

The IAM access key ID is a sequence of alphanumeric characters. You received the key ID when you created the IAM user account (see section "Creating an IAM user account for work with Kaspersky Security Center" on page [833](#)).

The field is available if you selected an AWS IAM access key for authorization instead of an IAM role.

- **Secret key**

The secret key that you received with the access key ID when you created the IAM user account (see section "Creating an IAM user account for work with Kaspersky Security Center" on page [833](#)).

The characters of the secret key are displayed as asterisks. After you begin entering the secret key, the **Show** button is displayed. Click and hold this button for the necessary amount of time to view the characters you entered.

The field is available if you selected an AWS IAM access key for authorization instead of an IAM role.

To see the characters that you entered, click and hold the **Show** button.

- If you selected Azure, specify the following settings:

- **Azure Application ID**

You created (see section "Creating a subscription, Application ID, and password" on page [843](#)) this application ID on the Azure portal.

You can provide only one Azure Application ID for polling and other purposes. If you want to poll another Azure segment, you must first delete the existing Azure connection.

- **Azure Subscription ID**

You created (see section "Creating a subscription, Application ID, and password" on page [843](#)) the subscription on the Azure portal.

- **Azure Application password**

You received the password of the Application ID when you created the Application ID (see section "Creating a subscription, Application ID, and password" on page [843](#)).

The characters of the password are displayed as asterisks. After you begin entering the password, the **Show** button becomes available. Click and hold this button to view the characters you entered.

To see the characters that you entered, click and hold the **Show** button.

- **Azure storage account name**

You created the name of the Azure storage account (see section "Creating Azure storage account" on page [846](#)) for working with Kaspersky Security Center.

- **Azure storage access key**

You received a password (key) when you created Azure storage account for working with Kaspersky Security Center.

The key is available in section "Overview of the Azure storage account", in subsection "Keys".

To see the characters that you entered, click and hold the **Show** button.

If you selected Google Cloud, specify the following settings:

- **Client email address**
- **Project ID**
- **Private key**

To see the characters that you entered, click and hold the **Show** button.

2. If you want, click **Set polling schedule** and change the default settings (see section "Configuring the polling schedule via Kaspersky Security Center 13 Web Console" on page [1381](#)).

The connection is saved in the application settings.

After the new cloud segment is polled for the first time, the subgroup corresponding to that segment appears in the **Managed devices\Cloud** administration group.

If you specify incorrect credentials, no instances will be found during cloud segment polling and a new subgroup will not appear in the **Managed devices\Cloud** administration group.

Deleting a connection for cloud segment polling

This section describes features applicable only to Kaspersky Security Center 12.1 or a later version.

If you no longer have to poll a specific cloud segment, you can delete the connection corresponding to it from the list of available connections. You can also delete a connection if, for example, permissions to poll a cloud segment have been transferred to another user who has different credentials.

► *To delete a connection:*

1. Go to **DISCOVERY & DEPLOYMENT** → **DISCOVERY** → **Cloud**.
2. In the window that opens, click **Properties**.
3. In the **Settings** window that opens, click the name of the segment that you want to delete.
4. Click **Delete**.
5. In the window that opens, click the **OK** button to confirm your selection.

The connection is deleted. The devices in the cloud segment corresponding to this connection are automatically deleted from the administration groups.

Configuring the polling schedule via Kaspersky Security Center 13 Web Console

Cloud segment polling is performed according to schedule. You can set the polling frequency.

The polling frequency is automatically set at 5 minutes by the Cloud Environment Configuration Wizard. You can change this value at any time and set a different schedule. However, it is not recommended to configure polling to run more frequently than every 5 minutes, because this could lead to errors in the API operation.

► *To configure a cloud segment polling schedule:*

1. Go to **DISCOVERY & DEPLOYMENT** → **DISCOVERY** → **Cloud**.
2. In the window that opens, click **Properties**.
3. In the **Settings** window that opens, click the name of the segment for which you want to configure a polling schedule.

This opens the **Cloud segment settings** window.

4. In the **Cloud segment settings** window, click the **Set polling schedule** button.

This opens the **Schedule** window.

5. In the **Schedule** window, define the following settings:

- **Scheduled start**

Polling schedule options:

- **Every N days**

The polling runs regularly, with the specified interval in days, starting from the specified date and time.

By default, the polling runs every day, starting from the current system date and time.

- **Every N minutes**

The polling runs regularly, with the specified interval in minutes, starting from the specified time.

By default, the polling runs every five minutes, starting from the current system time.

- **By days of week**

The polling runs regularly, on the specified days of week, and at the specified time.

By default, the polling runs every Friday at 6:00:00 P.M.

- **Every month on specified days of selected weeks**

The polling runs regularly, on the specified days of each month, and at the specified time.

By default, no days of month are selected; the default start time is 6:00:00 P.M.

- **Start interval (min)**

- **Starting from**

- **Run missed tasks**

If the Administration Server is switched off or unavailable during the time for which the poll is scheduled, the Administration Server can either start the poll immediately after it is switched on, or wait for the next time for which the poll scheduled.

If this option is enabled, the Administration Server starts polling immediately after it is

switched on.

If this option is disabled, the Administration Server waits for the next time for which the polling is scheduled.

By default, this option is enabled.

6. Click **Save** to save the changes.

The polling schedule for the segment is configured and saved.

Viewing the results of cloud segment polling via Kaspersky Security Center 13 Web Console

This section describes features applicable only to Kaspersky Security Center 12.1 or a later version.

You can view the results of cloud segment polling, that is, view the list of cloud devices managed by the Administration Server.

- *To view the results of cloud segment polling,*

Go to **DISCOVERY & DEPLOYMENT** → **DISCOVERY** → **Cloud**.

This displays the cloud segments available for polling.

Viewing the properties of cloud devices via Kaspersky Security Center 13 Web Console

This section describes features applicable only to Kaspersky Security Center 12.1 or a later version.

You can view the properties of each cloud device.

► *To view the properties of a cloud device:*

1. Go to **DEVICES** → **MANAGED DEVICES**.
2. Click the name of the device whose properties you want to view.
A properties window opens with the **General** section selected.
3. If you want to view the properties specific for cloud devices, select the **System** section in the properties window.

The properties are displayed depending on the cloud platform of the device.

For the devices in AWS, the following properties are displayed:

- **Device discovered using API** (value: **AWS**)
- **Cloud Region**
- **Cloud VPC**
- **Cloud availability zone**
- **Cloud subnet**
- **Cloud placement group** (this unit is only displayed if the instance belongs to a placement group; otherwise, it is not displayed)

For the devices in Azure, the following properties are displayed:

- **Device discovered using API** (value: **Microsoft Azure**)
- **Cloud Region**
- **Cloud subnet**

For the devices in Google Cloud, the following properties are displayed:

- **Device discovered using API** (value: **Google Cloud**)
- **Cloud Region**
- **Cloud VPC**
- **Cloud availability zone**
- **Cloud subnet**

Synchronization with Cloud: configuring the moving rule

This section describes features applicable only to Kaspersky Security Center 12.1 or a later version.

During the Cloud Environment Configuration Wizard operation, the Synchronize with Cloud rule is created automatically. This rule allows you to automatically move devices detected in each poll from the Unassigned devices group to the Managed devices\Cloud group, to make these devices available for centralized management. By default, the rule is active after it is created. You can disable, modify, or enforce the rule at any time.

