KASPERSKY lab

Kaspersky Security Center 10

Подготовительные процедуры

643.46856491.00069-05 91 01

Версия программы: 10.5.1781.0

Уважаемый пользователь!

Спасибо, что доверяете нам. Мы надеемся, что этот документ поможет вам в работе и ответит на большинство возникающих вопросов.

Дата редакции документа: 11.05.2018

Обозначение документа:

https://www.kaspersky.ru
https://help.kaspersky.com/ru
https://support.kaspersky.ru

Содержание

Об этом документе

Настоящий документ представляет собой подготовительные процедуры программного изделия "Kaspersky Security Center 10" (далее также "Kaspersky Security Center", "программа").

Подготовительные процедуры изложены в разделах "Подготовка к установке программы", "Установка программы", "Подготовка программы к работе" и "Процедура приемки" и содержат процедуры безопасной установки и первоначальной настройки программы, которые необходимы для получения безопасной (сертифицированной) конфигурации. В разделе "Требования" приведены минимально необходимые системные требования для безопасной установки программы.

В документе также содержатся разделы с дополнительной информацией о программе.

Документ адресован техническим специалистам, в обязанности которых входит установка и администрирование Kaspersky Security Center, а также поддержка организаций, использующих Kaspersky Security Center.

Источники информации о программе

Указанные источники информации о программе (в частности, электронная справка) созданы для удобства пользователя и не являются полноценным эквивалентом этого документа.

Этот раздел содержит описание источников информации о программе.

Вы можете выбрать наиболее удобный источник информации в зависимости от важности и срочности вопроса.

В этом разделе

Источники для самостоятельного поиска информации

Вы можете использовать следующие источники для самостоятельного поиска информации о Kaspersky Security Center:

- страница Kaspersky Security Center на веб-сайте "Лаборатории Касперского";
- страница Kaspersky Security Center на веб-сайте Службы технической поддержки (База знаний);
- электронная справка;
- документация.

Если вы не нашли решения возникшей проблемы самостоятельно, обратитесь в Службу технической поддержки "Лаборатории Касперского".

Для использования источников информации на веб-сайтах требуется подключение к интернету.

Страница Kaspersky Security Center на веб-сайте "Лаборатории Касперского"

На странице Kaspersky Security Center (http://www.kaspersky.ru/security-center) вы можете получить общую информацию о программе, ее возможностях и особенностях работы.

Страница Kaspersky Security Center содержит ссылку на интернет-магазин. В нем вы можете приобрести программу или продлить право пользования программой.

Страница Kaspersky Security Center в Базе знаний

База знаний – это раздел веб-сайта Службы технической поддержки.

На странице Kaspersky Security Center в Базе знаний (https://support.kaspersky.ru/ksc10) вы найдете статьи, которые содержат полезную информацию, рекомендации и ответы на часто задаваемые вопросы о приобретении, установке и использовании программы.

Статьи Базы знаний могут отвечать на вопросы, которые относятся не только к Kaspersky Security Center, но и к другим программам "Лаборатории Касперского". Статьи Базы знаний также могут содержать новости Службы технической поддержки.

Электронная справка

Программа содержит файлы полной и контекстной справки.

В полной справке вы можете найти информацию о настройке и использовании Kaspersky Security Center.

В контекстной справке вы можете найти информацию об окнах Kaspersky Security Center: описание параметров Kaspersky Security Center и ссылки на описания задач, в которых используются эти параметры.

Справка может быть включена в состав программы либо располагаться онлайн на веб-ресурсе "Лаборатории Касперского". Если справка расположена онлайн, то при ее вызове будет открыто окно браузера. Для отображения онлайн-справки требуется соединение с интернетом.

Документация

В состав документации к программе входят файлы Руководства по эксплуатации и Подготовительные процедуры.

В руководстве по эксплуатации вы можете найти информацию о настройке и использовании Kaspersky Security Center.

В документе "Подготовительные процедуры" вы можете найти информацию для выполнения следующих задач:

- планирование установки программы (учитывая принципы работы программы, системные требования, типовые схемы развертывания, особенности совместимости с другими программами);
- подготовка к установке, установка и активация Kaspersky Security Center;
- настройка программы после установки.

Обсуждение программ "Лаборатории Касперского" на форуме

Если ваш вопрос не требует срочного ответа, вы можете обсудить его со специалистами "Лаборатории Касперского" и с другими пользователями на нашем форуме (https://forum.kaspersky.com).

На форуме вы можете просматривать опубликованные темы, добавлять свои комментарии, создавать новые темы для обсуждения.

Требования

Этот раздел содержит аппаратные и программные требования для установки и работы программы, а также указания по эксплуатации и требования к среде.

В этом разделе

Аппаратные и программные требования

Сервер администрирования

Аппаратные требования:

- Процессор с частотой 1 ГГц или выше. При работе с 64-разрядной операционной системой минимальная частота процессора – 1.4 ГГц.
- Оперативная память: 4 ГБ.
- Объем свободного места на диске: 10 ГБ. При использовании функциональности Системное администрирование объем свободного места на диске должен быть не менее 100 ГБ.

Программные требования:

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

Операционная система:

- Microsoft Windows 10 Home 32-разрядная / 64-разрядная;
- Microsoft Windows 10 Pro 32-разрядная / 64-разрядная;
- Microsoft Windows 10 Enterprise 32-разрядная / 64-разрядная;
- Microsoft Windows 10 Education 32-разрядная / 64-разрядная;
- Microsoft Windows 8.1 Pro 32-разрядная / 64-разрядная;
- Microsoft Windows 8.1 Enterprise 32-разрядная / 64-разрядная;
- Microsoft Windows 8 Pro 32-разрядная / 64-разрядная;
- Microsoft Windows 8 Enterprise 32-разрядная/64-разрядная;
- Microsoft Windows 7 Professional SP1 32-разрядная / 64-разрядная;
- Microsoft Windows 7 Enterprise SP1 32-разрядная / 64-разрядная;
- Microsoft Windows 7 Ultimate SP1 32-разрядная / 64-разрядная;
- Microsoft Windows 7 Professional 32-разрядная / 64-разрядная;
- Microsoft Windows 7 Enterprise 32-разрядная / 64-разрядная;
- Microsoft Windows 7 Ultimate 32-разрядная / 64-разрядная;
- Microsoft Small Business Server 2008 Standard 64-разрядная;
- Microsoft Small Business Server 2008 Premium 64-разрядная;
- Microsoft Small Business Server 2011 Essentials 64-разрядная;
- Microsoft Small Business Server 2011 Premium Add-on 64-разрядная;
- Microsoft Small Business Server 2011 Standard 64-разрядная;
- Microsoft Windows Server® 2008 Datacenter SP1 32-разрядная / 64-разрядная;
- Microsoft Windows Server 2008 Enterprise SP1 32-разрядная / 64-разрядная;

- Microsoft Windows Server 2008 Foundation SP2 32-разрядная / 64-разрядная;
- Microsoft Windows Server 2008 SP1 Server Core 32-разрядная / 64-разрядная;
- Microsoft Windows Server 2008 Standard SP1 32-разрядная / 64-разрядная;
- Microsoft Windows Server 2008 Standard 32-разрядная / 64-разрядная;
- Microsoft Windows Server 2008 Enterprise 32-разрядная / 64-разрядная;
- Microsoft Windows Server 2008 Datacenter 32-разрядная / 64-разрядная;
- Microsoft Windows Server 2008 R2 Server Core 64-разрядная;
- Microsoft Windows Server 2008 R2 Datacenter 64-разрядная;
- Microsoft Windows Server 2008 R2 Datacenter SP1 64-разрядная;
- Microsoft Windows Server 2008 R2 Enterprise 64-разрядная;
- Microsoft Windows Server 2008 R2 Enterprise SP1 64-разрядная;
- Microsoft Windows Server 2008 R2 Foundation 64-разрядная;
- Microsoft Windows Server 2008 R2 Foundation SP1 64-разрядная;
- Microsoft Windows Server 2008 R2 SP1 Core Mode 64-разрядная;
- Microsoft Windows Server 2008 R2 Standard 64-разрядная;
- Microsoft Windows Server 2008 R2 Standard SP1 64-разрядная;
- Microsoft Windows Server 2012 Server Core 64-разрядная;
- Microsoft Windows Server 2012 Datacenter 64-разрядная;
- Microsoft Windows Server 2012 Essentials 64-разрядная;
- Microsoft Windows Server 2012 Foundation 64-разрядная;
- Microsoft Windows Server 2012 Standard 64-разрядная;
- Microsoft Windows Server 2012 R2 Server Core 64-разрядная;

- Microsoft Windows Server 2012 R2 Datacenter 64-разрядная;
- Microsoft Windows Server 2012 R2 Essentials 64-разрядная;
- Microsoft Windows Server 2012 R2 Foundation 64-разрядная;
- Microsoft Windows Server 2012 R2 Standard 64-разрядная
- Microsoft Windows Server 2016 Datacenter Edition 64-разрядная;
- Microsoft Windows Server 2016 Standard Edition 64-разрядная;
- Microsoft Windows Server 2016 Server Core 64-разрядная.

Сервер баз данных (может быть установлен на другом устройстве):

- Microsoft SQL Server® 2008 Express 32-разрядная;
- Microsoft SQL 2008 R2 Express 64-разрядная;
- Microsoft SQL 2012 Express 64-разрядная;
- Microsoft SQL 2014 Express 64-разрядная;
- Microsoft SQL Server 2008 (все редакции) 32-разрядная / 64-разрядная;
- Microsoft SQL Server 2008 R2 (все редакции) 64-разрядная;
- Microsoft SQL Server 2008 R2 Service Pack 2 64-разрядная;
- Microsoft SQL Server 2012 (все редакции) 64-разрядная;
- Microsoft SQL Server 2014 (все редакции) 64-разрядная;
- Microsoft SQL Server 2016 (все редакции) 64-разрядная;
- Microsoft Azure SQL Database;
- MySQL 5.5 32-разрядная / 64-разрядная (не поддерживаются версии MySQL 5.5.1, 5.5.2, 5.5.3, 5.5.4, 5.5.5);
- MySQL Enterprise 5.5 32-разрядная / 64-разрядная;

- MySQL 5.6 32-разрядная / 64-разрядная;
- MySQL Enterprise 5.6 32-разрядная / 64-разрядная;
- MySQL 5.7 32-разрядная / 64-разрядная;
- MySQL Enterprise 5.7 32-разрядная / 64-разрядная.

Сервер мобильных устройств iOS Mobile Device Management (iOS MDM)

Аппаратные требования:

- Процессор: с частотой 1 ГГц или выше. При работе с 64-разрядной операционной системой минимальная частота процессора – 1.4 ГГц.
- Оперативная память: 2 ГБ.
- Объем свободного места на диске: 2 ГБ.

Программные требования: операционная система Microsoft Windows (версия поддерживаемой операционной системы определяется требованиями Сервера администрирования).

Сервер мобильных устройств Exchange ActiveSync

Программные и аппаратные требования для Сервера мобильных устройств Exchange ActiveSync полностью включены в требования для сервера Microsoft Exchange Server.

Поддерживается работа с Microsoft Exchange Server 2007, Microsoft Exchange Server 2010 и Microsoft Exchange Server 2013.

Консоль администрирования

Аппаратные требования:

- Процессор: с частотой не менее 1 ГГц. При работе с 64-разрядной операционной системой минимальная частота процессора – 1.4 ГГц.
- Оперативная память: 512 МБ.
- Объем свободного места на диске: 1 ГБ.

Программные требования:

- Операционная система Microsoft Windows (версия поддерживаемой операционной системы определяется требованиями Сервера администрирования);
- Microsoft Management Console 2.0;
- Microsoft Windows Installer 4.5;
- Microsoft Internet Explorer 9.0 при работе с Microsoft Windows Server 2008, Microsoft Windows Server 2008 R2, Microsoft Windows Server 2012, Microsoft Windows Server 2012 R2, Microsoft Windows Vista, Microsoft Windows 7. При работе с Microsoft Windows Server 2008 SP2 требуется наличие обновления платформы.
- Microsoft Internet Explorer 10.0 при работе с Microsoft Windows Server 2008 R2 SP1, Microsoft Windows Server 2012, Microsoft Windows Server 2012 R2, Windows 7 SP1, Microsoft Windows 8, Microsoft Windows 8.1, Microsoft Windows 10.
- Microsoft Internet Explorer 11.0 при работе с Microsoft Windows Server 2008 R2, Microsoft Windows Server 2008 R2 SP1, Microsoft Windows Server 2016, Windows 7 SP1,Microsoft Windows 8.1, Microsoft Windows 10.
- Microsoft Edge при работе с Microsoft Windows 10.

Агент администрирования

Аппаратные требования:

- Процессор: с частотой 1 ГГц или выше. При работе с 64-разрядной операционной системой минимальная частота процессора – 1.4 ГГц.
- Оперативная память: 1 ГБ.
- Объем свободного места на диске: 4 ГБ.

Программные требования:

- Windows Embedded POSReady 7 32-разрядная / 64-разрядная;
- Windows Embedded Standard 7 SP1 32-разрядная / 64-разрядная;

- Windows Embedded 8 Standard 32-разрядная / 64-разрядная;
- Windows Embedded 8 Industry Pro 32-разрядная / 64-разрядная;
- Windows Embedded 8 Industry Enterprise 32-разрядная / 64-разрядная;
- Windows Embedded 8.1 Industry Pro 32-разрядная / 64-разрядная;
- Windows Embedded 8.1 Industry Enterprise 32-разрядная / 64-разрядная;
- Windows Embedded 8.1 Industry Update 32-разрядная / 64-разрядная;
- Windows 10 Home 32-разрядная / 64-разрядная;
- Windows 10 Pro 32-разрядная / 64-разрядная;
- Windows 10 Enterprise 32-разрядная / 64-разрядная;
- Windows 10 Education 32-разрядная / 64-разрядная;
- Windows 8.1 Pro 32-разрядная / 64-разрядная;
- Windows 8.1 Enterprise 32-разрядная / 64-разрядная;
- Windows 8 Pro 32-разрядная / 64-разрядная;
- Windows 8 Enterprise 32-разрядная / 64-разрядная;
- Windows 7 Professional SP1 32-разрядная / 64-разрядная;
- Windows 7 Enterprise SP1 32-разрядная / 64-разрядная;
- Windows 7 Ultimate SP1 32-разрядная / 64-разрядная;
- Windows 7 Professional 32-разрядная / 64-разрядная;
- Windows 7 Enterprise 32-разрядная / 64-разрядная;
- Windows 7 Ultimate 32-разрядная / 64-разрядная;
- Windows 7 Home Basic 32-разрядная / 64-разрядная;
- Windows 7 Premium 32-разрядная / 64-разрядная;

- Essential Business Server 2008 64-разрядная;
- Small Business Server 2008 Standard 64-разрядная;
- Small Business Server 2008 Premium 64-разрядная;
- Small Business Server 2011 Essentials 64-разрядная;
- Small Business Server 2011 Premium Add-on 64-разрядная;
- Small Business Server 2011 Standard 64-разрядная;
- Windows Home Server 2011 64-разрядная;
- Windows MultiPoint™ Server 2011 64-разрядная;
- Windows Server 2008 Datacenter SP1 32-разрядная / 64-разрядная;
- Windows Server 2008 Enterprise SP1 32-разрядная / 64-разрядная;
- Windows Server 2008 Foundation SP2 32-разрядная / 64-разрядная;
- Windows Server 2008 SP1 Server Core 32-разрядная / 64-разрядная;
- Windows Server 2008 Standard SP1 32-разрядная / 64-разрядная;
- Windows Server 2008 32-разрядная / 64-разрядная;
- Windows Server 2008 R2 Server Core 64-разрядная;
- Windows Server 2008 R2 Datacenter 64-разрядная;
- Windows Server 2008 R2 Datacenter SP1 64-разрядная;
- Windows Server 2008 R2 Enterprise 64-разрядная;
- Windows Server 2008 R2 Enterprise SP1 64-разрядная;
- Windows Server 2008 R2 Foundation 64-разрядная;
- Windows Server 2008 R2 Foundation SP1 64-разрядная;
- Windows Server 2008 R2 SP1 Core Mode 64-разрядная;

- Windows Server 2008 R2 Standard 64-разрядная;
- Windows Server 2008 R2 Standard SP1 64-разрядная;
- Windows Server 2012 Server Core 64-разрядная;
- Windows Server 2012 Datacenter 64-разрядная;
- Windows Server 2012 Essentials 64-разрядная;
- Windows Server 2012 Foundation 64-разрядная;
- Windows Server 2012 Standard 64-разрядная;
- Windows Server 2012 R2 Server Core 64-разрядная;
- Windows Server 2012 R2 Datacenter 64-разрядная;
- Windows Server 2012 R2 Essentials 64-разрядная;
- Windows Server 2012 R2 Foundation 64-разрядная;
- Windows Server 2012 R2 Standard 64-разрядная;
- Windows Server 2016 Datacenter Edition;
- Windows Server 2016 Standard Edition.