► *To edit the properties of the Synchronize with Cloud rule and/or enforce the rule:*

1. Go to **DISCOVERY & DEPLOYMENT** → **DEPLOYMENT & ASSIGNMENT** → **Moving rules**.

This opens a list of moving rules.

2. In the list of moving rules, select **Synchronize with cloud**.

This opens the rule properties window.

3. If necessary, specify the following settings in the **Rule conditions** tab, in the **Cloud segments** tab:

- **Device is in a cloud segment**

The rule only applies to devices that are in the selected cloud segment. Otherwise, the rule applies to all devices that have been discovered.

By default, this property is selected.

- **Include child objects**

The rule applies to all devices in the selected segment and in all nested cloud subsections. Otherwise, the rule only applies to devices that are in the root segment.

By default, this option is selected.

- **Move devices from nested objects to corresponding subgroups**

If this option is enabled, devices from nested objects are automatically moved to the subgroups that correspond to their structure.

If this option is disabled, devices from nested objects are automatically moved to the root of the Cloud subgroup without any further branching.

By default, this option is enabled.

- **Create subgroups corresponding to containers of newly detected devices**

If this option is enabled, when the structure of the **Managed devices\Cloud** group has no subgroups that will match the section containing the device, Kaspersky Security Center creates such subgroups. For example, if a new subnet is discovered during device discovery, a new group with the same name will be created under the **Managed devices\Cloud** group.

If this option is disabled, Kaspersky Security Center does not create any new subgroups. For example, if a new subnet is discovered during network poll, a new group with the same name will not be created under the **Managed devices\Cloud** group, and the devices that are in that subnet will be moved into the **Managed devices\Cloud** group.

By default, this option is enabled.

- **Delete subgroups for which no match is found in the cloud segments**

If this option is enabled, the application deletes from the Cloud group all the subgroups that do not match any existing cloud objects.

If this option is disabled, subgroups that do not match any of the existing cloud objects are retained.

By default, this option is enabled.

If you enabled the **Synchronize administration groups with cloud structure** option when using the Cloud Environment Configuration Wizard, the **Synchronize with cloud** rule is created with the **Create subgroups corresponding to containers of newly detected devices** and **Delete subgroups for which no match is found in the cloud segments** options enabled.

If you did not enable the **Synchronize administration groups with cloud structure** option, the **Synchronize with cloud** rule is created with these options disabled (cleared). If your work with Kaspersky Security Center requires that the structure of subgroups in the **Managed devices\Cloud** subgroup matches the structure of cloud segments, enable the **Create subgroups corresponding to containers of newly detected devices** and **Delete subgroups for which no match is found in the cloud segments** options in the rule properties, and then enforce the rule.

4. In the **Device discovered using API** drop-down list, select one of the following values:
 - **No**. The device cannot be detected by using AWS, Azure, or Google API, that is, it is either outside the cloud environment, or it is in the cloud environment but it cannot be detected by using an API for some reason.
 - **AWS**. The device is discovered by using AWS API, that is, the device definitely is in the AWS cloud environment.
 - **Azure**. The device is discovered by using Azure API, that is, the device definitely is in the Azure cloud environment.
 - **Google Cloud**. The device is discovered by using Google API, that is, the device definitely is in the Google cloud environment.
 - No value. This criterion cannot be applied.
5. If necessary, set up other rule properties in the other sections.

The moving rule is configured.

See also:

Step 4. Segment polling, configuring synchronization with Cloud and choosing further actions[1374](#)

Creating Backup of the Administration Server data task by using a cloud DBMS

This section describes features applicable only to Kaspersky Security Center 12.1 or a later version.

Backup tasks are Administration Server tasks. You create a backup task if you want to use a DBMS located in a cloud environment (AWS or Azure).

To create an Administration Server data backup task:

1. Go to **DEVICES** → **TASKS**.
2. Click **Add**.
The New Task Wizard starts.
3. On the first page of the Wizard, in the **Application** list, select **Kaspersky Security Center 13**, and in the **Task type** list, select **Backup of Administration Server data**.
4. On the corresponding page of the Wizard, specify the following information:
 - If you are working with a database in AWS:
 - **S3 bucket name**

The name of the S3 bucket (see section "Preparing Amazon S3 bucket for database" on page [840](#)) that you created for the Backup.

- **Access key ID**

You received the key ID (sequence of alphanumeric characters) when you created the IAM user account (see section "Creating an IAM user account for work with Kaspersky Security Center" on page [833](#)) for working with S3 bucket storage instance.

The field is available if you selected RDS database on an S3 bucket.

- **Secret key**

The secret key that you received with the access key ID when you created the IAM user account (see section "Creating an IAM user account for work with Kaspersky Security Center" on page [833](#)).

The characters of the secret key are displayed as asterisks. After you begin entering the secret key, the **Show** button is displayed. Click and hold this button for the necessary amount of time to view the characters you entered.

The field is available if you selected an AWS IAM access key for authorization instead of an IAM role.

- If you are working with a database in Microsoft Azure:

- **Azure storage account name**

You created the name of the Azure storage account (see section "Creating Azure storage account" on page [846](#)) for working with Kaspersky Security Center.

- **Azure Subscription ID**

You created (see section "Creating a subscription, Application ID, and password" on page [843](#)) the subscription on the Azure portal.

- **Azure password**

You received the password of the Application ID when you created the Application ID (see section "Creating a subscription, Application ID, and password" on page [843](#)).

The characters of the password are displayed as asterisks. After you begin entering the password, the **Show** button becomes available. Click and hold this button to view the characters you entered.

- **Azure Application ID**

You created (see section "Creating a subscription, Application ID, and password" on page [843](#)) this application ID on the Azure portal.

You can provide only one Azure Application ID for polling and other purposes. If you want to poll another Azure segment, you must first delete the existing Azure connection.

- **Azure SQL server name**

The name and the resource group are available in your Azure SQL Server properties.

- **Azure SQL server resource group**

The name and the resource group are available in your Azure SQL Server properties.

- **Azure storage access key**

Available in the properties of your storage account (see section "Working with Azure SQL" on page [846](#)), in the Access Keys section. You can use any of the keys (key1 or

key2).

The task is created and displayed in the list of tasks. If you enable the **Open task details when creation is complete** option, you can modify the default task settings immediately after the task is created. If you do not enable this option, the task is created with the default settings. You can modify the default settings later, at any time.

Remote diagnostics of client devices

This section describes features applicable only to Kaspersky Security Center 12.1 or a later version.

You can use remote diagnostics for remote execution of the following operations on client devices:

- Enabling and disabling tracing, changing the tracing level, and downloading the trace file.
- Downloading system information and application settings.
- Downloading event logs.
- Generating a dump file for an application.
- Starting diagnostics and downloading diagnostics reports.
- Starting, stopping, and restarting applications.

You can use event logs and diagnostics reports downloaded from a client device to troubleshoot problems on your own. Also, if you contact Kaspersky Technical Support, a Technical Support specialist might ask you to download trace files, dump files, event logs, and diagnostics reports from a client device for further analysis at Kaspersky.

The remote diagnostics is performed using Administration Server.