Вы можете получить сведения о последней версии аппаратных и программных требований на веб-сайте Службы технической поддержки, на странице Kaspersky Security Center, в разделе Системные требования (http://support.kaspersky.ru/ksc10#requirements).

См. также

Указания по эксплуатации и требования к среде

1. Установка, конфигурирование и управление программой должны осуществляться в соответствии с эксплуатационной документацией.
2. Программа должна эксплуатироваться на компьютерах, отвечающих минимальным требованиям, приведенным в разделе "Аппаратные и программные требования".
3. Перед установкой и началом эксплуатации программы необходимо установить все доступные обновления используемых версий ПО среды функционирования.
4. Должен быть обеспечен доступ программы ко всем объектам информационной системы, которые необходимы программе для реализации своих функциональных возможностей (к контролируемым объектам информационной системы).
5. Должна быть обеспечена совместимость программы с контролируемыми ресурсами информационной системы.
6. Должна быть обеспечена возможность корректной совместной работы программы со средствами антивирусной защиты других производителей в случае их совместного использования в информационной системе.

7. Должна быть обеспечена физическая защита элементов информационной системы, на которых установлена программа.

8. Должна быть обеспечена синхронизация по времени между компонентами программы, а также между программой и средой ее функционирования.

9. Персонал, ответственный за функционирование программы, должен обеспечивать надлежащее функционирование программы, руководствуясь эксплуатационной документацией.

10. Должна быть обеспечена доверенная связь между программой и уполномоченными субъектами информационной системы (администраторами безопасности).

11. Функционирование программы должно осуществляться в среде функционирования, предоставляющей механизмы аутентификации и идентификации администраторов безопасности программы.

12. Должен быть обеспечен доверенный канал получения обновлений БД ПКВ.

13. Должна быть обеспечена защищенная область для выполнения функций безопасности программы.

14. Управление атрибутами безопасности, связанными с доступом к функциям и данным программы, должно предоставляться только уполномоченным ролям (администраторам программы и информационной системы).

15. Администратор должен установить в среде ИТ максимальное число попыток неуспешных попыток аутентификации с момента последней успешной попытки аутентификации пользователя с последующей блокировкой попыток аутентификации при превышении установленного значения.

16. Администратор должен задать метрику качества паролей, включающую требования к длине паролей, требования по запрещению использования определенных комбинаций символов, а также требования к категории используемых символов.

Основные понятия

Этот раздел содержит развернутые определения основных понятий, относящихся к программе Kaspersky Security Center.

В этом разделе

Сервер администрирования

Компоненты Kaspersky Security Center позволяют осуществлять удаленное управление программами "Лаборатории Касперского", установленными на клиентских устройствах.

Устройства, на которых установлен компонент Сервер администрирования, называются *Серверами администрирования* (далее также *Серверами*).

Сервер администрирования устанавливается на устройство в качестве службы со

следующим набором атрибутов:

- под именем "Сервер администрирования Kaspersky Security Center";
- с автоматическим типом запуска при старте операционной системы;
- с учетной записью **Локальная система** либо учетной записью пользователя в соответствии с выбором, сделанным при установке Сервера администрирования.

Сервер администрирования выполняет следующие функции:

- хранение структуры групп администрирования;
- хранение информации о конфигурации клиентских устройств;
- организация хранилищ дистрибутивов программ;
- удаленная установка программ на клиентские устройства и удаление программ;
- обновление баз и модулей программ "Лаборатории Касперского";
- управление политиками и задачами на клиентских устройствах;
- хранение информации о событиях, произошедших на клиентских устройствах;
- формирование отчетов о работе программ "Лаборатории Касперского";
- распространение ключей на клиентские устройства, хранение информации о ключах;
- отправка уведомлений о ходе выполнения задач (например, об обнаружении вирусов на клиентском устройстве).

Вы можете подключиться к Серверу администрирования с помощью Консоли администрирования (см. раздел "Сервер администрирования и Консоль администрирования" на стр. 65).

Иерархия Серверов администрирования

Серверы администрирования могут образовывать иерархию вида "главный сервер – подчиненный сервер". Каждый Сервер администрирования может иметь несколько

подчиненных Серверов администрирования (далее также *подчиненных Серверов*) на разных уровнях иерархии. Уровень вложенности подчиненных Серверов не ограничен. При этом в состав групп администрирования главного Сервера будут входить клиентские устройства всех подчиненных Серверов. Таким образом, независимые участки компьютерной сети могут управляться различными Серверами администрирования, которые, в свою очередь, управляются главным Сервером.

Частным случаем подчиненных Серверов администрирования являются *виртуальные Серверы администрирования* (см. раздел "Виртуальный Сервер администрирования" на стр. 32).

Иерархию Серверов администрирования можно использовать для следующих целей:

- Ограничение нагрузки на Сервер администрирования (по сравнению с одним установленным в сети Сервером).
- Сокращение трафика внутри сети и упрощение работы с удаленными офисами. Нет необходимости устанавливать соединение между главным Сервером и всеми устройствами сети, которые могут находиться, например, в других регионах. Достаточно установить в каждом участке сети подчиненный Сервер администрирования, распределить устройства в группах администрирования подчиненных Серверов и обеспечить подчиненным Серверам соединение с главным Сервером по быстрым каналам связи.
- Разделение ответственности между администраторами антивирусной безопасности. При этом сохраняются все возможности централизованного управления и мониторинга состояния антивирусной безопасности сети организации.
- Использование Kaspersky Security Center сервис-провайдерами. Сервис-провайдеру достаточно установить Kaspersky Security Center. Для управления большим числом клиентских устройств различных организаций сервис-провайдер может включать в иерархию Серверов администрирования виртуальные Серверы администрирования.

Каждое устройство, включенное в иерархию групп администрирования, может быть подключено только к одному Серверу администрирования. Вам нужно самостоятельно проверять подключение устройств к Серверам администрирования. Для этого можно использовать функцию поиска устройств по сетевым атрибутам в группах администрирования различных Серверов.

См. также

Иерархия Серверов администрирования: главный и подчиненный Серверы администрирования 69

Виртуальный Сервер администрирования

Виртуальный Сервер администрирования (далее также *виртуальный Сервер*) – компонент программы Kaspersky Security Center, предназначенный для управления сетью организации-клиента.

Виртуальный Сервер администрирования является частным случаем подчиненного Сервера администрирования и, по сравнению с физическим Сервером администрирования, имеет следующие основные ограничения:

- Виртуальный Сервер администрирования может функционировать только в составе главного Сервера администрирования.
- Виртуальный Сервер администрирования использует для работы базу данных главного Сервера администрирования: задачи резервного копирования и восстановления данных, проверки и получения обновлений не поддерживаются на виртуальном Сервере. Эти задачи решаются в рамках главного Сервера администрирования.
- Для виртуального Сервера не поддерживается создание подчиненных Серверов администрирования (в том числе и виртуальных).

Кроме того, виртуальный Сервер администрирования имеет следующие ограничения:

- В окне свойств виртуального Сервера ограничен набор разделов.
- Для удаленной установки программ "Лаборатории Касперского" на клиентские устройства, работающие под управлением виртуального Сервера, необходимо, чтобы на одном из клиентских устройств был установлен Агент администрирования для связи с виртуальным Сервером. При первом подключении к виртуальному Серверу это устройство автоматически назначается агентом обновлений и выполняет роль шлюза соединений клиентских устройств с виртуальным Сервером.
- Виртуальный Сервер может опрашивать сеть только через агенты обновлений.
- Чтобы перезапустить виртуальный Сервер, работоспособность которого была нарушена, Kaspersky Security Center перезапускает главный Сервер администрирования и все виртуальные Серверы.

Администратор виртуального Сервера обладает всеми правами в рамках этого виртуального Сервера.

Сервер мобильных устройств

Сервер мобильных устройств – это компонент Kaspersky Security Center, который предоставляет доступ к мобильным устройствам и позволяет управлять ими через Консоль администрирования. Сервер мобильных устройств получает информацию о мобильных устройствах и хранит их профили.

Существуют два вида Серверов мобильных устройств:

- Сервер мобильных устройств Exchange ActiveSync. Устанавливается на устройство, на котором установлен сервер Microsoft Exchange, и позволяет получать данные с сервера Microsoft Exchange и передавать их на Сервер администрирования. Этот Сервер мобильных устройств используется для управления мобильными устройствами, поддерживающими протокол Exchange ActiveSync.

- Сервер iOS MDM. Этот Сервер мобильных устройств используется для управления мобильными устройствами, поддерживающими сервис Apple® Push Notifications (APNs).

Серверы мобильных устройств Kaspersky Security Center позволяют управлять следующими объектами:

- Отдельным мобильным устройством.
- Несколькими мобильными устройствами.
- Несколькими мобильными устройствами, подключенными к кластеру серверов, одновременно. При подключении к кластеру серверов Сервер мобильных устройств, установленный на этом кластере, отображается в Консоли администрирования как один сервер.

Агент администрирования. Группа администрирования

Взаимодействие между Сервером администрирования и устройствами осуществляет компонент программы Kaspersky Security Center *Агент администрирования*. Агент администрирования требуется установить на все устройства, где управление работой программ "Лаборатории Касперского" выполняется с помощью Kaspersky Security Center.

Агент администрирования устанавливается на устройстве в качестве службы со следующим набором атрибутов:

- под именем "Агент администрирования Kaspersky Security Center";
- с автоматическим типом запуска, при старте операционной системы;
- с учетной записью **Локальная система**.

Устройство, сервер или рабочая станция, на которых установлен Агент администрирования и управляемые программы "Лаборатории Касперского", называется *клиентом Сервера администрирования* (далее также *клиентским устройством* или *устройством*).

Множество устройств сети организации может быть разбито на группы, образующие иерархическую структуру. Такие группы называются *группами администрирования*. Иерархия групп администрирования отображается в дереве консоли в узле Сервера администрирования.

Группа администрирования (далее также *группа*) – это набор клиентских устройств, объединенных по какому-либо признаку, с целью управления устройствами группы как единым целым. Для всех клиентских устройств в группе устанавливаются:

- единые параметры работы программ – с помощью *групповых политик*;
- единый режим работы программ – путем создания *групповых задач* с заданным набором параметров (например, создание и установка единого *инсталляционного пакета*, обновление баз и модулей программ, проверка устройства по требованию и постоянная защита).

Клиентское устройство может входить в состав только одной группы администрирования.

Вы можете создавать иерархию Серверов и групп любой глубины вложенности. На одном уровне иерархии могут располагаться подчиненные и виртуальные Серверы администрирования, группы и клиентские устройства.

Рабочее место администратора

Устройства, на которых установлен компонент *Консоль администрирования*, называются *рабочими местами администраторов*. С этих устройств администраторы могут осуществлять удаленное централизованное управление программами "Лаборатории Касперского", установленными на клиентских устройствах.

После установки Консоли администрирования на устройстве в меню **Пуск** → **Программы** → **Kaspersky Security Center** появляется значок для ее запуска.

Количество рабочих мест администратора не ограничивается. С каждого рабочего места администратора можно управлять группами администрирования сразу нескольких Серверов администрирования в сети. Рабочее место администратора можно подключить к Серверу администрирования (как к физическому, так и к виртуальному) любого уровня иерархии.

Рабочее место администратора можно включить в состав группы администрирования в качестве клиентского устройства.

В пределах групп администрирования любого Сервера одно и то же устройство может быть одновременно и клиентом Сервера администрирования, и Сервером администрирования, и рабочим местом администратора.

Плагин управления программой

Управление программами «Лаборатории Касперского» через Консоль администрирования выполняется при помощи специального компонента – *плагина управления программой*. В состав каждой программы «Лаборатории Касперского», которой можно управлять при помощи Kaspersky Security Center, входит плагин управления.

С помощью плагина управления программой в Консоли администрирования можно выполнять следующие действия:

- создавать и редактировать политики и параметры программы, а также параметры задач этой программы;
- получать информацию о задачах программы, событиях в ее работе, а также о статистике работы программы, получаемой с клиентских устройств.

Политики, параметры программы и задачи

Именованное действие, выполняемое программой "Лаборатории Касперского", называется *задачей*. В соответствии с выполняемыми функциями задачи разделяют по *типам*.

Каждой задаче соответствует набор параметров работы программы при ее выполнении. Набор параметров работы программы, общий для всех типов ее задач, составляет параметры программы. Параметры работы программы, специфичные для каждого типа задач, образуют параметры задачи.

Подробное описание типов задач для каждой программы "Лаборатории Касперского" приводится в Руководствах к ним.

Параметры программы, которые определяются для отдельного клиентского устройства через локальный интерфейс или удаленно через Консоль администрирования, называются *локальными параметрами программы*.

Централизованная настройка параметров работы программ, установленных на клиентских устройствах, осуществляется через определение политик.

Политика – это набор параметров работы программы, определенный для группы администрирования. Политика определяет не все параметры программы.

Для одной программы может быть определено несколько политик с различными значениями параметров, но активная политика для программы может быть только одна.

Для разных групп параметры работы программы могут быть различными. В каждой группе может быть создана собственная политика для программы.

Параметры программы определяются параметрами политик и задач.

Вложенные группы и подчиненные Серверы администрирования наследуют задачи групп более высоких уровней иерархии. Задача, определенная для группы, выполняется не только на клиентских устройствах, включенных в состав этой группы, но и на клиентских устройствах, включенных в состав вложенных в нее групп и подчиненных Серверов, на всех последующих уровнях иерархии.

Каждый параметр, представленный в политике, имеет атрибут "замок":  . "Замок" показывает, наложен ли запрет на изменение параметра в политиках вложенного уровня иерархии (для вложенных групп и подчиненных Серверов администрирования), в параметрах задач и локальных параметрах программы. Если в политике для параметра установлен "замок", переопределить значение будет невозможно (см. раздел "Взаимосвязь политики и локальных параметров программы" на стр. 39).

В окне свойств унаследованной политики есть флажок **Наследовать параметры из политики верхнего уровня**, расположенный в блоке **Наследование параметров** раздела **Общие**. Если флажок снят, то действие "замка" для этой политики отменяется. Снять флажок возможно только после того, как вы создадите новую политику. Новая политика

наследует настройки из политики верхнего уровня.Предусмотрена возможность активировать политику, не являющуюся активной, при наступлении события, что позволяет, например, устанавливать более жесткие параметры антивирусной защиты в периоды вирусных эпидемий.

Также можно сформировать политику для автономных пользователей.

Создание и настройка задач для объектов, находящихся под управлением одного Сервера администрирования, осуществляется централизованно. Могут быть определены задачи следующих типов:

- *групповая задача* – задача, определяющая параметры работы программ, установленных на устройствах, включенных в группу администрирования;
- *локальная задача* – задача для отдельного устройства;
- *задача для набора устройств* – задача для произвольного набора устройств, как входящих, так и не входящих в группы администрирования;
- *задача Сервера администрирования* – задача, определяемая непосредственно для Сервера администрирования.

Для группы может быть определена групповая задача, даже если программа "Лаборатории Касперского" установлена не на все клиентские устройства группы. В этом случае групповая задача выполняется только для тех устройств, на которых указанная программа установлена.

Задачи, созданные для клиентского устройства локально, выполняются только для этого устройства. При синхронизации клиентского устройства с Сервером администрирования локальные задачи добавляются в перечень сформированных задач для клиентского устройства.

Поскольку параметры работы программы определяются политикой, в параметрах задачи могут быть переопределены те из них, на которые в политике не наложен запрет на изменение, а также параметры, которые могут быть установлены только для конкретного экземпляра задачи. Например, для задачи проверки диска это имя диска и маски проверяемых файлов.

Задача может запускаться автоматически (по расписанию) или вручную. Результаты выполнения задач сохраняются на Сервере администрирования и локально. Администратор может получать уведомления о том, как выполнена та или иная задача, а также просматривать подробные отчеты.

Информация о политиках, параметрах программы, параметрах задач для наборов устройств и о групповых задачах сохраняется на Сервере и распространяется на клиентские устройства в ходе синхронизации. При этом на Сервере администрирования сохраняются сведения о локальных изменениях, разрешенных политикой и проведенных на клиентских устройствах. Кроме того, обновляется список программ, функционирующих на клиентском устройстве, их статус и перечень сформированных задач.

Взаимосвязь политики и локальных параметров программы

При помощи политик могут быть установлены одинаковые значения параметров работы программы для всех устройств, входящих в состав группы.

Переопределить значения параметров, заданные политикой, для отдельных устройств в группе можно при помощи локальных параметров программы. При этом можно установить значения только тех параметров, изменение которых не запрещено политикой (параметр не закрыт "замком").

Значение параметра, которое использует программа на клиентском устройстве (см. рис. ниже), определяется наличием «замка» у параметра в политике:

- Если на изменение параметра наложен запрет, на всех клиентских устройствах используется одно и то же значение – заданное политикой.

- Если запрет не наложен, то на каждом клиентском устройстве программа использует локальное значение параметра, а не то, которое указано в политике. При этом значение параметра может изменяться через локальные параметры программы.

Рисунок 1. Политика и локальные параметры программы

Таким образом, при выполнении задачи на клиентском устройстве программа использует параметры, заданные двумя разными способами:

- параметрами задачи и локальными параметрами программы, если в политике не был установлен запрет на изменение параметра;
- политикой группы, если в политике был установлен запрет на изменение параметра.

Локальные параметры программы изменяются после первого применения политики в соответствии с параметрами политики.

Агент обновлений

Агент обновлений – это устройство с установленным Агентом администрирования, который используется для распространения обновлений, удаленной установки программ, получения информации об устройствах в сети. Агент обновлений может выполнять следующие функции:

- Распространять обновления и инсталляционные пакеты, полученные от Сервера администрирования, на клиентские устройства группы (в том числе и с помощью широковещательной рассылки по протоколу UDP). Обновления могут быть получены как с Сервера администрирования, так и с серверов обновлений "Лаборатории Касперского". В последнем случае для агента обновлений должна быть создана задача обновления.

  Агенты обновлений ускоряют распространение обновлений и позволяют высвободить ресурсы Сервера администрирования.

- Распространять политики и групповые задачи с помощью широковещательной рассылки по протоколу UDP.

- Выполнять роль шлюза соединений с Сервером администрирования для устройств группы администрирования (см. раздел "Использование агента обновлений в качестве шлюза соединений" на стр. 207).

  Если нет возможности создать прямое соединение между управляемыми устройствами группы и Сервером администрирования, агент обновлений можно назначить шлюзом соединений этой группы с Сервером администрирования. В этом случае управляемые устройства подключаются к шлюзу соединений, который, в свою очередь, подключается к Серверу администрирования.

  Наличие агента обновлений, работающего в режиме шлюза соединений, не исключает прямого соединения управляемых устройств с Сервером администрирования. Если шлюз соединений недоступен, а прямое соединение с

Сервером администрирования технически возможно, управляемые устройства напрямую подключаются к Серверу.

- Опрашивать сеть с целью обнаружения новых устройств и обновления информации об обнаруженных устройствах. Агент обновлений может выполнять те же виды опроса сети, что и Сервер администрирования.

- Выполнять удаленную установку как сторонних программ, так и программ "Лаборатории Касперского" средствами Microsoft Windows, в том числе на клиентские устройства без установленного Агента администрирования.

  Эта функция позволяет удаленно передавать инсталляционные пакеты Агента администрирования на клиентские устройства, расположенные в сетях, к которым у Сервера администрирования нет прямого доступа.

Передача файлов агенту обновлений Сервером администрирования осуществляется по протоколу HTTP или, если настроено использование SSL-соединения, по протоколу HTTPS. Использование протокола HTTP или HTTPS обеспечивает более высокую производительность по сравнению с использованием протокола SOAP за счет сокращения трафика.

Устройства с установленным Агентом администрирования могут быть назначены агентами обновлений вручную администратором или автоматически Сервером администрирования. Полный список агентов обновлений для указанных групп администрирования отображается в отчете по списку агентов обновлений.

Областью действия агента обновлений является группа администрирования, для которой он назначен администратором, а также ее подгруппы всех уровней вложенности. Если в иерархии групп администрирования назначено несколько агентов обновлений, Агент администрирования управляемого устройства подключается к наиболее близкому по иерархии агенту обновлений.

Областью действия агентов обновлений также может являться сетевое местоположение. Сетевое местоположение используется для формирования вручную набора устройств, на которые агент обновлений будет распространять обновления. Определение сетевого местоположения доступно только для устройств под управлением операционной системы Windows.

Если агенты обновлений назначаются автоматически Сервером администрирования, то Сервер назначает агенты обновлений по широковещательным доменам, а не по группам администрирования. Это происходит после того, как становятся известны широковещательные домены. Агент администрирования обменивается с другими Агентами администрирования своей подсети сообщениями и отправляет Серверу администрирования информацию о себе и краткую информацию о других Агентах администрирования. На основании этой информации Сервер администрирования может сгруппировать Агенты администрирования по широковещательным доменам. Широковещательные домены становятся известны Серверу администрирования после того, как опрошено более 70% Агентов администрирования в группах администрирования. Сервер администрирования опрашивает широковещательные домены каждые два часа.После того как агенты обновлений назначены по широковещательным доменам, их нельзя назначить снова по группам администрирования.

Если агенты обновлений назначаются администратором вручную, возможно назначение только по группам администрирования.

Агенты администрирования с активным профилем соединения не участвуют в определении широковещательного домена.

Kaspersky Security Center присваивает каждому Агенту администрирования уникальный адрес многоадресной IP-рассылки, который не пересекается с другими адресами. Это позволяет избежать превышения нагрузки на сеть, которое возникло бы из-за пересечения адресов. Функция присвоения уникальных адресов работает в версиях Kaspersky Security Center 10 Service Pack 3 и выше. Адреса многоадресной IP-рассылки, уже присвоенные в прошлых версиях программы, изменены не будут.

Если на одном участке сети или в группе администрирования назначаются два агента обновлений или более, один из них становится активным агентом обновлений, остальные назначаются резервными. Активный агент обновлений скачивает обновления и инсталляционные пакеты непосредственно с Сервера администрирования, резервные агенты обновлений обращаются за обновлениями только к активному агенту обновлений. В этом случае файлы загружаются только один раз с Сервера администрирования и далее распределяются между агентами обновлений. Если активный агент обновлений по

каким-либо причинам становится недоступным, один из резервных агентов обновлений назначается активным. Сервер администрирования назначает агента обновлений резервным автоматически.

> Статус агента обновлений (*Активный* / *Резервный*) отображается флажком в отчете утилиты klnagchk.

Для работы агента обновлений необходимо не менее 4 ГБ свободного места на жестком диске. Если объем свободного места на диске агента обновлений меньше 2 ГБ, Kaspersky Security Center создает инцидент с уровнем важности *Предупреждение*. Инцидент будет опубликован в свойствах устройства в разделе **Инциденты**.

При работе задач удаленной установки на устройстве с агентом обновлений потребуется дополнительное свободное дисковое пространство. Свободное дисковое пространство должно быть больше размера всех устанавливаемых инсталляционных пакетов.

При работе задачи установки обновлений (патчей) и закрытия уязвимостей на устройстве с агентом обновлений потребуется дополнительное свободное дисковое пространство. Свободное дисковое пространство должно быть как минимум в два раза больше размера всех устанавливаемых патчей.

Сценарии развертывания Kaspersky Security Center

В этом разделе описан основной краткий сценарий развертывания Kaspersky Security Center и даны ссылки на другие сценарии развертывания. Основной краткий сценарий позволяет развернуть Сервер администрирования, а также установить на устройства сети Агент администрирования и программы защиты. Вы можете использовать этот сценарий и для ознакомления с программой, и для установки программы с целью дальнейшей работы.

Развертывание Kaspersky Security Center в сети организации предполагает планирование ресурсов; установку Сервера администрирования; установку Агента администрирования и программ защиты на клиентских устройствах; объединение устройств в группы администрирования.

В этом сценарии рекомендуется отвести на установку Сервера администрирования не менее часа, а на выполнение сценария целиком – не менее одного рабочего дня.

Сценарий развертывания Kaspersky Security Center состоит из следующих шагов:

1. **Выбор структуры защиты организации**

   Ознакомьтесь с компонентами Kaspersky Security Center (см. раздел "Развертывание и первоначальная настройка" на стр. 111). Выберите структуру защиты (см. раздел "Выбор структуры защиты организации" на стр. 85) и конфигурацию сети (см. раздел "Типовые конфигурации Kaspersky Security Center" на стр. 89), наиболее подходящие для вашей организации. Исходя из конфигурации сети и пропускной способности каналов связи определите, какое количество Серверов администрирования необходимо использовать и как их разместить по офисам (см. раздел "Планирование развертывания Kaspersky Security Center" на стр. 83), если вы работаете с распределенной сетью.

   Для достижения и сохранения оптимальной производительности при различных условиях работы учитывайте количество защищаемых устройств в сети, топологию сети и необходимый вам набор функций Kaspersky Security Center (подробнее см. в Руководстве по масштабированию Kaspersky Security Center https://help.kaspersky.com/KSC/SP3/ru-RU/162088.htm).

   Определите, будет ли использоваться в вашей сети иерархия Серверов администрирования (на стр. 30). Для этого нужно понять, возможно и целесообразно ли обслуживание всех клиентских устройств одним Сервером администрирования или требуется выстроить иерархию Серверов администрирования. Вам также может потребоваться выстроить иерархию Серверов администрирования, совпадающую с организационной структурой предприятия, сеть которого вы защищаете.

   Если вам требуется обеспечить защиту мобильных устройств, выполните подготовительные действия по настройке Сервера мобильных устройств Exchange ActiveSync (см. раздел "Сервер мобильных устройств Exchange ActiveSync" на стр. 102) и Сервера iOS MDM (см. раздел "Сервер iOS MDM" на стр. 107).

   Убедитесь, что устройства, выбранные вами для использования в качестве Серверов администрирования, а также для установки Консоли администрирования, соответствуют аппаратным и программным требованиям (см. стр. 18).

2. **Лицензирование Kaspersky Security Center**

   Если вы планируете использовать версию Kaspersky Security Center с поддержкой мобильных устройств и / или с поддержкой функциональности Системное администрирование, убедитесь, что у вас имеется файл ключа либо код активации для лицензирования программы.

3. **Лицензирование управляемых программ защиты**

   Во время развертывания защиты вам потребуется предоставить "Лаборатории Касперского" действующие лицензии на те программы, которыми вы планируете управлять с помощью Kaspersky Security Center (см. список доступных для управления программ защиты (см. раздел "Удаленная установка программ" на стр. 265)). Подробнее о лицензировании каждой из программ защиты вы можете прочитать в справках к этим программам.

4. **Выбор аппаратной конфигурации Сервера администрирования и СУБД**

   Спланируйте аппаратную конфигурацию для СУБД и Сервера администрирования (см. раздел "Аппаратные требования для СУБД и Сервера администрирования" на стр. 398) с учетом количества устройств в вашей сети.

5. **Выбор СУБД**

   При выборе СУБД (см. раздел "Выбор СУБД" на стр. 121) учитывайте количество управляемых устройств, которые будет обслуживать Сервер администрирования. Если в вашей сети менее 10 000 устройств и вы не планируете увеличивать их количество, вы можете выбрать бесплатную СУБД SQL Express или MySQL и установить ее на одном устройстве с Сервером администрирования. Если в вашей сети более 10 000 устройств (или вы планируете расширение сети до такого количества устройств), рекомендуется выбирать платную СУБД SQL и размещать ее на отдельном устройстве. Платная СУБД может работать с несколькими Серверами администрирования, а бесплатная СУБД – только с одним.

6. **Установка СУБД и создание базы данных**

   Установите СУБД. Запишите и сохраните параметры СУБД, поскольку они потребуются вам при установке Сервера администрирования. Эти параметры

включают имя SQL-сервера, номер порта для подключения к SQL-серверу, имя учетной записи и пароль для доступа к SQL-серверу.

По умолчанию инсталлятор Kaspersky Security Center создает базу данных для размещения информации Сервера администрирования (см. раздел "Шаг 8. Настройка параметров SQL-сервера" на стр. 152), однако вы можете отказаться от ее создания и использовать другую базу данных. В этом случае убедитесь, что база данных создана, вы знаете ее имя и имеете доступ к ней.

При необходимости обратитесь за информацией к администратору СУБД.

7. **Настройка портов**

Убедитесь, что для взаимодействия компонентов согласно выбранной вами структуре защиты открыты необходимые порты (см. раздел "Порты, используемые Kaspersky Security Center" на стр. 53).

Если требуется предоставить доступ к Серверу администрирования из интернета (см. раздел "Предоставление доступа к Серверу администрирования из интернета" на стр. 92), настройте порты и параметры подключения в зависимости от конфигурации сети.