In this section

Opening the remote diagnostics window	1388
Enabling and disabling tracing for applications	1388
Downloading trace files of an application	1390
Deleting trace files	1391
Downloading application settings	1391
Downloading event logs.....	1392
Starting, stopping, restarting the application	1392
Running the remote diagnostics of an application and downloading the results.....	1393
Running an application on a client device	1393

Opening the remote diagnostics window

This section describes features applicable only to Kaspersky Security Center 12.1 or a later version.

To perform remote diagnostics on a client device, you first have to open the remote diagnostics window.

► *To open the remote diagnostics window:*

1. To select the device for which you want to open the remote diagnostics window, perform one of the following:
 - If the device belongs to an administration group, go to **DEVICES** → **Groups** → **<group name>** → **MANAGED DEVICES**.
 - If the device belongs to the Unassigned devices group, go to **DISCOVERY & DEPLOYMENT** → **UNASSIGNED DEVICES**.
2. Click the name of the required device.
3. In the device properties window that opens, select the **Advanced** tab.
4. In the window that opens, in the left pane, select **Remote diagnostics**.

This opens the **Remote diagnostics** window of a client device.

Enabling and disabling tracing for applications

This section describes features applicable only to Kaspersky Security Center 12.1 or a later version.

You can enable and disable tracing for applications, including Xperf tracing.

Enabling and disabling tracing

► *To enable or disable tracing on a remote device:*

1. Open the remote diagnostics window of a client device (see section "Opening the remote diagnostics window" on page [1388](#)).
2. In the remote diagnostics window, click **Remote diagnostics**.
3. In the **Statuses and logs** window that opens, select the **Kaspersky applications** section.
This opens the list of Kaspersky applications installed on the device.
4. In the application list, select the application for which you want to enable or disable tracing.
The list of remote diagnostics options is displayed.
5. If you want to enable tracing:
 - a. In the **Tracing** section of the list, click **Enable tracing**.
 - b. In the **Modify tracing level** window that opens, we recommend that you keep the default values of the settings. When required, a Technical Support specialist will guide you through the configuration process. The following settings are available:

- **Tracing level**

The tracing level defines the amount of detail that the trace file contains.

- **Rotation-based tracing**

The application overwrites the tracing information to prevent excessive increase in the size of the trace file. Specify the maximum number of files to be used to store the tracing information, and the maximum size of each file. If the maximum number of trace files of the maximum size are written, the oldest trace file is deleted so that a new trace file can be written.

This setting is available for Kaspersky Endpoint Security only.

- a. Click **Save**.

The tracing is enabled for the selected application. In some cases, the security application and its task must be restarted in order to enable tracing.

1. If you want to disable tracing for the selected application, click **Disable tracing**.

The tracing is disabled for the selected application.

Enabling Xperf tracing

For Kaspersky Endpoint Security, a Technical Support specialist may ask you to enable Xperf tracing for information about the system performance.

► *To enable and configure Xperf tracing:*

1. Open the remote diagnostics window of a client device (see section "Opening the remote diagnostics window" on page [1388](#)).

2. In the remote diagnostics window, click **Remote diagnostics**.

3. In the **Statuses and logs** window that opens, select the **Kaspersky applications** section.

This opens the list of Kaspersky applications installed on the device.

4. In the list of applications, select Kaspersky Endpoint Security for Windows.

The list of remote diagnostics options for Kaspersky Endpoint Security for Windows is displayed.

5. In the **Xperf tracing** section of the list, click **Enable Xperf tracing**.

If Xperf tracing is already enabled, the **Disable Xperf tracing** button is displayed instead.

6. In the **Change Xperf tracing level** window that opens, depending on the request from the Technical Support specialist, do the following:

- a. Select one of the following tracing levels:

- **Light level**

A trace file of this type contains the minimum amount of information about the system.

By default, this option is selected.

- **Deep level**

A trace file of this type contains more detailed information than trace files of the *Light* type and may be requested by Technical Support specialists when a trace file of the *Light* type is not enough for the performance evaluation. A *Deep* trace file contains technical information about the system including information about hardware, operating system, list of started and finished processes and applications, events used for performance evaluation, and events from Windows System Assessment Tool.

- b. Select one of the following Xperf tracing types:

- **Basic type**

The tracing information is received during operation of the Kaspersky Endpoint Security

application.

By default, this option is selected.

- **On-restart type**

The tracing information is received when the operating system starts on the managed device. This tracing type is effective when the issue that affects the system performance occurs after the device is turned on and before Kaspersky Endpoint Security starts.

You may also be asked to enable the **Rotation file size, in MB** option to prevent excessive increase in the size of the trace file. Then specify the maximum size of the trace file. When the file reaches the maximum size, the oldest tracing information is overwritten with new information.

- c. Define the rotation file size.
- d. Click **Save**.

Xperf tracing is enabled and configured.

► *To disable Xperf tracing:*

1. Open the remote diagnostics window of a client device (see section "Opening the remote diagnostics window" on page [1388](#)).
2. In the remote diagnostics window, click **Remote diagnostics**.
3. In the **Statuses and logs** window that opens, select the **Kaspersky applications** section.
This opens the list of Kaspersky applications installed on the device.
4. In the list of applications, select Kaspersky Endpoint Security for Windows.
The tracing options for Kaspersky Endpoint Security for Windows are displayed.
5. In the **Xperf tracing** section of the list, click **Disable Xperf tracing**.

If Xperf tracing is already disabled, then the **Enable Xperf tracing** button is displayed instead.

Xperf tracing is disabled.

Downloading trace files of an application

This section describes features applicable only to Kaspersky Security Center 12.1 or a later version.

► *To download a trace file of an application:*

1. Open the remote diagnostics window of a client device (see section "Opening the remote diagnostics window" on page [1388](#)).
2. In the remote diagnostics window, click **Remote diagnostics**.
3. In the **Statuses and logs** window that opens, select the **Kaspersky applications** section.
This opens the list of Kaspersky applications installed on the device.
In the **Tracing** section, click the **Trace files** button.
This opens the **Device tracing logs** window, where a list of trace files is displayed.
4. In the list of trace files, select the file that you want.
5. Do one of the following:

- Download the selected file by clicking the **Download entire file**.
- Download a portion of the selected file:
 - a. Click **Download a portion**.
 - b. In the window that opens, specify the name and the file portion to download, according to your needs.
 - c. Click **Download**.

The selected file, or its portion, is downloaded to the location that you specify.

Deleting trace files

This section describes features applicable only to Kaspersky Security Center 12.1 or a later version.

You can delete trace files that are no longer needed.

► *To delete a trace file:*

1. Open the remote diagnostics window of a client device (see section "Opening the remote diagnostics window" on page [1388](#)).
2. In the remote diagnostics window that opens, click **Remote diagnostics**.
3. In the **Statuses and logs** window that opens, make sure that the **Operating system logs** section is selected.
4. In the **Trace files** section, click the **Windows Update logs** button or **Remote installation logs** button, depending on which trace files you want to delete.

This opens the list of trace files.

5. In the list of trace files, select the file that you want to delete.
6. Click the **Remove** button.

The selected trace file is deleted.

Downloading application settings

This section describes features applicable only to Kaspersky Security Center 12.1 or a later version.