8. **Проверка учетных записей**

Проверьте наличие у вас прав локального администратора для успешной установки Сервера администрирования Kaspersky Security Center и развертывания защиты на устройствах. Права локального администратора на клиентских устройствах нужны только для установки на эти устройства Агента администрирования. После установки Агента администрирования вы сможете с его помощью удаленно устанавливать программы на устройства, не пользуясь учетной записью с правами администратора устройства.

По умолчанию инсталлятор Kaspersky Security Center создает на устройстве, выбранном для установки Сервера администрирования, три локальные учетные записи, от имени которых будет запускаться Сервер администрирования (см. раздел "Шаг 5. Выбор учетной записи для запуска Сервера администрирования" на стр. 149) и службы Kaspersky Security Center (см. раздел "Шаг 6. Выбор учетной записи для запуска служб Kaspersky Security Center" на стр. 150):

KL-AK-*: учетная запись службы Сервера администрирования.

KlScSvc: учетная запись для прочих служб из состава Сервера администрирования.

KlPxeUser: учетная запись для развертывания операционных систем.

Вы можете отказаться от создания учетных записей для службы Сервера администрирования и прочих служб и использовать вместо них уже имеющиеся у вас учетные записи, например, доменные, если вы планируете установить Сервер администрирования на отказоустойчивый кластер (см. раздел "Создание учетных записей для служб Сервера администрирования на отказоустойчивом кластере" на стр. 120) или по какой-либо другой причине планируете использовать доменные учетные записи вместо локальных. В этом случае убедитесь, что учетные записи для запуска Сервера администрирования и служб Kaspersky Security Center созданы, являются непривилегированными и обладают необходимыми правами для доступа к СУБД (см. раздел "Учетные записи для работы ч" на стр. 132). (Если вы планируете в дальнейшем разворачивать операционные системы на устройствах средствами Kaspersky Security Center, не отказывайтесь от создания учетных записей.)

9. **Установка Сервера администрирования, Консоли администрирования и плагинов управления для программ защиты**

Установите Сервер администрирования на выбранное устройство (либо устройства, если вам необходимо использовать более одного Сервера администрирования (см. раздел "Типовая конфигурация: один офис" на стр. 89)). Вы можете выбрать стандартную или выборочную установку Сервера администрирования. Вместе с Сервером администрирования установится Консоль администрирования.

Стандартная установка (на стр. 137) рекомендуется, если вы хотите ознакомиться с программой Kaspersky Security Center, например, протестировать ее работу на небольшом участке сети вашей организации. При стандартной установке вы настраиваете только параметры базы данных и можете установить только заданный по умолчанию набор плагинов управления программами "Лаборатории Касперского". Вы также можете воспользоваться стандартной установкой, если вы уже имеете опыт работы с Kaspersky Security Center и знаете, как после стандартной установки настроить все необходимые вам параметры.

Выборочная установка (на стр. 144) позволяет настроить параметры Kaspersky Security Center, такие как путь к папке общего доступа, учетные записи и порты

подключения к Серверу администрирования, и параметры базы данных. Выборочная установка позволяет указать, какие плагины управления программами "Лаборатории Касперского" будут установлены. При необходимости вы можете запустить выборочную установку в неинтерактивном режиме (см. раздел "Установка в неинтерактивном режиме" на стр. 157).

Вместе с Сервером администрирования устанавливаются также Консоль администрирования и серверная версия Агента администрирования.

10. Первоначальная настройка

После завершения установки Сервера администрирования при первом подключении к Серверу администрирования автоматически запускается Мастер первоначальной настройки (см. раздел "Мастер первоначальной настройки Сервера администрирования" на стр. 176). Выполните первоначальную настройку Сервера администрирования в соответствии с вашими требованиями. На этапе первоначальной настройки мастер создает необходимые для развертывания защиты политики и задачи (см. раздел "Политики, параметры программы и задачи" на стр. 36) с параметрами по умолчанию. Эти параметры могут оказаться неоптимальными для нужд вашей организации. При необходимости вы можете изменить параметры политик и задач (см. раздел "Настройка защиты в сети организации-клиента" на стр. 193).

11. Обнаружение устройств в сети

Этот шаг имеется в мастере первоначальной настройки (см. раздел "Шаг 10. Опрос сети" на стр. 192). Вы можете также запустить опрос сети вручную. В результате Сервер администрирования Kaspersky Security Center получает адреса и имена всех устройств, зарегистрированных в сети. В дальнейшем вы можете с помощью Kaspersky Security Center устанавливать программы "Лаборатории Касперского" и других производителей на обнаруженные устройства. Kaspersky Security Center запускает опрос сети регулярно, поэтому, если в сети появятся новые устройства, они будут обнаружены автоматически.

12. Проверка успешности установки Сервера администрирования

После успешного выполнения предыдущих шагов Сервер администрирования установлен и готов к дальнейшей работе.

Убедитесь, что работает Консоль администрирования и что вы можете подключиться через Консоль к Серверу администрирования. Убедитесь также, что на Сервере администрирования имеется задача загрузки обновлений в хранилище Сервера администрирования (в папке **Задачи** дерева консоли) и политика для Kaspersky Endpoint Security (в папке **Политики** дерева консоли).

После проверки приступайте к следующим шагам, которые касаются развертывания защиты в сети организации.

13. Установка Агента администрирования и программ защиты на устройства в сети

Развертывание защиты (см. раздел "Настройка защиты в сети организации-клиента" на стр. 193) в сети организации подразумевает установку Агента администрирования и программ защиты (например, Kaspersky Endpoint Security) на устройства, которые были обнаружены Сервером администрирования при опросе сети организации.

Программы защиты защищают устройства от вирусов и / или других программ, представляющих угрозу. Агент администрирования обеспечивает связь устройства с Сервером администрирования). Параметры Агента администрирования автоматически настраиваются по умолчанию.

Перед тем как установить Агент администрирования и программы защиты на устройства в сети, убедитесь, что эти устройства доступны (включены).

Возможна удаленная или локальная установка программ защиты и Агента администрирования.

Удаленная установка (см. раздел "Удаленная установка программ" на стр. 265) – с помощью мастера развертывания защиты вы можете удаленно установить программу защиты (например, Kaspersky Endpoint Security) и Агент администрирования на устройствах, которые были обнаружены Сервером администрирования в сети организации. Как правило, задача удаленной установки успешно распространяет защиту на большинство устройств сети, но на некоторых устройствах задача может завершиться с ошибкой – например, если устройство выключено или по каким-то другим причинам недоступно. В этом случае рекомендуется вручную подключиться к устройству и использовать локальную установку.

Локальная установка (см. раздел "Локальная установка программ" на стр. 298) – используется на тех устройствах сети, на которых не удалось развернуть защиту с помощью задачи удаленной установки. Чтобы установить защиту на такие устройства, создайте автономный пакет установки для запуска на этих устройствах локально.

Установка Агента администрирования на устройства под управлением операционных систем Linux и MacOS описана в *Руководстве администратора Kaspersky Endpoint Security 10 для Linux* и в *Руководстве администратора Kaspersky Endpoint Security 10 для Mac* соответственно. (Несмотря на то, что устройства под управлением операционных систем Linux и MacOS считаются менее уязвимыми, чем устройства под управлением Windows, на них также рекомендуется устанавливать программы защиты.)

После установки убедитесь, что программа защиты установлена на управляемые устройства. Для этого запустите Отчет о версиях программ "Лаборатории Касперского" и ознакомьтесь с его результатами.

14. Распространение ключей на клиентские устройства

Распространите ключи на клиентские устройства, чтобы активировать управляемые программы защиты на этих устройствах.

15. Настройка защиты мобильных устройств

Этот шаг имеется в мастере первоначальной настройки.

Если в сети организации используются мобильные устройства, разверните управление мобильными устройствами (см. раздел "Развертывание систем управления мобильными устройствами" на стр. 314).

16. Создание структуры групп администрирования

В некоторых случаях для развертывания защиты на устройствах сети оптимальным образом может потребоваться разделить устройства на группы администрирования (см. раздел "Построение структуры групп администрирования и назначение агентов обновлений" на стр. 201) с учетом организационной структуры организации. Вы можете создать правила перемещения для распределения устройств по группам (см. раздел "Правила перемещения устройств" на стр. 213) или распределить устройства

вручную. Для групп администрирования можно назначать групповые задачи, определять область действия политик и назначать агенты обновлений.

Убедитесь, что все управляемые устройства правильно распределены по соответствующим группам администрирования и что у вас в сети не осталось нераспределенных устройств.

17. **Назначение агентов обновлений**

    Агенты обновлений (см. раздел "Об агентах обновлений" на стр. 96) для групп администрирования назначаются автоматически, но при необходимости вы можете назначить их вручную. Агенты обновлений рекомендуется использовать в больших сетях для снижения нагрузки на Сервер администрирования, а также в сетях с распределенной структурой для предоставления Серверу администрирования доступа к устройствам или группам устройств, соединенным каналами с низкой пропускной способностью.

Результаты развертывания Kaspersky Security Center

В результате выполнения шагов сценария в сети организации будет развернута защита:

- Установлена СУБД для Сервера администрирования.
- Установлен Сервер администрирования Kaspersky Security Center.
- Созданы необходимые политики и задачи, а также настроены заданные по умолчанию параметры политик и задач.
- На управляемые устройства установлены программы защиты (например, Kaspersky Endpoint Security) и Агент администрирования.
- Созданы группы администрирования (возможно, объединенные в иерархию).
- При необходимости развернута защита мобильных устройств.
- При необходимости назначены агенты обновлений.

См. также

Порты, используемые Kaspersky Security Center

Ниже перечислены порты, которые должны быть открыты на Серверах администрирования и на клиентских устройствах (см. таблицу ниже). Курсивом обозначены порты, которые потребуется открыть, только если вы работаете с мобильными устройствами, с Веб-консолью и Self Service Portal (см. графы "Назначение порта" и "Область функциональности").

Таблица 1. Порты, используемые Kaspersky Security Center

Устройство	Номер порта	Имя процесса, открывающего порт	Протокол	Используется ли TLS (кроме портов UDP)	Назначение порта	Область функциональности
Сервер администрирования	8060	klcsweb	TCP	Нет	Передача на клиентские устройства опубликованных инсталляционных пакетов	Публикация инсталляционных пакетов
	8061	klcsweb	TCP	Да	Передача на клиентские устройства опубликованных инсталляционных пакетов	Публикация инсталляционных пакетов
	9000	*CSWebInterface*	*TCP*	*Да*	*Прием входящих подключений от сервера Apache*	*Работа с Веб-консолью и Self Service Portal*

Устройство	Номер порта	Имя процесса, открывающего порт	Протокол	Используется ли TLS (кроме портов UDP)	Назначение порта	Область функциональности
	13000	klserver	TCP	Да	Прием подключений от Агентов администрирования и от подчиненных Серверов администрирования; используется также на подчиненных серверах для приема подключений от главного Сервера (например, если подчиненный Сервер находится в демилитаризованной зоне)	Управление клиентскими устройствами и подчиненными Серверами администрирования

Устройство	Номер порта	Имя процесса, открывающего порт	Протокол	Используется ли TLS (кроме портов UDP)	Назначение порта	Область функциональности
	13000	klserver	UDP	Нет значения	Прием информации от Агентов администрирования о выключении устройств	Управление клиентскими устройствами
	13291	klserver	TCP	Да	Прием подключений от Консоли администрирования к Серверу администрирования	Управление Сервером администрирования
	13292	*klserver*	*TCP*	*Да*	*Прием подключений от мобильных устройств*	*Управление мобильными устройствами*
	13294	*klserver*	*TCP*	*Да*	*Прием подключений от устройств с защитой на уровне UEFI*	*Управление клиентскими устройствами с защитой на уровне UEFI*

Устройство	Номер порта	Имя процесса, открывающего порт	Протокол	Используется ли TLS (кроме портов UDP)	Назначение порта	Область функциональности
	13299	klserver	TCP	Да	Прием подключений по OpenAPI	OpenAPI
	14000	klserver	TCP	Нет	Прием подключений от Агентов администрирования	Управление клиентскими устройствами
	13111	*ksnproxy*	*TCP*	*Нет*	*Прием запросов от управляемых устройств к прокси-серверу KSN*	*Прокси-сервер KSN*
	15111	*ksnproxy*	*UDP*	*Нет значения*	*Прием запросов от управляемых устройств к прокси-серверу KSN*	*Прокси-сервер KSN*

Устройство	Номер порта	Имя процесса, открывающего порт	Протокол	Используется ли TLS (кроме портов UDP)	Назначение порта	Область функциональности
	17000	klactprx	TCP	Да	Прием подключений для активации лицензии от управляемых устройств (кроме мобильных устройств)	Прокси-сервер активации для мобильных устройств
	17100	*klactprx*	*TCP*	*Да*	*Прием подключений для активации лицензии от мобильных устройств*	*Прокси-сервер активации для мобильных устройств*

Устройство	Номер порта	Имя процесса, открывающего порт	Протокол	Используется ли TLS (кроме портов UDP)	Назначение порта	Область функциональности
Агент администрирования	15000	klnagent	UDP	Нет значения	Многоадресная рассылка Агентам администрирования	Доставка обновлений и инсталляционных пакетов
Агент обновлений	15001	klnagent	UDP	Нет значения	Многоадресная рассылка Агентам администрирования	Доставка обновлений и инсталляционных пакетов
	13000	klnagent	TCP	Да	Прием подключений от Агентов администрирования	Управление клиентскими устройствами, доставка обновлений и инсталляционных пакетов
Сервер iOS MDM	*443*	*kliosmdmservicesrv*	*TCP*	*Да*	*Прием соединений от мобильных устройств iOS*	*Управление мобильными устройствами*

См. также

Схемы взаимодействия компонентов Kaspersky Security Center и программ защиты 61

Схемы взаимодействия компонентов Kaspersky Security Center и программ защиты

В этом разделе приведены схемы взаимодействия между компонентами в составе Kaspersky Security Center и управляемыми программами защиты. На схемах приведены номера портов, которые должны быть доступны, и имена процессов, открывающих порты.

В этом разделе

Условные обозначения

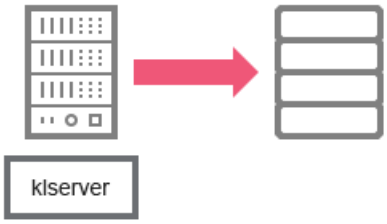
В таблице ниже приведены условные обозначения, использованные в схемах.

Таблица 2. Условные обозначения

Значок	Пояснение
	Сервер администрирования
	Подчиненный Сервер администрирования
	СУБД
	Клиентское устройство, на котором установлены Агент администрирования и программа семейства Kaspersky Endpoint Security (либо другая программа защиты, которой может управлять Kaspersky Security Center)
	Шлюз соединений
	Агент обновлений
	Мобильное клиентское устройство с установленной программой Kaspersky Security для мобильных устройств
	Браузер на устройстве пользователя
	Процесс, запущенный на устройстве и открывающий какой-либо порт

	Трафик TCP (направление стрелки обозначает направление трафика)
	Трафик UDP (направление стрелки обозначает направление трафика)
	Вызов COM
	Транспорт СУБД
	Граница демилитаризованной зоны

Сервер администрирования и СУБД



Данные от Сервера администрирования поступают в базу данных SQL Server или MySQL.

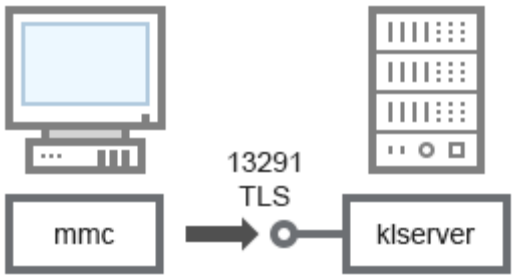
См. также

Условные обозначения 62

Схемы взаимодействия компонентов Kaspersky Security Center и программ защиты 61

Порты, используемые Kaspersky Security Center 53

Сервер администрирования и Консоль администрирования



Пояснения к схеме см. в таблице ниже.

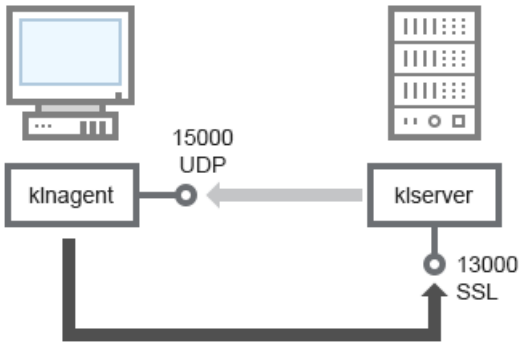
Таблица 3. Сервер администрирования и Консоль администрирования (трафик)

Устройство	Номер порта	Имя процесса, открывающего порт	Протокол	Используется ли TLS	Назначение порта
Сервер администрирования	13291	klserver	TCP	Да	Прием подключений от Консоли администрирования

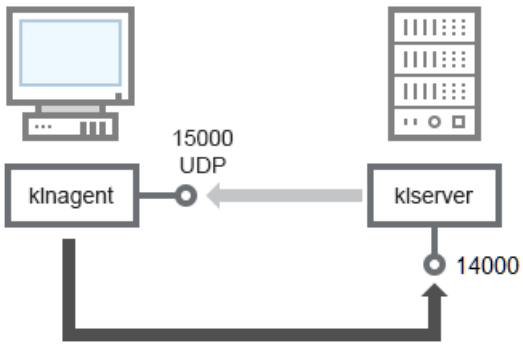
См. также

Сервер администрирования и клиентское устройство: управление программой защиты

Сервер администрирования принимает подключение от Агентов администрирования по защищенному порту 13000 (см. рис. ниже).



Если вы использовали Kaspersky Security Center одной из предыдущих версий, то в вашей сети Сервер администрирования может принимать подключения от Агентов администрирования по незащищенному порту 14000 (см. рис. ниже). Kaspersky Security Center 10 также поддерживает подключение Агентов администрирования по порту 14000, однако рекомендуется использовать защищенный порт 13000.



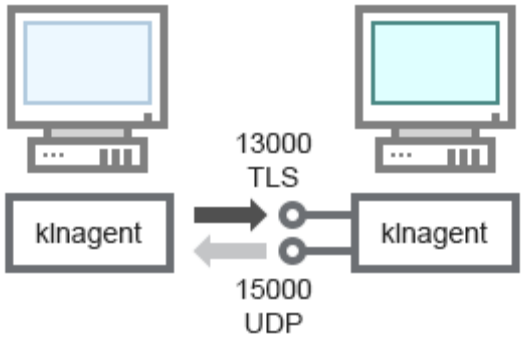
Пояснения к схемам см. в таблице ниже.

Таблица 4. Сервер администрирования и клиентское устройство: управление программой защиты (трафик)

Устройство	Номер порта	Имя процесса, открывающего порт	Протокол	Используется ли TLS для TCP	Назначение порта
Агент администрирования	15000	klnagent	UDP	Нет значения	Многоадресная рассылка Агентам администрирования
Сервер администрирования	13000	klserver	TCP	Да	Прием подключений от Агентов администрирования
Сервер администрирования	14000	klserver	TCP	Нет	Прием подключений от Агентов администрирования

См. также

Обновление программного обеспечения на клиентском устройстве с помощью агента обновлений



Пояснения к схеме см. в таблице ниже.

Таблица 5. Обновление программного обеспечения с помощью агента обновлений (трафик)

Устройство	Номер порта	Имя процесса, открывающего порт	Протокол	Используется ли TLS для TCP	Назначение порта
Агент администрирования	15000	klnagent	UDP	Нет значения	Многоадресная рассылка Агентам администрирования
Агент обновлений	13000	klnagent	TCP	Да	Прием подключений от Агентов администрирования

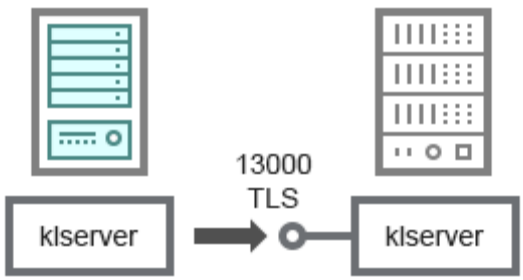
См. также

Иерархия Серверов администрирования: главный и подчиненный Серверы администрирования

На схеме (см. рис. ниже) показано, как используется порт 13000 для взаимодействия Серверов администрирования, объединенных в иерархию.

При объединении Серверов в иерархию необходимо, чтобы порт 13291 обоих Серверов был доступен. Через порт 13291 происходит подключение Консоли администрирования к Серверу администрирования (см. раздел "Сервер администрирования и Консоль администрирования" на стр. 65).

В дальнейшем, после объединения Серверов в иерархию, вы сможете администрировать оба Сервера через Консоль администрирования, подключенную к главному Серверу администрирования. Таким образом, необходимо только, чтобы порт 13291 главного Сервера был доступен.



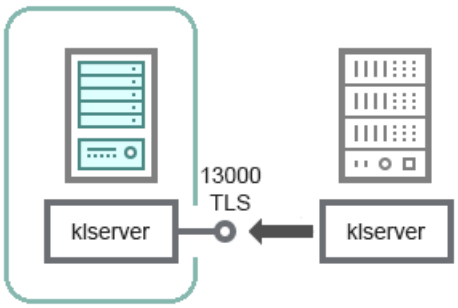
Пояснения к схеме см. в таблице ниже.

Таблица 6. Иерархия Серверов администрирования (трафик)

Устройство	Номер порта	Имя процесса, открывающего порт	Протокол	Используется ли TLS	Назначение порта
Главный Сервер администрирования	13000	klserver	TCP	Да	Прием подключений от подчиненных Серверов администрирования

См. также

Иерархия Серверов администрирования с подчиненным Сервером в демилитаризованной зоне



На схеме показана иерархия Серверов администрирования, в которой подчиненный Сервер, находящийся в демилитаризованной зоне, принимает подключение от главного Сервера (пояснения к схеме см. в таблице ниже). При объединении Серверов в иерархию необходимо, чтобы порт 13291 обоих Серверов был доступен. Через порт 13291 происходит подключение Консоли администрирования к Серверу администрирования (см. раздел "Сервер администрирования и Консоль администрирования" на стр. 65).

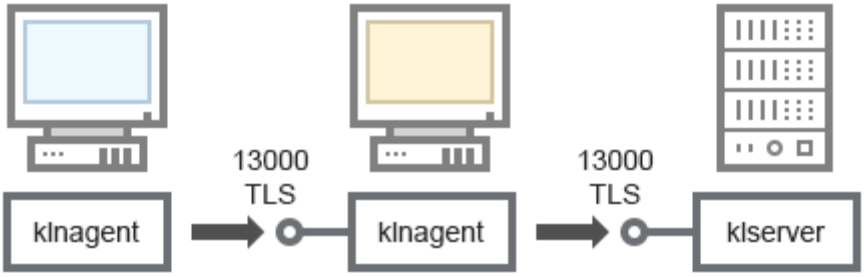
В дальнейшем, после объединения Серверов в иерархию, вы сможете администрировать оба Сервера через Консоль администрирования, подключенную к главному Серверу администрирования. Таким образом, необходимо только, чтобы порт 13291 главного Сервера был доступен.

Таблица 7. Иерархия Серверов администрирования с подчиненным Сервером в демилитаризованной зоне (трафик)

Устройство	Номер порта	Имя процесса, открывающего порт	Протокол	Используется ли TLS	Назначение порта
Подчиненный Сервер администрирования	13000	klserver	TCP	Да	Прием подключений от главного Сервера администрирования

См. также

Сервер администрирования, шлюз соединений в сегменте сети и клиентское устройство



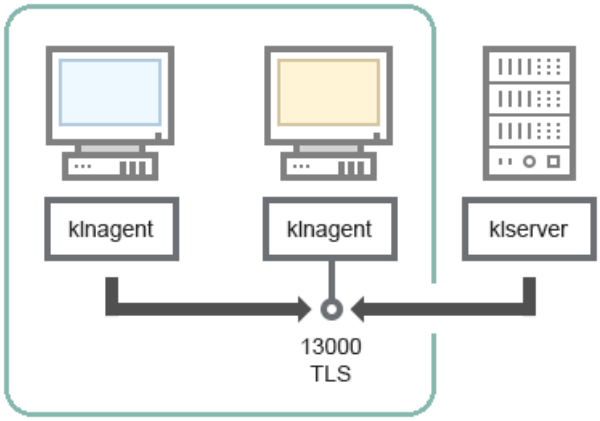
Пояснения к схеме см. в таблице ниже.

Таблица 8. Сервер администрирования, шлюз соединений в сегменте сети и клиентское устройство (трафик)

Устройство	Номер порта	Имя процесса, открывающего порт	Протокол	Используется ли TLS	Назначение порта
Сервер администрирования	13000	klserver	TCP	Да	Прием подключений от Агентов администрирования
Агент администрирования	13000	klnagent	TCP	Да	Прием подключений от Агентов администрирования

См. также

Сервер администрирования; шлюз соединений и клиентское устройство в демилитаризованной зоне



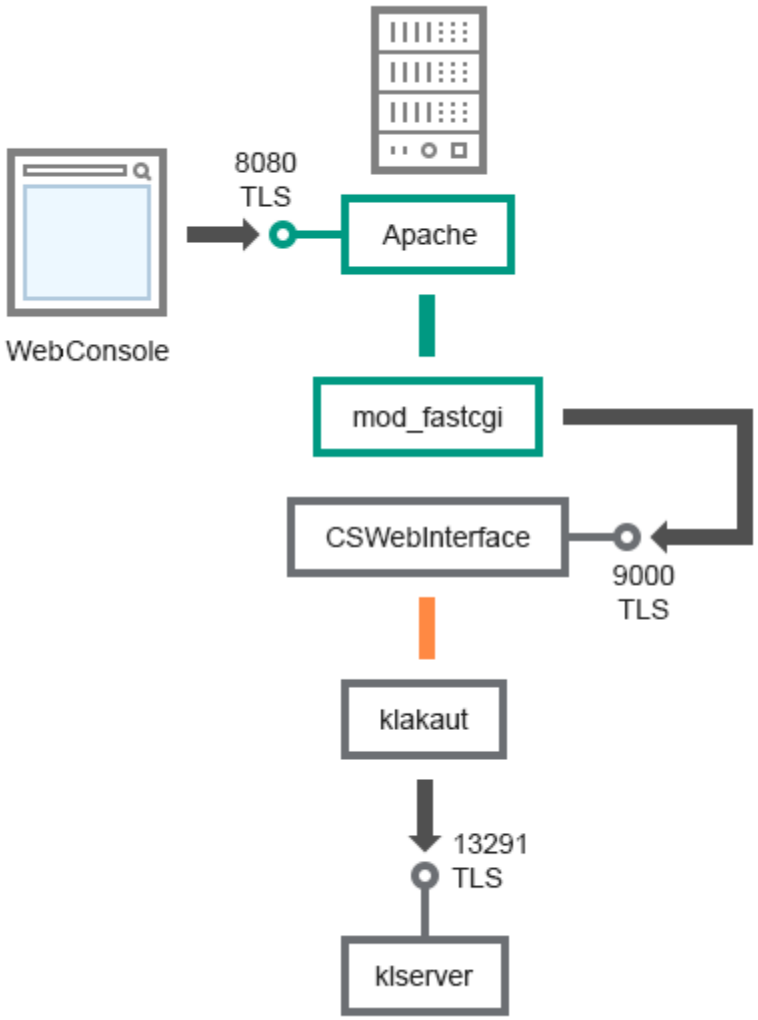
Пояснения к схеме см. в таблице ниже.

Таблица 9. Сервер администрирования, шлюз соединений в сегменте сети и клиентское устройство (трафик)

Устройство	Номер порта	Имя процесса, открывающего порт	Протокол	Используется ли TLS	Назначение порта
Агент администрирования	13000	klnagent	TCP	Да	Прием подключений от Агентов администрирования

См. также

Сервер администрирования и Веб-консоль



Пояснения к схеме см. в таблице ниже.

Таблица 10. Сервер администрирования и Веб-консоль (трафик)

Устройство	Номер порта	Имя процесса, открывающего порт	Протокол	Используется ли TLS	Назначение порта
Сервер администрирования	13291	klserver	TCP	Да	Прием подключений от Консоли администрирования к Серверу администрирования
Сервер администрирования	9000	CSWebInterface	TCP	Да	Прием входящих подключений от сервера Apache
Локальное устройство	8080	apache	TCP	Да	Прием подключений от Веб-консоли

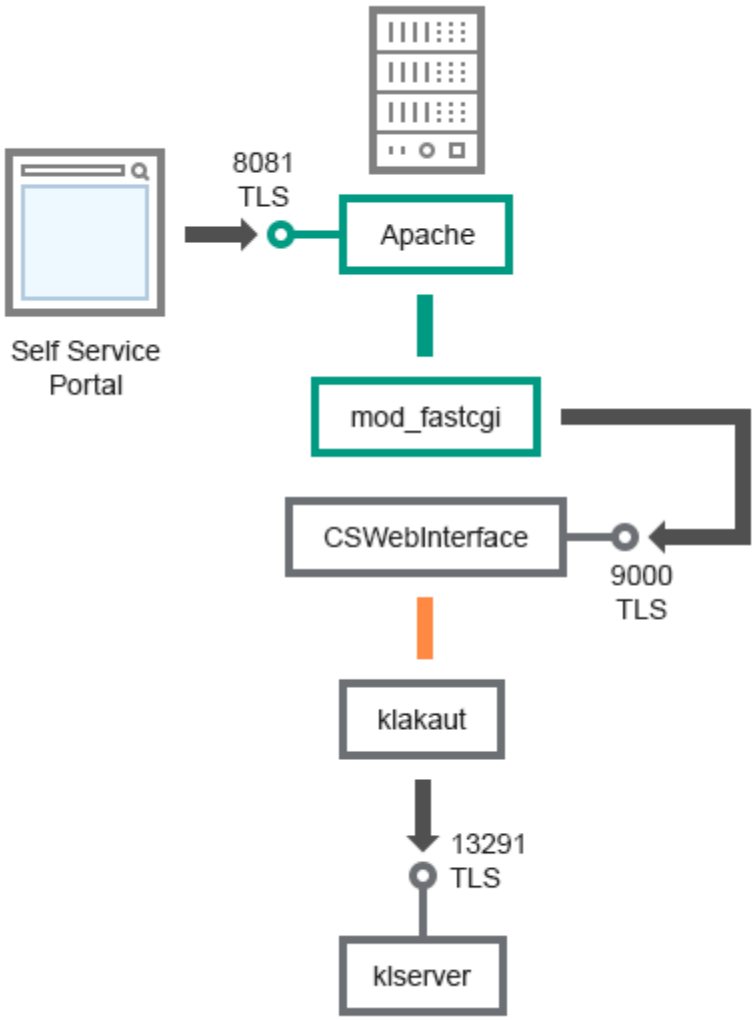
См. также

Условные обозначения 62

Схемы взаимодействия компонентов Kaspersky Security Center и программ защиты 61

Порты, используемые Kaspersky Security Center 53

Сервер администрирования и Self Service Portal



Пояснения к схеме см. в таблице ниже.