► *To download application settings from a client device:*

1. Open the remote diagnostics window of a client device (see section "Opening the remote diagnostics window" on page [1388](#)).
2. In the remote diagnostics window that opens, click **Remote diagnostics**.
3. In the **Statuses and logs** window that opens, make sure that the **Operating system logs** is selected in the right pane.

- In the **System Info** section, click the **Download file** button to download the system information about the client device.
- In the **Application settings** section, click the **Download file** button to download information about the settings of the applications installed on the device.

The information is downloaded to the location that you specify as a file.

Downloading event logs

This section describes features applicable only to Kaspersky Security Center 12.1 or a later version.

► *To download an event log from a remote device:*

1. Open the remote diagnostics window of a client device (see section "Opening the remote diagnostics window" on page [1388](#)).
2. In the remote diagnostics window, click **Device logs**.
3. In the **All device logs** window, select the relevant log.
4. Do one of the following:
 - Download the selected log by clicking **Download entire file**.
 - Download a portion of the selected log:
 - a. Click **Download a portion**.
 - b. In the window that opens, specify the name and the file portion to download, according to your needs.
 - c. Click **Download**.

The selected event log, or a portion of it, is downloaded to the location that you specify.

Starting, stopping, restarting the application

This section describes features applicable only to Kaspersky Security Center 12.1 or a later version.

You can start, stop, and restart applications on a client device.

► *To start, stop, or restart an application:*

1. Open the remote diagnostics window of a client device (see section "Opening the remote diagnostics window" on page [1388](#)).
2. In the remote diagnostics window, click **Remote diagnostics**.
3. In the **Statuses and logs** window that opens, select the **Kaspersky applications** section.
This opens the list of Kaspersky applications installed on the device.
4. In the list of applications, select the application that you want to start, stop, or restart.
5. Select an action by clicking one of the following buttons:
 - **Stop application**
This button is available only if the application is currently running.

- **Restart application**

This button is available only if the application is currently running.

- **Start application**

This button is available only if the application is not currently running.

Depending on the action that you have selected, the required application is started, stopped, or restarted on the client device.

If you restart the Network Agent, a message is displayed stating that the current connection of the device to the Administration Server will be lost.

Running the remote diagnostics of an application and downloading the results

This section describes features applicable only to Kaspersky Security Center 12.1 or a later version.

► *To start diagnostics for an application on a remote device and download the results:*

1. Open the remote diagnostics window of a client device (see section "Opening the remote diagnostics window" on page [1388](#)).
2. In the remote diagnostics window, click **Remote diagnostics**.
3. In the **Statuses and logs** window that opens, select the **Kaspersky applications** section.
This opens the list of Kaspersky applications installed on the device.
4. In the list of applications, select the application for which you want to run remote diagnostics.
The list of remote diagnostics options is displayed.
5. In the **Diagnostics report** section of the list, click the **Run diagnostics** button.
This starts the remote diagnostics process and generates a diagnostics report. When the diagnostics process is complete, the **Download diagnostics report** button becomes available.
6. Download the report by clicking the **Download diagnostics report** button.

The report is downloaded to the location that you specified.

Running an application on a client device

This section describes features applicable only to Kaspersky Security Center 12.1 or a later version.

You may have to run an application on the client device, if a Kaspersky support specialist requests it.

You do not have to install the application on that device.

► *To run an application on the client device:*

1. Open the remote diagnostics window of a client device (see section "Opening the remote diagnostics window" on page [1388](#)).
2. In the remote diagnostics window that opens, click **Remote diagnostics**.
3. In the **Statuses and logs** window that opens, select the **Running a remote application** section.

4. In the **Running a remote application** window, in the **Application files** section, do one of the following, according to what a Kaspersky specialist asks you to do:
 - Select a ZIP archive containing the application that you want to run on the client device by clicking the **Browse** button.
 - Specify a command-line application and its arguments, if necessary.
5. Follow the instructions of the specialist.

API Reference Guide

This Kaspersky Security Center OpenAPI reference guide is designed to assist in the following tasks:

- Automation and customization. You can automate (see section "Kaspersky Security Center operation automation. klakout utility" on page [889](#)) tasks that you might not want to handle manually by using Administration Console. You can also implement custom scenarios that are not yet supported in Administration Console. For example, as an administrator, you can use Kaspersky Security Center OpenAPI to create and run scripts that will facilitate developing the structure of administration groups and keep that structure up-to-date.
- Custom development. For example, you can develop an alternative MMC-based Administration Console for your clients, which permits a limited set of actions.

You can use the search field in the right part of the screen to locate the information you need in the OpenAPI reference guide.



OPENAPI REFERENCE GUIDE

https://click.kaspersky.com/?hl=KSCAPI&link=online_help&pid=KSC&version=13.0.0&helpid=index

You can find examples of the matching between some user scenarios and OpenAPI methods in the table below.

Table 99. Matching between user scenarios and samples of Kaspersky Security Center OpenAPI

Scenario	Sample	Purpose of the sample
Kaspersky Security Center 13 Web Console activity logging	Log KlAkParams https://click.kaspersky.com/?hl=KSCAPI&link=online_help&pid=KSC&version=13.0.0&helpid=a00404	This module presents samples of using the <code>KlAkOAPIWrapperLib</code> package to parse, compose, and output the <code>KlAkParams</code> object. <code>KlAkParams</code> corresponds to parameters container that is part of Kaspersky Security Center OpenAPI.
Configuring Administration Server	Create and destroy a primary / secondary relationship https://click.kaspersky.com/?hl=KSCAPI&link=online_help&pid=KSC&version=13.0.0&helpid=a00405	This module presents samples of using the <code>KlAkOAPIWrapperLib</code> package to create a primary / secondary relationship.
Configuring Administration Server	Create a group structure based on the Active Directory organization units' structure https://click.kaspersky.com/?hl=KSCAPI&link=online_help&pid=KSC&version=13.0.0&helpid=a00406	This module presents samples of using the <code>KlAkOAPIWrapperLib</code> package to create a group structure that is the same as the Active Directory organizational unit structure.
Configuring Administration Server	Create a group structure based on the cached Active Directory organizational unit structure https://click.kaspersky.com/?hl=KSCAPI&link=online_help&pid=KSC&version=13.0.0&helpid=a00407	This module presents samples of using the <code>KlAkOAPIWrapperLib</code> package to create a group structure based on the cached Active Directory organizational unit structure.
Configuring network protection	Create IP subnets based on Active Directory Site and Services https://click.kaspersky.com/?hl=KSCAPI&link=online_help&pid=KSC&version=13.0.0&helpid=a00408	This module presents samples of using the <code>KlAkOAPIWrapperLib</code> package to create IP subnets based on Active Directory Site and Services.
Updating Kaspersky databases and applications	Register update agents for devices in a group https://click.kaspersky.com/?hl=KSCAPI&link=online_help&pid=KSC&version=13.0.0&helpid=a00409	This module presents samples of using the <code>KlAkOAPIWrapperLib</code> package to set update agents.
Configuring Administration Server	Enumerate all groups https://click.kaspersky.com/?hl=KSCAPI&link=online_help&pid=KSC&version=13.0.0&helpid=a00410	This module presents samples of using the <code>KlAkOAPIWrapperLib</code> package to enumerate groups.