Таблица 11. Сервер администрирования и Self Service Portal (трафик)

Устройство	Номер порта	Имя процесса, открывающего порт	Протокол	Используется ли TLS	Назначение порта
Сервер администрирования	13291	klserver	TCP	Да	Прием подключений от Консоли администрирования к Серверу администрирования
Сервер администрирования	9000	CSWebInterface	TCP	Да	Прием входящих подключений от сервера Apache
Локальное устройство	8081	apache	TCP	Да	Прием подключений от Self Service Portal

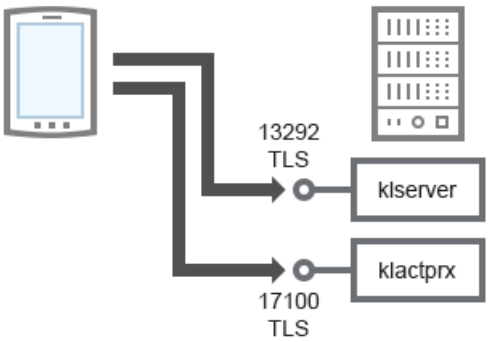
См. также

Условные обозначения 62

Схемы взаимодействия компонентов Kaspersky Security Center и программ защиты 61

Порты, используемые Kaspersky Security Center 53

Активация лицензии и управление программой защиты на мобильном устройстве



Пояснения к схеме см. в таблице ниже.

Таблица 12. Активация лицензии и управление программой защиты на мобильном устройстве (трафик)

Устройство	Номер порта	Имя процесса, открывающего порт	Протокол	Используется ли TLS	Назначение порта
Сервер администрирования	13292	klserver	TCP	Да	Прием подключений от Консоли администрирования к Серверу администрирования
Сервер администрирования	17100	klserver	TCP	Да	Прием подключений для активации лицензии от мобильных устройств

См. также

Условные обозначения 62

Схемы взаимодействия компонентов Kaspersky Security Center и программ защиты 61

Порты, используемые Kaspersky Security Center 53

Развертывание системы управления по протоколу Exchange ActiveSync 314

Подготовка к установке программы

Перед установкой программы убедитесь, что программные и аппаратные ресурсы компьютера, на который будет произведена установка, удовлетворяют требованиям, приведенным в разделе "Аппаратные и программные требования".

Также нужно убедиться, что для операционной системы и программных средств, необходимых для установки (если таковые имеются), установлены самые последние пакеты обновлений, выпускаемые производителями операционной системы и программного обеспечения.

Планирование развертывания Kaspersky Security Center

Этот раздел содержит информацию об оптимальных вариантах развертывания компонентов Kaspersky Security Center в сети организации в зависимости от различных факторов:

- общего количества устройств;
- наличия организационно или географически обособленных подразделений (офисов, филиалов);
- наличия обособленных сетей, связанных узкими каналами;
- необходимости доступа к Серверу администрирования из интернета.

В этом разделе

Общая информация о планировании развертывания Kaspersky Security Center в сети организации

Один Сервер администрирования может обслуживать не более чем 100 000 устройств. Если общее количество устройств в сети организации превышает 100 000, следует разместить в сети организации несколько Серверов администрирования, объединенных в иерархию для удобства централизованного управления.

Если в составе организации есть крупные географически удаленные офисы (филиалы) с собственными администраторами, целесообразно разместить в этих офисах Серверы администрирования. В противном случае такие офисы следует рассматривать как

обособленные сети, связанные узкими каналами, см. раздел "Типовая конфигурация: несколько крупных офисов с собственными администраторами (на стр. 90)".

При наличии обособленных сетей, связанных узкими каналами, в целях экономии трафика в таких сетях следует назначить один или несколько Агентов администрирования агентами обновлений (см. таблицу для расчета количества агентов обновлений (см. раздел "Расчет количества и конфигурации агентов обновлений" на стр. 98)). В этом случае все устройства обособленной сети будут получать обновления с таких "локальных центров обновлений". Сами же агенты обновлений могут загружать обновления как с Сервера администрирования (поведение по умолчанию), так и с размещенных в интернете серверов "Лаборатории Касперского", см. раздел "Типовая конфигурация: множество небольших удаленных офисов (на стр. 91)".

В разделе "Типовые конфигурации Kaspersky Security Center (на стр. 89)" приведены подробные описания типовых конфигураций Kaspersky Security Center. При планировании развертывания следует, в зависимости от структуры организации, выбрать наиболее подходящую типовую конфигурацию.

На этапе планирования развертывания следует рассмотреть необходимость задания Серверу администрирования специального сертификата X.509. Задание сертификата X.509 для Сервера администрирования может быть целесообразно в следующих случаях (неполный список):

- для инспекции SSL трафика посредством SSL termination proxy или для использования Reverse Proxy;
- для интеграции с инфраструктурой открытых ключей (PKI) организации;
- для задания желательных значений полей сертификата;
- для обеспечения желаемой криптографической стойкости сертификата.

Выбор структуры защиты организации

Выбор структуры защиты организации определяют следующие факторы:

- Топология сети организации.

- Организационная структура.
- Число сотрудников, отвечающих за защиту сети, и распределение обязанностей между ними.
- Аппаратные ресурсы, которые могут быть выделены для установки компонентов управления защитой.
- Пропускная способность каналов связи, которые могут быть выделены для работы компонентов защиты в сети организации.
- Допустимое время выполнения важных административных операций в сети организации. К важным административным операциям относятся, например, распространение обновлений антивирусных баз и изменение политик для клиентских устройств.

При выборе структуры защиты рекомендуется сначала определить имеющиеся сетевые и аппаратные ресурсы, которые могут использоваться для работы централизованной системы защиты.

Для анализа сетевой и аппаратной инфраструктуры рекомендуется следующий порядок действий:

1. Определить следующие параметры сети, в которой будет развертываться защита:
   - число сегментов сети;
   - скорость каналов связи между отдельными сегментами сети;
   - число управляемых устройств в каждом из сегментов сети;
   - пропускную способность каждого канала связи, которая может быть выделена для функционирования защиты.
2. Определить допустимое время выполнения ключевых операций администрирования для всех управляемых устройств.
3. Проанализировать информацию из пунктов 1 и 2, а также данные нагрузочного тестирования системы администрирования (см. раздел "Нагрузка на сеть" на стр. 368). На основании проведенного анализа ответить на следующие вопросы:

- Возможно ли обслуживание всех клиентов одним Сервером администрирования или требуется иерархия Серверов администрирования?
- Какая аппаратная конфигурация Серверов администрирования требуется для обслуживания всех клиентов за время, определенное в пункте 2?
- Требуется ли использование агентов обновлений для снижения нагрузки на каналы связи?

После ответа на перечисленные вопросы вы можете составить набор допустимых структур защиты организации.

В сети организации можно использовать одну из следующих типовых структур защиты:

- Один Сервер администрирования. Все клиентские устройства подключены к одному Серверу администрирования. Роль агента обновлений выполняет Сервер администрирования.
- Один Сервер администрирования с агентами обновлений. Все клиентские устройства подключены к одному Серверу администрирования. В сети выделены клиентские устройства, выполняющие роль агентов обновлений.
- Иерархия Серверов администрирования. Для каждого сегмента сети выделен отдельный Сервер администрирования, включенный в общую иерархию Серверов администрирования. Роль агента обновлений выполняет главный Сервер администрирования.
- Иерархия Серверов администрирования с агентами обновлений. Для каждого сегмента сети выделен отдельный Сервер администрирования, включенный в общую иерархию Серверов администрирования. В сети выделены клиентские устройства, выполняющие роль агентов обновлений.

См. также

Типовая конфигурация агентов обновлений: один офис 202

Типовая конфигурация: несколько крупных офисов с собственными администраторами 90

Типовая конфигурация: множество небольших удаленных офисов 91

О выборе СУБД для Сервера администрирования

При выборе СУБД, используемой Сервером администрирования, следует руководствоваться количеством устройств, которые обслуживает Сервер администрирования.

SQL Server Express Edition ограничен по количеству используемой памяти, по количеству используемых ядер процессора и по максимальному размеру базы данных. Поэтому SQL Server Express Edition не может использоваться, если Сервер администрирования обслуживает более 10 000 устройств, либо если на управляемых устройствах используется компонент Контроль программ.

Если Сервер администрирования обслуживает более 10 000 устройств, рекомендуется использовать SQL Server с меньшими ограничениями, например: SQL Server Workgroup Edition, SQL Server® Web Edition, SQL Server Standard Edition, SQL Server Enterprise Edition.

Если Сервер администрирования обслуживает не более 10 000 устройств и если на управляемых устройствах не используется компонент Контроль программ, вы можете использовать в качестве СУБД также MySQL 5.5, 5.6, 5.7. Не поддерживаются версии MySQL 5.5.1, 5.5.2, 5.5.3, 5.5.4, 5.5.5.

См. также

Типовые конфигурации Kaspersky Security Center

В этом разделе описаны следующие типовые конфигурации размещения компонентов Kaspersky Security Center в сети организации:

- один офис;
- несколько крупных географически распределенных офисов с собственными администраторами;
- множество небольших географически распределенных офисов.

В этом разделе

Типовая конфигурация: один офис

В сети организации может быть размещен один или несколько Серверов администрирования. Количество Серверов может быть выбрано как исходя из наличия доступного аппаратного обеспечения (см. раздел "Аппаратные требования для СУБД и

Сервера администрирования" на стр. 398), так и в зависимости от общего количества управляемых устройств.

Один Сервер администрирования может обслуживать до 100 000 устройств. Нужно учесть возможность увеличения количества управляемых устройств в ближайшем будущем: может оказаться желательным подключение несколько меньшего количества устройств к одному Серверу администрирования.

Серверы администрирования могут быть размещены как во внутренней сети, так и в демилитаризованной зоне, в зависимости от того, нужен ли доступ к Серверам администрирования из интернета.

Если Серверов несколько, рекомендуется объединить их в иерархию. Наличие иерархии Серверов администрирования позволяет избежать дублирования политик и задач, работать со всем множеством управляемых устройств, как если бы они все управлялись одним Сервером администрирования: выполнять поиск устройств, создавать выборки устройств, создавать отчеты.

См. также

Об агентах обновлений..... 96

Оценка места на диске для агента обновлений 404

Оценка трафика между Агентом администрирования и Сервером администрирования . 429

Роль иерархии Серверов администрирования..... 99

Порты, используемые Kaspersky Security Center 53

Типовая конфигурация: несколько крупных офисов с собственными администраторами

При наличии нескольких крупных удаленных офисов следует рассмотреть возможность размещения Серверов администрирования в каждом из офисов, по одному или по несколько Серверов администрирования в каждом, в зависимости от количества клиентских устройств

и доступного аппаратного обеспечения. В таком случае каждый из офисов может быть рассмотрен как "Типовая конфигурация: один офис (на стр. 89)". Для упрощения администрирования все Серверы администрирования следует объединить в иерархию, возможно, многоуровневую.

При наличии сотрудников, которые перемещаются между офисами вместе с устройствами (ноутбуками), в политике Агента администрирования следует создать правила переключения Агента администрирования между Серверами администрирования.

См. также

Настройка профилей соединения для автономных пользователей 311

Роль иерархии Серверов администрирования..... 99

Типовая конфигурация: один офис 89

Порты, используемые Kaspersky Security Center 53

Типовая конфигурация: множество небольших удаленных офисов

Эта типовая конфигурация предусматривает один главный офис и множество небольших удаленных офисов, возможно, связанных с главным офисом через интернет. Возможно, каждый из удаленных офисов находится за Network Address Translation (далее также NAT), то есть подключение из одного удаленного офиса в другой невозможно, офисы изолированы друг от друга.

В главном офисе следует поместить Сервер администрирования, а в остальных офисах назначить по одному или по несколько агентов обновлений. Если связь между офисами осуществляется через интернет, то может быть целесообразным создать для агентов обновлений задачу **Принудительная загрузка обновлений в хранилища агентов обновлений**, так, чтобы агенты обновлений загружали обновления не с Сервера администрирования, а непосредственно с серверов "Лаборатории Касперского".

Если в удаленном офисе часть устройств не имеет прямого доступа к Серверу администрирования (например, доступ к Серверу администрирования осуществляется через интернет, но доступ в интернет есть не у всех устройств), то агенты обновлений следует переключить в режим шлюза (Connection Gateway). В таком случае Агенты администрирования на устройствах в удаленном офисе будут подключаться (с целью синхронизации) к Серверу администрирования не напрямую, а через шлюз.

Поскольку Сервер администрирования, скорее всего, не сможет опрашивать сеть в удаленном офисе, целесообразно возложить выполнение этой функции на один из агентов обновлений.

Сервер администрирования не сможет посылать уведомления на порт 15000 UDP управляемым устройствам, размещенным за NAT в удаленном офисе. Для решения этой проблемы целесообразно включить в свойствах устройств, являющихся агентами обновлений, режим постоянного соединения с Сервером администрирования (флажок **Не разрывать соединение с Сервером администрирования**). Этот режим доступен, если общее количество агентов обновлений не превышает 300.

См. также

Об агентах обновлений 96

Предоставление доступа к Серверу администрирования из интернета 92

Порты, используемые Kaspersky Security Center 53

Предоставление доступа к Серверу администрирования из интернета

В ряде случаев необходимо предоставить доступ к Серверу администрирования из интернета:

- для управления устройствами (ноутбуками) автономных пользователей;
- для управления устройствами, находящимися в удаленных офисах;

- при взаимодействии с главным или подчиненными Серверами администрирования, находящимися в удаленных офисах;
- для управления мобильными устройствами.

В этом разделе рассмотрены типичные способы обеспечения доступа к Серверу администрирования из интернета. Во всех случаях предоставления доступа к Серверу администрирования из интернета может понадобиться задать Серверу администрирования специальный сертификат (см. раздел "Задание сертификата Сервера администрирования" на стр. 124).

В этом разделе

Доступ из интернета: Сервер администрирования в локальной сети

Если Сервер администрирования располагается во внутренней сети организации, с помощью механизма "Port Forwarding" порт Сервера администрирования 13000 TCP делается доступным извне. Если требуется управление мобильными устройствами, то делается доступным извне порт 13292 TCP.

Доступ из интернета: Сервер администрирования в демилитаризованной зоне

Если Сервер администрирования располагается в демилитаризованной зоне сети организации, у него отсутствует доступ во внутреннюю сеть организации. Как следствие, возникают следующие ограничения:

- Сервер администрирования не может самостоятельно обнаруживать новые устройства.
- Сервер администрирования не может выполнять первоначальное развертывание Агента администрирования посредством push-инсталляции на устройства внутренней сети организации.

Речь идет только о первоначальной установке Агента администрирования. Последующие обновления версии Агента администрирования или установка программы защиты уже могут быть выполнены Сервером администрирования. Однако первоначальное развертывание Агентов администрирования может быть выполнено иными средствами, например, при помощи групповых политик Microsoft® Active Directory®.

- Сервер администрирования не может посылать управляемым устройствам уведомления на порт 15000 UDP, что не является критичным для функциональности Kaspersky Security Center.
- Сервер администрирования не может опрашивать Active Directory. Однако результаты опроса Active Directory не нужны в большинстве сценариев.

Если описанные выше ограничения критичны, они могут быть сняты при помощи агентов обновлений, размещенных в сети организации:

- Для выполнения первоначального развертывания на устройства без Агента администрирования следует предварительно установить Агент администрирования на одно из устройств и назначить это устройство агентом обновлений. В результате первоначальная установка Агента администрирования на прочие устройства будет выполняться Сервером администрирования через этот агент обновлений.

- Для обнаружения новых устройств во внутренней сети организации и для опроса Active Directory следует на одном из агентов обновлений включить желаемые виды опроса сети.

- Для успешной отправки уведомлений управляемым устройствам, размещенным во внутренней сети организации, на порт 15000 UDP, следует покрыть всю сеть предприятия агентами обновлений. В свойствах назначенных агентов обновлений следует установить флажок **Не разрывать соединение с Сервером администрирования**. В результате Сервер администрирования будет иметь постоянную связь с агентами обновлений, а агенты обновлений смогут посылать уведомления на порт 15000 UDP устройствам, размещенным во внутренней сети организации (см. раздел "Об агентах обновлений" на стр. 96).

Доступ из интернета: Агент администрирования в качестве шлюза соединений в демилитаризованной зоне

Описанный ниже режим доступа применим для Kaspersky Security Center 10 Service Pack 1 и более поздних версий.

Сервер администрирования может располагаться во внутренней сети организации, а в демилитаризованной зоне сети может находиться устройство с Агентом администрирования, работающим в качестве шлюза соединений с обратным направлением подключения (Сервер администрирования устанавливает соединение с Агентом администрирования). В этом случае для организации доступа из интернета нужно выполнить следующие условия:

- На устройство, находящееся в демилитаризованной зоне, следует установить Агент администрирования. При установке Агента администрирования в окне мастера установки **Шлюз соединений** выбрать вариант **Использовать в качестве шлюза соединений в демилитаризованной зоне**.

- На Сервере администрирования следует создать отдельную группу администрирования, в свойствах которой назначить по адресу в качестве шлюза

соединений указанное выше устройство из демилитаризованной зоны. В эту группу администрирования не следует добавлять какие-либо устройства.

- Для Агентов администрирования, обращающихся к Серверу администрирования из интернета, при установке следует указать созданный выше шлюз соединений с помощью параметра **Подключаться к Серверу через шлюз соединений**.

Для шлюза соединений, находящегося в демилитаризованной зоне, Сервер администрирования создает сертификат, подписанный сертификатом Сервера администрирования. Если администратор принял решение задать Серверу администрирования пользовательский сертификат, то это следует сделать до создания шлюза соединений в демилитаризованной зоне.

При наличии сотрудников с ноутбуками, которые могут подключаться к Серверу администрирования как из локальной сети, так и из интернета, может быть целесообразно создать в политике Агента администрирования правило переключения Агента администрирования.

Об агентах обновлений

Агент администрирования может быть использован в качестве агента обновлений. В этом режиме Агент администрирования может выполнять следующие функции:

- Раздавать обновления, причем обновления могут быть получены как с Сервера администрирования, так и с серверов "Лаборатории Касперского". В последнем случае для устройства, являющегося агентом обновлений, должна быть создана задача **Принудительная загрузка обновлений в хранилища агентов обновлений**.

- Устанавливать программное обеспечение на другие устройства, в том числе выполнять первоначальное развертывание Агентов администрирования на устройствах.

- Опрашивать сеть с целью обнаружения новых устройств и обновления информации об уже известных устройствах. Агент обновлений может выполнять те же виды опроса сети, что и Сервер администрирования.

Размещение агентов обновлений в сети организации преследует следующие цели:

- Уменьшить нагрузку на Сервер администрирования.
- Оптимизировать трафик.
- Предоставить Серверу администрирования доступ к устройствам в труднодоступных частях сети организации. Наличие агента обновлений в находящейся за NAT (по отношению к Серверу администрирования) сети позволяет Серверу администрирования выполнять следующие действия:
  - отправлять устройствам уведомления по UDP;
  - опрашивать сеть;
  - выполнять первоначальное развертывание.

Агент обновлений назначается на группу администрирования. В этом случае областью действия агента обновлений будут устройства, находящиеся в такой группе администрирования и всех ее подгруппах. При этом устройство, являющееся агентом обновлений, не обязано находиться в группе администрирования, на которую оно назначено.

Вы можете назначить агент обновлений шлюзом соединений. В этом случае находящиеся в его области действия устройства будут подключаться к Серверу администрирования не напрямую, а через шлюз. Данный режим полезен в сценариях, когда между устройствами с Агентом администрирования и Сервером администрирования невозможно прямое соединение.

См. также

Построение структуры групп администрирования и назначение агентов обновлений 201

Расчет количества и конфигурации агентов обновлений

Чем больше клиентских устройств в сети, тем больше необходимость в агентах обновлений. Рекомендуется не отключать автоматическое назначение агентов обновлений. При включенном автоматическом назначении агентов обновлений Сервер администрирования назначает агенты обновлений, если число клиентских устройств достаточно велико, и определяет их конфигурацию.

Использование постоянно включенных и доступных устройств

Если вы планируете использовать в качестве агентов обновлений какие-то определенные устройства (например, выделенные для этого серверы), то вы можете не использовать автоматическое назначение агентов обновлений. В этом случае убедитесь, что устройства, которые вы хотите назначить агентом обновлений, имеют достаточно свободного места на диске (см. раздел "Оценка места на диске для агента обновлений" на стр. 404), их не отключают регулярно и на них выключен "спящий режим".

Если вы планируете использовать в качестве агента обновлений специально выделенное для этого устройство, то рекомендуется назначать один агент обновлений не более чем на 1000 клиентских устройств. Если вы планируете использовать в качестве агентов обновлений обычное клиентское устройство, то рекомендуется назначать один агент обновлений не более чем на 100 устройств. При превышении рекомендуемого числа клиентских устройств на один агент обновлений возрастает нагрузка на процессор, что может помешать повседневной работе пользователей.

Использование устройств, которые регулярно бывают отключены или недоступны

Если устройство, назначенное агентом обновлений, отключено или по другим причинам недоступно, то управляемые устройства, которые подключаются к этому агенту обновлений, могут обращаться за обновлениями к Серверу администрирования.

Если вы планируете использовать в качестве агентов обновлений устройства, которые регулярно бывают отключены или уходят в "спящий режим", то во избежание избыточной нагрузки на Сервер администрирования рекомендуется назначать агенты обновлений следующим образом (см. таблицу ниже):

Таблица 13. Количество агентов обновлений в зависимости от количества устройств

в сети

Количество устройств в сети	Количество агентов обновлений
Менее 10	0 (не назначать агенты обновлений)
10–30	1
30–300	2
Более 300	(N/1000 +1), где N – число устройств в сети, но не менее 3 агентов обновлений

Роль иерархии Серверов администрирования

В организации может быть более одного Сервера администрирования. Администрировать несколько разрозненных Серверов неудобно, поэтому целесообразно объединять их в иерархию. Взаимодействие "главный – подчиненный" между двумя Серверами администрирования предоставляет следующие возможности:

- Подчиненный Сервер наследует с главного Сервера политики и задачи, устраняется дублирование параметров.
- Выборки устройств на главном Сервере могут включать в себя устройства с подчиненных Серверов.
- Отчеты на главном Сервере могут включать в себя данные (в том числе и детальные) с подчиненных Серверов.

Виртуальные Серверы администрирования

В рамках физического Сервера администрирования можно создать несколько виртуальных Серверов администрирования, во многом подобных подчиненным Серверам. По сравнению

с моделью разделения доступа, основанной на списках контроля доступа (ACL), модель виртуальных Серверов более функциональна и предоставляет большую степень изоляции. Помимо собственной структуры групп администрирования для распределенных устройств с политиками и задачами, каждый виртуальный Сервер администрирования имеет также собственную группу нераспределенных устройств, собственные наборы отчетов, выборок устройств и событий, инсталляционных пакетов, правил перемещения устройств и так далее. Функциональность виртуальных Серверов администрирования может быть использована как сервис-провайдерами (xSP) для максимальной изоляции разных заказчиков друг от друга, так и крупными организациями со сложной структурой и большим количеством администраторов.

Виртуальные Серверы во многом подобны подчиненным Серверам администрирования, однако имеют следующие отличия:

- виртуальный Сервер не имеет большинства глобальных параметров и собственных TCP-портов;
- у виртуального Сервера не может быть подчиненных Серверов;
- у виртуального Сервера не может быть собственных виртуальных Серверов;
- на физическом Сервере администрирования видны устройства, группы, события и объекты с управляемых устройств (элементы карантина, реестра приложений и прочее) всех его виртуальных Серверов;
- виртуальный Сервер может сканировать сеть только посредством подключенных к нему агентов обновлений.

Установка образов операционных систем

Kaspersky Security Center позволяет разворачивать на устройства сети организации wim-образы настольных и серверных версий операционных систем Windows®.

Образ операционной системы, пригодный для развертывания средствами Kaspersky Security Center, может быть получен следующими способами:

- импортом из файла install.wim, который входит в состав дистрибутива Windows;
- захватом образа с эталонного устройства.

Поддерживаются два сценария развертывания образа операционной системы:

- развертывание на "чистое" устройство, то есть на устройство без установленной на нем операционной системы;
- развертывание на устройство, работающее под управлением операционной системы Windows.

В составе Сервера администрирования неявно присутствует служебный образ WinPE (Windows Preinstallation Environment), который всегда используется как при захвате, так и во время развертывания образов операционной системы. В WinPE следует добавить все драйверы, необходимые для правильной работы всех устройств. Как правило, требуется добавить драйверы чипсета, необходимые для работы сетевого интерфейса Ethernet.

Для реализации сценариев развертывания и захвата образов должны быть выполнены следующие требования:

- На Сервер администрирования должен быть установлен Windows Automated Installation Kit (WAIK) версии 2.0 и выше или Windows Assessment and Deployment Kit (WADK). Если предполагаются работы по установке или захвату образов на Windows XP, следует установить WAIK.
- В сети, в которой расположено устройство, должен присутствовать DHCP-сервер.
- Папка общего доступа Сервера администрирования должна быть доступна для чтения из сети, в которой находится устройство. Если папка общего доступа расположена на Сервере администрирования, то доступ нужен для учетной записи KlPxeUser (эта учетная запись создается автоматически на этапе работы инсталлятора Сервера администрирования). Если папка расположена вне Сервера администрирования, то доступ нужен для всех.

При выборе образа операционной системы для установки администратор должен явно указать архитектуру процессора устройства: x86 или x86-64.

Подготовка к управлению мобильными устройствами

Этот раздел содержит информацию:

- о сервере мобильных устройств Exchange ActiveSync для управления мобильными устройствами по протоколу Exchange ActiveSync;
- о сервере iOS MDM для управления iOS-устройствами путем установки на них специализированных iOS MDM-профилей;
- об управлении мобильными устройствами с установленным приложением Kaspersky Endpoint Security для Android.

В этом разделе

Сервер мобильных устройств Exchange ActiveSync

Сервер мобильных устройств Exchange ActiveSync® позволяет управлять мобильными устройствами, которые подключаются к Серверу администрирования по протоколу Exchange ActiveSync (EAS-устройствами).

В этом разделе

Способы развертывания Сервера мобильных устройств Exchange ActiveSync

Если в организации развернуто несколько серверов Microsoft Exchange с ролью клиентского доступа, объединенных в массив (Client Access Server Array), то Сервер мобильных устройств Exchange ActiveSync следует устанавливать на каждый сервер в массиве. В мастере установки Сервера мобильных устройств Exchange ActiveSync необходимо выбрать **Режим кластера**. В этом случае совокупность экземпляров Сервера мобильных устройств Exchange ActiveSync, установленных на серверы массива, будет называться кластером Серверов мобильных устройств Exchange ActiveSync.

Если в организации не развернут массив серверов Microsoft Exchange с ролью клиентского доступа, то Сервер мобильных устройств Exchange ActiveSync следует устанавливать на сервер Microsoft Exchange, имеющий роль Client Access. При этом в мастере установки Сервера мобильных устройств Exchange ActiveSync необходимо выбрать **Обычный режим**.

Вместе с Сервером мобильных устройств Exchange ActiveSync на устройство необходимо установить Агент администрирования, с помощью которого осуществляется интеграция Сервера с Kaspersky Security Center.

По умолчанию область сканирования Сервера мобильных устройств Exchange ActiveSync – это текущий домен Active Directory, в котором он установлен. В случае развертывания Сервера мобильных устройств Exchange ActiveSync на сервере Microsoft Exchange 2010–2013 имеется возможность расширить область сканирования на весь лес доменов, см. раздел Настройка области сканирования. Запрашиваемая при сканировании информация включает в себя учетные записи пользователей сервера Microsoft Exchange, политики

Exchange ActiveSync и мобильные устройства пользователей, подключенные к серверу Microsoft Exchange по протоколу Exchange ActiveSync.

В пределах одного домена недопустима установка нескольких экземпляров Сервера мобильных устройств Exchange ActiveSync, работающих в **Обычном режиме** и управляемых одним и тем же Сервером администрирования.

В пределах одного леса доменов Active Directory также недопустима установка нескольких экземпляров Сервера мобильных устройств Exchange ActiveSync (или нескольких кластеров Сервера мобильных устройств Exchange ActiveSync), работающих в **Обычном режиме**, с расширенной областью сканирования на весь лес доменов и подключенных к одному и тому же Серверу администрирования.

Необходимые права для развертывания Сервера мобильных устройств Exchange ActiveSync

Для развертывания Сервера мобильных устройств Exchange ActiveSync на серверах Microsoft Exchange 2010–2013 требуются права доменного администратора и роль Organization Management. Для развертывания Сервера мобильных устройств Exchange ActiveSync на сервере Microsoft Exchange 2007 требуются права доменного администратора и членство в группе безопасности Exchange Organization Administrators.

Учетная запись для работы службы Exchange ActiveSync

В процессе установки Сервера мобильных устройств Exchange ActiveSync в Active Directory автоматически создается учетная запись:

- на сервере Microsoft Exchange 2010–2013 – учетная запись KLMDM4ExchAdmin***** с ролью KLMDM Role Group;
- на сервере Microsoft Exchange 2007 – учетная запись KLMDM4ExchAdmin*****, являющаяся членом группы безопасности KLMDM Secure Group.

Под этой учетной записью работает служба Сервера мобильных устройств Exchange ActiveSync.