Scenario	Sample	Purpose of the sample
Configuring Administration Server	Enumerate tasks, query task statistics, and run a task https://click.kaspersky.com/?hl=KSCAPI&link=online_help&pid=KSC&version=13.0.0&helpid=a00411	This module presents samples of using the <code>KlAkOAPIWrapperLib</code> package to find and execute a task by name.
Configuring Administration Server	Create and run a task https://click.kaspersky.com/?hl=KSCAPI&link=online_help&pid=KSC&version=13.0.0&helpid=a00412	This module presents samples of using the <code>KlAkOAPIWrapperLib</code> package to create a task.
Kaspersky applications: licensing and activation	Enumerate license keys https://click.kaspersky.com/?hl=KSCAPI&link=online_help&pid=KSC&version=13.0.0&helpid=a00413	This module presents samples of using the <code>KlAkOAPIWrapperLib</code> package to view licenses.
Configuring network protection	Create and find an internal user https://click.kaspersky.com/?hl=KSCAPI&link=online_help&pid=KSC&version=13.0.0&helpid=a00414	This module presents samples of using the <code>KlAkOAPIWrapperLib</code> package to add an internal user.
Configuring network protection	Create a custom category https://click.kaspersky.com/?hl=KSCAPI&link=online_help&pid=KSC&version=13.0.0&helpid=a00415	This module presents samples of using the <code>KlAkOAPIWrapperLib</code> package to create a custom category.
Configuring network protection	Enumerate users by using <code>SrvView</code> https://click.kaspersky.com/?hl=KSCAPI&link=online_help&pid=KSC&version=13.0.0&helpid=a00416	This module presents samples of using the <code>KlAkOAPIWrapperLib</code> package to iterate over <code>SrvView</code> .

Best Practices for Service Providers

This section provides information about how to configure and use Kaspersky Security Center.

This section contains recommendations on how to deploy, configure, and use the application, as well as describes ways of resolving typical issues in the application operation.

Best Practices for Service Providers:

<https://support.kaspersky.com/KSC/13/en-US/155352.htm>

Sizing Guide

This section provides information about Kaspersky Security Center sizing.

Sizing Guide:

<https://support.kaspersky.com/KSC/13/en-US/162088.htm>

Contact Technical Support

This section describes how to get technical support and the terms on which it is available.

In this chapter

How to get technical support	1401
Get technical support by phone	1401
Technical Support via Kaspersky CompanyAccount.....	1402

How to get technical support

If you can't find a solution to your issue in the application documentation or in any of the sources of information about the application, contact Technical Support. Technical Support specialists will answer all your questions about installing and using the application.

Kaspersky provides support of this application during its lifecycle (see the product support lifecycle page (<https://support.kaspersky.com/corporate/lifecycle>)). Before contacting Technical Support, please read the support rules (https://support.kaspersky.com/support/rules#en_us).

You can contact Technical Support in one of the following ways:

- By calling Technical Support (<https://support.kaspersky.com/b2b>)
- By sending a request to Technical Support from the Kaspersky CompanyAccount portal (<https://companyaccount.kaspersky.com>)

Technical support is available only to users who purchased a commercial license. Users who have received a trial license are not entitled to technical support.

Get technical support by phone

You can call Technical Support specialists from most regions worldwide. You can find information about how to obtain technical support in your region and contact information for Technical Support on the Kaspersky Technical Support website (<https://support.kaspersky.com/b2b>).

Before contacting Technical Support, please read the support rules (https://support.kaspersky.com/support/rules#en_us).

Technical Support via Kaspersky CompanyAccount

Kaspersky CompanyAccount (<https://companyaccount.kaspersky.com>) is a portal for companies that use Kaspersky applications. The Kaspersky CompanyAccount portal is designed to facilitate interaction between users and Kaspersky specialists through online requests. You can use Kaspersky CompanyAccount to track the status of your online requests and store a history of them as well.

You can register all of your organization's employees under a single account on Kaspersky CompanyAccount. A single account lets you centrally manage electronic requests from registered employees to Kaspersky and also manage the privileges of these employees via Kaspersky CompanyAccount.

The Kaspersky CompanyAccount portal is available in the following languages:

- English
- Spanish
- Italian
- German
- Polish
- Portuguese
- Russian
- French
- Japanese

To learn more about Kaspersky CompanyAccount, visit the Technical Support website (https://support.kaspersky.com/faq/companyaccount_help).

Sources of information about the application

Kaspersky Security Center page on the Kaspersky website

On the Kaspersky Security Center page on the Kaspersky website (<https://www.kaspersky.com/small-to-medium-business-security/security-center>), you can view general information about the application, its functions, and features.

Kaspersky Security Center page in the Knowledge Base

The *Knowledge Base* is a section on the Kaspersky Technical Support website.

On the Kaspersky Security Center page in the Knowledge Base, you can read articles that provide useful information, recommendations, and answers to frequently asked questions on how to buy, install, and use the application.

Articles in the Knowledge Base may provide answers to questions that relate both to Kaspersky Security Center as well as to other Kaspersky applications. Articles in the Knowledge Base may also contain Technical Support news.

Discuss Kaspersky applications with the community

If your question does not require an immediate answer, you can discuss it with Kaspersky experts and other users in our community (<https://community.kaspersky.com/>).

In the community, you can view discussion topics, post your comments, and create new discussion topics.

An Internet connection is required to access website resources.

If you cannot find a solution to your problem, contact Technical Support (see section "How to get technical support" on page [1401](#)).

Glossary

A

Active key

A license key that is currently used by the application.

Additional license key

A key that certifies the right to use the application but is not currently being used.

Administration Console

A Kaspersky Security Center component that provides a user interface for the administrative services of Administration Server and Network Agent.

Administration group

A set of devices grouped by function and by installed Kaspersky applications. Devices are grouped as a single entity for the convenience of management. A group can include other groups. Group policies and group tasks can be created for each installed application in the group.

Administration Server

A component of Kaspersky Security Center that centrally stores information about all Kaspersky applications that are installed on the corporate network. It can also be used to manage these applications.

Administration Server certificate

The certificate used for the Administration Server authentication during connection of Administration Consoles to it and data exchange with client computers. The Administration Server certificate is created and installed on Administration Server in the ALLUSERSPROFILE%\Application Data\KasperskyLab\adminikit\1093\cert folder.

Administration Server client (Client device)

A device, server, or workstation on which Network Agent is installed and managed Kaspersky applications are running.

Administration Server data backup

Copying of the Administration Server data for backup and subsequent restoration performed by using the backup utility. The utility can save:

- Database of the Administration Server (policies, tasks, application settings, events saved on the Administration Server)
- Configuration information about the structure of administration groups and client devices
- Repository of the installation files for remote installation of applications (content of the folders: Packages, Uninstall Updates)

- Administration Server certificate

Administrator rights

The level of the user's rights and privileges required for administration of Exchange objects within an Exchange organization.

Administrator's workstation

A device with Administration Console installed. This component provides a Kaspersky Security Center management interface.

The administrator's workstation is used to configure and manage the server side of Kaspersky Security Center. Using the administrator's workstation, the administrator builds and manages a centralized anti-virus protection system for a corporate LAN based on Kaspersky applications.

Amazon EC2 instance

A virtual machine created based on an AMI image using Amazon Web Services.

Amazon Machine Image (AMI)

The template containing the software configuration necessary for running the virtual machine. Multiple instances can be created based on a single AMI.

Anti-virus databases

Databases that contain information about computer security threats known to Kaspersky as of when the anti-virus databases are released. Entries in anti-virus databases allow malicious code to be detected in scanned objects. Anti-virus databases are created by Kaspersky specialists and updated hourly.

Anti-virus protection service provider

An organization that provides a client organization with anti-virus protection services based on Kaspersky solutions.

Application Shop

Component of Kaspersky Security Center. Application Shop is used for installing applications on Android devices owned by users. Application Shop allows you to publish the APK files of applications and links to applications in Google Play.

Authentication Agent

Interface that lets you complete authentication to access encrypted hard drives and load the operating system after the bootable hard drive has been encrypted.

Available update

A set of updates for Kaspersky application modules, including critical updates accumulated over a certain period of time and changes to the application's architecture.

AWS Application Program Interface (AWS API)

The application programming interface of the AWS platform that is used by Kaspersky Security Center. Specifically, AWS API tools are used for cloud segment polling and installing Network Agent on instances.

AWS IAM access key

A combination consisting of the key ID (which looks like "AKIAIOSFODNN7EXAMPLE") and secret key (which looks like "wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY"). This pair belongs to the IAM user and is used to obtain access to AWS services.

AWS Management Console

The web interface for viewing and managing AWS resources. AWS Management Console is available on the web at <https://aws.amazon.com/console/>.

B

Backup folder

Special folder for storage of Administration Server data copies created using the backup utility.

Broadcast domain

A logical area of a network in which all nodes can exchange data using a broadcasting channel at the level of OSI (Open Systems Interconnection Basic Reference Model).

C

Centralized application management

Remote application management using the administration services provided in Kaspersky Security Center.

Client administrator

A staff member of a client organization who is responsible for monitoring the anti-virus protection status.

Cloud environment

Virtual machines and other virtual resources that are based on a cloud platform and are combined into networks.

Configuration profile

Policy that contains a collection of settings and restrictions for an iOS MDM mobile device.

Connection gateway

A connection gateway is a Network Agent acting in a special mode. A connection gateway accepts connections from other Network Agents and tunnels them to the Administration Server through its own connection with the Server. Unlike an ordinary Network Agent, a connection gateway waits for connections from the Administration Server rather than establishes connections to the Administration Server.

D

Demilitarized zone (DMZ)

Demilitarized zone is a segment of a local network that contains servers, which respond to requests from the global Web. In order to ensure the security of an organization's local network, access to the LAN from the demilitarized zone is protected with a firewall.

Device owner

Device owner is a user whom the administrator can contact when the need arises to perform certain operations on a device.

Direct application management

Application management through a local interface.

Distribution point

Computer that has Network Agent installed and is used for update distribution, remote installation of applications, getting information about computers in an administration group and / or broadcasting domain. Distribution points are designed to reduce the load on the Administration Server during update distribution and to optimize network traffic. Distribution points can be assigned automatically, by the Administration Server, or manually, by the administrator. Distribution point was previously known as update agent.

E

EAS device

A mobile device connected to Administration Server through the Exchange ActiveSync protocol. Devices with the iOS, Android, and Windows Phone® operating systems can be connected and managed by using the Exchange ActiveSync protocol.

Event repository

A part of the Administration Server database dedicated to storage of information about events that occur in Kaspersky Security Center.

Event severity

Property of an event encountered during the operation of a Kaspersky application. There are the following severity levels:

- Critical event

- Functional failure
- Warning
- Info

Events of the same type can have different severity levels depending on the situation in which the event occurred.

Exchange Mobile Device Server

A component of Kaspersky Security Center that allows you to connect Exchange ActiveSync mobile devices to the Administration Server.

F

Forced installation

Method for remote installation of Kaspersky applications that allows you to install software on specific client devices. For successful forced installation, the account used for the task must have sufficient rights to start applications remotely on client devices. This method is recommended for installing applications on devices that are running Microsoft Windows operating systems and that support this functionality.

G

Group task

A task defined for an administration group and performed on all client devices included in that administration group.

H

Home Administration Server

Home Administration Server is the Administration Server that was specified during Network Agent installation. The home Administration Server can be used in settings of Network Agent connection profiles.

HTTPS

Secure protocol for data transfer, using encryption, between a browser and a web server. HTTPS is used to gain access to restricted information, such as corporate or financial data.

I

IAM role

Set of rights for making requests to AWS-based services. IAM roles are not linked to a specific user or group; they provide access rights without AWS IAM access keys. You can assign an IAM role to IAM users, EC2 instances, and AWS-based applications or services.

IAM user

The user of AWS services. An IAM user may have the rights to perform cloud segment polling.

Identity and Access Management (IAM)

The AWS service that enables management of user access to other AWS services and resources.

Incompatible application

An anti-virus application from a third-party developer or a Kaspersky application that does not support management through Kaspersky Security Center.

Installation package

A set of files created for remote installation of a Kaspersky application by using the Kaspersky Security Center remote administration system. The installation package contains a range of settings needed to install the application and get it running immediately after installation. Settings correspond to application defaults. The installation package is created using files with the .kpd and .kud extensions included in the application distribution kit.

Internal users

The accounts of internal users are used to work with virtual Administration Servers. Kaspersky Security Center grants the rights of real users to internal users of the application.

The accounts of internal users are created and used only within Kaspersky Security Center. No data on internal users is transferred to the operating system. Kaspersky Security Center authenticates internal users.

iOS MDM device

A mobile device that is connected to the iOS MDM Server by using the iOS MDM protocol. Devices running the iOS operating system can be connected and managed by means of the iOS MDM protocol.

iOS MDM profile

Collection of settings for connecting iOS mobile devices to Administration Server. The user installs an iOS MDM profile to a mobile device, after which this mobile device connects to Administration Server.

iOS MDM Server

A component of Kaspersky Security Center that is installed on a client device, allowing connection of iOS mobile devices to the Administration Server and management of iOS mobile devices through Apple Push Notifications (APNs).

J

JavaScript

A programming language that expands the performance of web pages. Web pages created using JavaScript can perform functions (for example, change the view of interface elements or open additional windows) without refreshing the web page with new data from a web server. To view pages created by using JavaScript, enable JavaScript support in the configuration of your browser.

K

Kaspersky Private Security Network (Private KSN)

Kaspersky Private Security Network is a solution that gives users of devices with Kaspersky applications installed access to reputation databases of Kaspersky Security Network and other statistical data—without sending data from their devices to Kaspersky Security Network. Kaspersky Private Security Network is designed for corporate customers who are unable to participate in Kaspersky Security Network for any of the following reasons:

- User devices are not connected to the Internet.
- Transmission of any data outside the country or the corporate LAN is prohibited by law or corporate security policies.

Kaspersky Security Center Administrator

The person managing application operations through the Kaspersky Security Center remote centralized administration system.

Kaspersky Security Center Operator

A user who monitors the status and operation of a protection system managed with Kaspersky Security Center.

Kaspersky Security Center System Health Validator (SHV)

A component of Kaspersky Security Center designed for checking the operating system's operability in case of concurrent operation of Kaspersky Security Center and Microsoft NAP.

Kaspersky Security Center Web Server

A component of Kaspersky Security Center that is installed together with Administration Server. Web Server is designed for transmission, over a network, of stand-alone installation packages, iOS MDM profiles, and files from a shared folder.

Kaspersky Security Network (KSN)

An infrastructure of cloud services that provides access to the Kaspersky database with constantly updated information about the reputation of files, web resources, and software. Kaspersky Security Network ensures faster responses by Kaspersky applications to threats, improves the performance of some protection components, and reduces the likelihood of false positives.

Kaspersky update servers

HTTP(S) servers at Kaspersky from which Kaspersky applications download database and application module updates.

KES device

A mobile device that is connected to Administration Server and managed through Kaspersky Endpoint Security for Android.

Key file

A file in xxxxxxxx.key format that makes it possible to use a Kaspersky application under a trial or commercial license.

L

License term

A time period during which you have access to the application features and rights to use additional services. The services you can use depend on the type of the license.

Licensed applications group

A group of applications created on the basis of criteria set by the administrator (for example, by vendor), for which statistics of installations on client devices are maintained.

Local installation

Installation of a security application on a device on a corporate network that presumes manual installation startup from the distribution package of the security application or manual startup of a published installation package that was pre-downloaded to the device.

Local task

A task defined and running on a single client computer.

M

Managed devices

Corporate networked devices that are included in an administration group.

Management plug-in

A specialized component that provides the interface for application management through Administration Console. Each application has its own plug-in. It is included in all Kaspersky applications that can be managed by using Kaspersky Security Center.

Manual installation

Installation of a security application on a device in the corporate network from the distribution package. Manual installation requires the involvement of an administrator or another IT specialist. Usually manual installation is done if remote installation has completed with an error.

Mobile Device Server

A component of Kaspersky Security Center that provides access to mobile devices and allows you to manage them through Administration Console.

N

Network Agent

A Kaspersky Security Center component that enables interaction between the Administration Server and Kaspersky applications that are installed on a specific network node (workstation or server). This component is common to all of the company's applications for Microsoft® Windows®. Separate versions of Network Agent exist for Kaspersky applications developed for Unix-like OS and macOS.

Network anti-virus protection

A set of technical and organizational measures that lower the risk of allowing viruses and spam to penetrate the network of an organization, and that prevent network attacks, phishing, and other threats. Network security increases when you use security applications and services and when you apply and adhere to the corporate data security policy.

Network protection status

Current protection status, which defines the safety of corporate networked devices. The network protection status includes such factors as installed security applications, usage of license keys, and number and types of threats detected.

P

Patch importance level

Attribute of the patch. There are five importance levels for Microsoft patches and third-party patches:

- Critical
- High
- Medium
- Low
- Unknown

The importance level of a third-party patch or Microsoft patch is determined by the least favorable severity level among the vulnerabilities that the patches should fix.

Policy

A policy determines an application's settings and manages the ability to configure that application on computers within an administration group. An individual policy must be created for each application. You can create multiple policies for applications installed on computers in each administration group, but only one policy can be applied at a time to each application within an administration group.

Profile

Collection of settings of Exchange mobile devices that define their behavior when connected to a Microsoft Exchange Server.

Program settings

Application settings that are common to all types of tasks and govern the overall operation of the application, such as application performance settings, report settings, and backup settings.

Protection status

Current protection status, which reflects the level of computer security.

Provisioning profile

Collection of settings for applications' operation on iOS mobile devices. A provisioning profile contains information about the license; it is linked to a specific application.

R

Remote installation

Installation of Kaspersky applications by using the services provided by Kaspersky Security Center.

Restoration

Relocation of the original object from Quarantine or Backup to its original folder where the object had been stored before it was quarantined, disinfected or deleted, or to a user-defined folder.

Restoration of Administration Server data

Restoration of Administration Server data from the information saved in Backup by using the backup utility. The utility can restore:

- Database of the Administration Server (policies, tasks, application settings, events saved on the Administration Server)
- Configuration information about the structure of administration groups and client computers
- Repository of the installation files for remote installation of applications (content of the folders: Packages, Uninstall Updates)
- Administration Server certificate

Role group

A group of users of Exchange ActiveSync mobile devices who have been granted identical administrator rights (on page [1405](#)).

S

Service provider's administrator

A staff member at an anti-virus protection service provider. This administrator performs installation and maintenance jobs for anti-virus protection systems based on Kaspersky anti-virus products and also provides technical support to customers.

Shared certificate

A certificate intended for identifying the user's mobile device.

SSL

A data encryption protocol used on the Internet and local networks. The Secure Sockets Layer (SSL) protocol is used in web applications to create a secure connection between a client and server.

T

Task

Functions performed by the Kaspersky application are implemented as tasks, such as: Real-time file protection, Full computer scan, and Database update.

Task for specific devices

A task assigned to a set of client devices from arbitrary administration groups and performed on those devices.

Task settings

Application settings that are specific for each task type.

U

UEFI protection device

Device with Kaspersky Anti-Virus for UEFI integrated at the BIOS level. Integrated protection ensures device security from the moment the system starts, while protection on devices without integrated software begins functioning only after the security application starts.

Update

The procedure of replacing / adding new files (databases or application modules) retrieved from the Kaspersky update servers.

V

Virtual Administration Server

A component of Kaspersky Security Center, designed for management of the protection system of a client organization's network.

Virtual Administration Server is a particular case of a secondary Administration Server and has the following restrictions as compared with a physical Administration Server:

- Virtual Administration Server can be created only on a primary Administration Server.
- Virtual Administration Server uses the primary Administration Server database in its operation. Data backup and restoration tasks, as well as update scan and download tasks, are not supported on a virtual Administration Server.
- Virtual Server does not support creation of secondary Administration Servers (including virtual Servers).

Virus activity threshold

Maximum allowed number of events of the specified type within a limited time; when this number is exceeded, it is interpreted as increased virus activity and as a threat of a virus outbreak. This feature is important during periods of virus outbreaks because it enables administrators to respond in a timely manner to virus attack threats.

Virus outbreak

A series of deliberate attempts to infect a device with a virus.

Vulnerability

A flaw in an operating system or an application that may be exploited by malware makers to penetrate the operating system or application and corrupt its integrity. Presence of a large number of vulnerabilities in an operating system makes it unreliable, because viruses that penetrate the operating system may cause disruptions in the operating system itself and in installed applications.

W

Windows Server Update Services (WSUS)

An application used for distribution of updates for Microsoft applications on users' computers in an organization's network.

Information about third-party code

Information about third-party code is contained in the file legal_notices.txt, in the application installation folder.

Trademark notices

Registered trademarks and service marks are the property of their respective owners.

Active Directory, ActiveSync, BitLocker, Excel, Forefront, Internet Explorer, InfoPath, Hyper-V, Microsoft, MultiPoint, MS-DOS, PowerShell, PowerPoint, SharePoint, SQL Server, OneNote, Outlook, Tahoma, Visio, Win32, Windows, Windows PowerShell, Windows Media, Windows Server, Windows Phone, Windows Vista, and Windows Azure are registered trademarks of Microsoft Corporation in the United States and other countries.

Adobe, Acrobat, Flash and PostScript are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

AirPlay, AirDrop, AirPrint, App Store, Apple, Apple Configurator, AppleScript, FaceTime, FileVault, iBook, iBooks, iPad, iPhone, iTunes, Leopard, macOS, Mac, Mac OS, OS X, Safari, Snow Leopard, Tiger, QuickTime, and Touch ID are trademarks of Apple Inc., registered in the U.S. and other countries.

AMD, AMD64 are trademarks or registered trademarks of Advanced Micro Devices, Inc.

Amazon, Amazon Web Services, AWS, Amazon EC2, AWS Marketplace are trademarks of Amazon.com, Inc. or its affiliates in the United States and/or other countries.

Android, Chrome, Chromium, Dalvik, Firebase, Google, Google Chrome, Google Play, Google Maps, Hangouts, and YouTube are trademarks of Google, Inc.

Apache and the Apache feather logo are trademarks of The Apache Software Foundation.

BlackBerry is owned by Research In Motion Limited and is registered in the United States and may be pending or registered in other countries.

The Bluetooth word, mark and logos are owned by Bluetooth SIG, Inc.

Cisco, Cisco Systems, iOS are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

Citrix, XenServer are trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries.

Corel is a trademark or registered trademark of Corel Corporation and/or its subsidiaries in Canada, the United States and/or other countries.

Debian is a registered trademark of Software in the Public Interest, Inc.

FusionCompute, FusionSphere are trademarks of Huawei Technologies Co., Ltd registered in China and other countries.

Mozilla Firefox is a trademark of the Mozilla Foundation.

FreeBSD is a registered trademark of The FreeBSD Foundation.

Oracle, Java, JavaScript, and TouchDown are registered trademarks of Oracle and/or its affiliates.

OpenAPI is a trademark of The Linux Foundation.

QRadar, IBM are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide.

Intel, Core, Xeon are trademarks of Intel Corporation in the U.S. and/or other countries.

CentOS, Fedora, and Red Hat Enterprise Linux are registered trademarks of Red Hat Inc. in the United States and other countries.

Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.

Micro Focus a trademark or registered trademark of Micro Focus (IP) Limited or its subsidiaries in the United Kingdom, United States and other countries.

Node.js is a trademark of Joyent, Inc.

Novell is a registered trademark of Novell Inc. in the United States and other countries.

Parallels Desktop is registered trademark of Parallels International GmbH.

SPL, Splunk are trademarks and registered trademarks of Splunk Inc. in the United States and other countries.

Symbian trademark is owned by the Symbian Foundation Ltd.

SUSE is a registered trademark of SUSE LLC in the United States and other countries.

UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company Limited.

VMware, VMware vSphere are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions.

Limitations and warnings

Kaspersky Security Center has a limitation that is not critical to operation of the application:

- In Windows 20H2, the **Force permission for RDP connection to device** option does not work after a successful installation of an operating system.

Kaspersky Security Center 13 Web Console has a number of limitations that are not critical to operation of the application:

- In the **Certificates** section of the Administration Server properties window, when adding a certificate, for example, a Web Server certificate, the **Close** button ("X") obscures the **Certificate type** field, and an unnecessary **Show** button is displayed.
- Reloading the Administration Server service on a secondary Administration Server causes disconnection between Kaspersky Security Center 13 Web Console and the primary Administration Server.
- Error messages of suspected Zip Slip and Zip Bomb attacks are displayed in English only.
- The properties window of a role cannot be opened from the list of roles assigned to the user.
- The list of unassigned devices is not refreshed after a device is moved to an administration group.
- Notifications cannot be sorted by date.
- The percent sign may occur in the statuses of completed tasks.
- In the properties of a virtual Administration Server user, multiple copies of the same role are displayed.
- In the properties of Microsoft updates, in the **Devices** section, searching by "Installation status" and "IP address" is unavailable.
- Deployment of Windows 10 version 2004 through Preboot Execution Environment (PXE) is not supported.
- Patches for Administration Server cannot be installed through Kaspersky Security Center 13 Web Console; only Administration Console can be used for installation.
- If you try to create an installation package with a name that already exists, no warning is displayed and a database error message occurs.
- An incorrect number of unread Kaspersky announcements may be displayed.
- When the Backup of Administration Server data task is running, an error message is displayed instead of a message saying that the Administration Server is currently busy.

Index

A

Active Directory.....	335
Administration groups	44, 384, 1404
Anti-virus protection	584

C

Cisco Network Admission Control	234
---------------------------------------	-----

E

exec	335
------------	-----

I

Installation package	344, 403, 1409
IP-диапазон	
изменение	310, 313
создание	312

K

Key358	
klbackup.....	262
klsrvswch	238
kpd-файл.....	350

L

License.....	319
key file	323

N

Network Agent	234, 242
---------------------	----------

P

Packages	344
Policy	51, 1412

R

riprep	353
--------------	-----

S

SHV	234
SQL-сервер	237

T

Tasks	
group tasks	374, 1408
local	376

U

Update Agents	350, 403, 427, 589, 593, 1407
Updating the app	262, 432

A

Автономный пакет установки	182, 332
Агент SNMP	234
Агент администрирования	
установка	178, 593

Б

База данных	236, 237
-------------------	----------

В

Виртуальный Сервер администрирования	46
--	----

Выборки событий	
настройка.....	519
просмотр журнала	519
создание	519
Выборочная установка	232

Г

Группа лицензионных программ.....	499
Групповые задачи	
наследование.....	377
фильтр	381
Группы	
структура	634

Д

Добавление	
клиентское устройство	644
Сервер администрирования	384, 605

З

Задача	51, 334
добавления ключа	361
управление клиентскими устройствами	646
Задачи	
выполнение	380
импорт	378
просмотр результатов	380
рассылка отчетов	510
резервное копирование	618
смена Сервера администрирования.....	645
экспорт.....	378

И

Импорт	
--------	--

задачи	378
политики	393
Инсталляционный пакет	
распространение	349, 350

К

Кластеры	645
Клиентское устройство	48
подключение к Серверу	638
сообщение пользователю	647
Ключ	
отчет	362
распространение	362
удаление	361
установка	361
Консоль администрирования	234
Контекстное меню	902

М

Массивы	645
Мастер конвертации политик и задач	379, 393
Мастер удаленной установки	338
Мобильное устройство Exchange ActiveSync	749
Мобильное устройство iOS MDM	755
Мобильные пользователи	
правила переключения	292
профиль	288
Мобильные устройства	242

Н

Настройка	
kpd-файл	350

О

Обновление	
получение	413
проверка	422
просмотр.....	424
распространение	424, 425, 427
Образ.....	714
Ограничение трафика.....	611
Опрос	
IP-диапазоны.....	310
Windows-сеть	305
группы Active Directory.....	308
Опрос сети	304, 589
Отчеты	342
ключи	362
просмотр.....	509
рассылка.....	510
создание	509

П

Папка общего доступа	240
Поддержка мобильных устройств	234
Подчиненные Серверы	
добавление	384
Политика	
создание	389
Политики	
активация	390
импорт	393
копирование	392
мобильные пользователи	291
удаление.....	392
экспорт.....	392
Порты	214

Р

Роль пользователя

добавить 744