Если вы хотите отказаться от автоматического создания учетной записи, то необходимо создать собственную учетную запись, обладающую следующими правами:

- В случае использования сервера Microsoft Exchange 2010–2013 учетная запись должна обладать ролью, для которой разрешено выполнение следующих командлетов:
  - Get-CASMailbox;
  - Set-CASMailbox;
  - Remove-ActiveSyncDevice;
  - Clear-ActiveSyncDevice;
  - Get-ActiveSyncDeviceStatistics;
  - Get-AcceptedDomain;
  - Set-AdServerSettings;
  - Get-ActiveSyncMailboxPolicy;
  - New-ActiveSyncMailboxPolicy;
  - Set-ActiveSyncMailboxPolicy;
  - Remove-ActiveSyncMailboxPolicy.
- В случае использования сервера Microsoft Exchange 2007, для учетной записи должны быть назначены права доступа к объектам Active Directory (см. таблицу ниже).

Таблица 14. Права доступа к объектам Active Directory

Доступ	Объект	Командлет
Полный	Ветка "CN=Mobile Mailbox Policies,CN=<Название организации>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<Имя домена>"	`Add-ADPermission -User <Имя пользователя или группы> -Identity "CN=Mobile Mailbox Policies,CN=<Название организации>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<Имя домена>" -InheritanceType All -AccessRight GenericAll`
Чтение	Ветка "CN=<Название организации>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<Имя домена>"	`Add-ADPermission -User <Имя пользователя или группы> -Identity "CN=<Название организации>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<Имя домена>" -InheritanceType All -AccessRight GenericRead`
Чтение и запись	Свойства msExchMobileMailboxPolicyLink и msExchOmaAdminWirelessEnable для объектов в Active Directory	`Add-ADPermission -User <Имя пользователя или группы> -Identity "DC=<Имя домена>" -InheritanceType All -AccessRight ReadProperty,WriteProperty -Properties msExchMobileMailboxPolicyLink, msExchOmaAdminWirelessEnable`

Доступ	Объект	Командлет
Расширенное право ms-Exch-Store-Active	Хранилища почтовых ящиков Exchange-сервера, ветка "CN=Databases,CN=Exchange Administrative Group (FYDIBOHF23SPDLT),CN=Administrative Groups,CN=<Название организации>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<Имя домена>"	`Get-MailboxDatabase | Add-ADPermission -User <Имя пользователя или группы> -ExtendedRights ms-Exch-Store-Admin`

Сервер iOS MDM

Сервер iOS MDM позволяет осуществлять управление iOS-устройствами путем установки на них специализированных iOS MDM-профилей. Поддерживаются следующие функции:

- блокирование устройства;
- сброс пароля;
- удаление данных устройства;
- установка или удаление приложений;
- применение iOS MDM-профиля с дополнительными параметрами (такими как параметры VPN, почты, Wi-Fi, камеры, сертификаты, и так далее).

Сервер iOS MDM представляет собой веб-сервис, который принимает входящие соединения от мобильных устройств на свой TLS-порт (по умолчанию порт 443) и управляется со стороны Kaspersky Security Center с помощью Агента администрирования. Агент администрирования устанавливается локально на устройстве с развернутым Сервером iOS MDM.

В процессе развертывания Сервера iOS MDM администратору необходимо выполнить следующие действия:

- обеспечить Агенту администрирования доступ к Серверу администрирования;

- обеспечить мобильным устройствам доступ к TCP-порту Сервера iOS MDM.

В этом разделе рассмотрены две типовые конфигурации Сервера iOS MDM.

В этом разделе

Типовая конфигурация: Kaspersky Device Management для iOS в демилитаризованной зоне

Сервер iOS MDM располагается в демилитаризованной зоне сети организациис доступом в интернет. Особенностью данного подхода является отсутствие проблем с доступностью веб-сервиса iOS MDM из интернета со стороны устройств.

Так как для управления Сервером iOS MDM требуется локально установленный Агент администрирования, необходимо обеспечить взаимодействие этого Агента администрирования с Сервером администрирования. Это можно сделать следующими способами:

- Поместить Сервер администрирования в демилитаризованную зону.
- Использовать шлюз соединений (см. раздел "Доступ из интернета: Агент администрирования в качестве шлюза соединений в демилитаризованной зоне" на стр. 95):
    a. На устройстве с развернутым Сервером iOS MDM подключить Агент администрирования к Серверу администрирования через шлюз соединений.
    b. На устройстве с развернутым Сервером iOS MDM назначить Агент администрирования шлюзом соединений.

См. также

Упрощенная схема развертывания 333

Типовая конфигурация: Сервер iOS MDM в локальной сети организации

Сервер iOS MDM располагается во внутренней сети организации. Порт 443 (порт по умолчанию) делается доступным извне. Например, посредством публикации веб-сервиса iOS MDM на Microsoft Forefront® Threat Management Gateway (далее TMG) (см. раздел "Схема подключения KES-устройств к Серверу с использованием принудительного делегирования Kerberos (KCD)" на стр. 352).

В любой типовой конфигурации потребуется обеспечить доступность для Сервера iOS MDM веб-сервисов Apple (диапазон адресов 17.0.0.0/8) по порту TCP 2195. Этот порт используется для оповещения устройств о новых командах через специализированный сервис APN (см. раздел "Настройка доступа к сервису Apple Push Notification" на стр. 343).

Управление мобильными устройствами с установленным Kaspersky Endpoint Security для Android

Управление мобильными устройствами с установленным приложением Kaspersky Endpoint Security для Android™ (далее KES-устройства) осуществляется с помощью Сервера администрирования. В программе Kaspersky Security Center 10 Service Pack 1 и выше поддерживаются следующие возможности по управлению KES-устройствами:

- работа с мобильными устройствами как с клиентскими устройствами:
  - членство в группах администрирования;
  - статусы, события, отчеты и прочее;

- изменение локальных параметров и назначение политик для приложения Kaspersky Endpoint Security для Android;

- централизованная отправка команд;

- удаленная установка пакетов мобильных приложений.

Обслуживание KES-устройств осуществляется Сервером администрирования по протоколу TLS, порт TCP 13292.

См. также

Предоставление доступа к Серверу администрирования из интернета 92

Задание сертификата Сервера администрирования 124

Развертывание и первоначальная настройка

Kaspersky Security Center представляет собой распределенное приложение. В состав Kaspersky Security Center входят следующие программы:

- Сервер администрирования – центральный компонент, ответственный за управление устройствами организации и хранение данных в СУБД.
- Консоль администрирования – основной инструмент администратора. Консоль администрирования поставляется вместе с Сервером администрирования, но может быть также установлена отдельно на одно или несколько устройств администратора.
- Агент администрирования – служит для управления установленной на устройстве программой защиты, а также для получения информации об устройстве. Агенты администрирования устанавливаются на устройства организации.

Развертывание Kaspersky Security Center в сети организации осуществляется следующим образом:

- установка Сервера администрирования;
- установка Консоли администрирования на устройстве администратора;
- установка Агента администрирования и программы защиты на устройства организации.

В этом разделе

Сведения о производительности Сервера администрирования

В разделе представлены результаты тестирования производительности Сервера администрирования для разных аппаратных конфигураций, а также ограничения на подключение управляемых устройств к Серверу администрирования.

В этом разделе

Ограничения подключений к Серверу администрирования

Сервер администрирования поддерживает управление до 100 000 устройств без потери производительности.

Ограничения на подключения к Серверу администрирования без потери производительности:

- Один Сервер администрирования может поддерживать до 500 виртуальных Серверов администрирования.
- Главный Сервер администрирования поддерживает одновременно не более 1000 сессий.
- Виртуальные Серверы администрирования поддерживают одновременно не более 1000 сессий.

См. также

Результаты тестов производительности Сервера администрирования 115

Результаты тестов производительности Сервера администрирования

Результаты тестов производительности Сервера администрирования позволили определить максимальные количества клиентских устройств, с которыми Сервер администрирования может выполнить синхронизацию за указанные промежутки времени. Эта информация может быть использована для выбора оптимальных схем развертывания антивирусной защиты в компьютерных сетях.

Для тестирования использовались устройства со следующими аппаратными конфигурациями (см. таблицы ниже):

Таблица 15. Аппаратная конфигурация Сервера администрирования

Параметр	Значение
Процессор	Intel(R) Xeon(R) CPU E5506, тактовая частота 2,13 ГГц, 1 сокет, 8 ядер
ОЗУ	4 ГБ
Жесткий диск	IBM ServeRAID M5015 SCSI Disk Device, 928 ГБ
Операционная система	Microsoft Windows Server 2008 R2 Standard, Service Pack 1, 6.1.7601
Сеть	Broadcom BCM5709C NetXtreme II GigE (NDIS VBD Client)

Таблица 16. Аппаратная конфигурация устройства с SQL Server

Параметр	Значение
Процессор	Intel(R) Xeon(R) CPU E5630, тактовая частота 2,53 Ггц, 1 сокет, 8 ядер, 16 логических процессоров
ОЗУ	26 ГБ
Жесткий диск	IBM ServeRAID M5014 SCSI Disk Device, 929 ГБ
Операционная система	Microsoft Windows Server 2012 R2 Standard, 6.3.9600
Сеть	Broadcom BCM5709C NetXtreme II GigE (NDIS VBD Client)

Сервер администрирования поддерживал создание 500 виртуальных Серверов администрирования.

Период синхронизации составлял по 15 минут на каждые 10 000 управляемых устройств (см. таблицу ниже).

Таблица 17. Обобщенные результаты нагрузочного тестирования Сервера администрирования

Период синхронизации, мин.	Количество управляемых устройств
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

При подключении Сервера администрирования к серверу базы данных MySQL и SQL Express не рекомендуется использовать программу для управления более чем 5000 устройств.

Типовые способы развертывания системы защиты

В этом разделе описаны типовые способы развертывания системы защиты в сети организации с помощью Kaspersky Security Center.

Необходимо обеспечить защиту системы от несанкционированного доступа всех видов. Рекомендуется перед установкой программы на устройство установить все доступные обновления безопасности операционной системы.

Вы можете развернуть систему защиты в сети организации с помощью Kaspersky Security Center, используя следующие схемы развертывания:

- Развертывание системы защиты средствами Kaspersky Security Center через Консоль администрирования.

  Установка программ "Лаборатории Касперского" на клиентские устройства и подключение клиентских устройств к Серверу администрирования происходит автоматически с помощью Kaspersky Security Center.

  Основной схемой развертывания является развертывание системы защиты через Консоль администрирования.

- Развертывание системы защиты вручную с помощью автономных пакетов установки, сформированных в Kaspersky Security Center.

  Установка программ "Лаборатории Касперского" на клиентские устройства и рабочее место администратора производится вручную, параметры подключения клиентских устройств к Серверу администрирования задаются при установке Агента администрирования.

  Этот вариант развертывания рекомендуется применять в случаях, когда невозможно провести удаленную установку.

> Kaspersky Security Center также позволяет разворачивать систему защиты с помощью групповых политик Active Directory®.

Требования к безопасности Kaspersky Security Center

Для работы с Kaspersky Security Center необходимо обеспечить безопасное окружение для Сервера администрирования. Для этого выполните следующие требования:

- Исключите доступ третьих лиц к оборудованию Сервера администрирования.
- Установите все последние обновления для операционной системы Сервера администрирования. Внедрите процедуру регулярной установки последних обновлений операционной системы Сервера администрирования.
- Не используйте оборудование Сервера администрирования в качестве рабочей станции. Не рекомендуется устанавливать на оборудование Сервера администрирования программное обеспечение, отсутствующее в списке системных требований к Серверу администрирования (см. раздел "Аппаратные и программные требования" на стр. 18).
- Включите сетевой экран и установите параметры, необходимые для контроля программного обеспечения и портов. Открытыми должны быть только те порты, которые понадобятся для работы Сервера администрирования (см. раздел "Порты, используемые Kaspersky Security Center" на стр. 53).
- Установите требование на использование сложных паролей и требование на срок истечения паролей в локальных политиках безопасности Windows.
- Отключите гостевые учетные записи и все неиспользуемые учетные записи пользователей.
- Настройте ведение журнала событий и внедрите процедуру регулярного инспектирования журнала событий.

Рекомендации по установке Сервера администрирования

В этом разделе содержатся рекомендации, касающиеся установки Сервера администрирования. В разделе также содержатся сценарии использования папки общего доступа на устройстве с Сервером администрирования для развертывания Агента администрирования на клиентских устройствах.

В этом разделе

Создание учетных записей для служб Сервера администрирования на отказоустойчивом кластере

По умолчанию инсталлятор самостоятельно создает непривилегированные учетные записи для служб Сервера администрирования. Такое поведение наилучшим образом подходит для установки Сервера администрирования на обычное устройство.

Однако при установке Сервера администрирования на отказоустойчивый кластер следует поступить иначе:

1. Создать непривилегированные доменные учетные записи для служб Сервера администрирования и сделать их членами глобальной доменной группы безопасности KLAdmins.

2. Задать в инсталляторе Сервера администрирования (см. раздел "Шаг 6. Выбор учетной записи для запуска служб Kaspersky Security Center" на стр. 150) созданные доменные учетные записи для служб.

Выбор СУБД

В процессе инсталляции Сервера администрирования необходимо выбрать СУБД, которую будет использовать Сервер администрирования. При выборе СУБД, используемой Сервером администрирования, следует руководствоваться количеством устройств, которые обслуживает Сервер администрирования.

В таблице ниже перечислены допустимые варианты СУБД и ограничения их использования.

Таблица 18. Ограничения СУБД

СУБД	Ограничения
SQL Server Express Edition 2008 и выше.	Не рекомендуется, если планируется обслуживание одним Сервером администрирования более 10 000 устройств или использование компонента Контроль программ.
Локальный SQL Server Edition, отличный от Express, 2008 и выше.	Нет ограничений.
Удаленный SQL Server Edition, отличный от Express, 2008 и выше.	Допустимо только в случае, если оба устройства находятся в одном домене Windows®. Если домены разные, то между ними должно быть установлено двустороннее отношение доверия.
Локальный или удаленный MySQL 5.5, 5.6, 5.7. Не поддерживаются версии MySQL 5.5.1, 5.5.2, 5.5.3, 5.5.4, 5.5.5.	Не рекомендуется, если планируется обслуживание одним Сервером администрирования более 10 000 устройств или использование компонента Контроль программ.

Недопустимо совместное использование СУБД Server Express Edition Сервером администрирования и каким-либо другим приложением.

См. также

О выборе СУБД для Сервера администрирования 88

Учетные записи для работы ч 132

Задание папки общего доступа

Во время установки Сервера администрирования (а также и после установки, в свойствах Сервера) можно задать местоположение папки общего доступа. По умолчанию папка общего доступа создается на устройстве с Сервером администрирования (с доступом на чтение для встроенной группы **Everyone**). Однако в некоторых случаях (высокая нагрузка, необходимость доступа из изолированной сети и прочее) целесообразно располагать папку общего доступа на специализированном файловом ресурсе.

Папка общего доступа используется в нескольких сценариях развертывания Агента администрирования.

См. также

Удаленная инсталляция средствами Сервера администрирования с помощью групповых политик Active Directory 123

Удаленная инсталляция рассылкой UNC-пути на автономный пакет 123

Обновление из папки 123

Установка образов операционных систем 100

Удаленная инсталляция средствами Сервера администрирования с помощью групповых политик Active Directory

В случае если устройства находятся в домене Windows (нет рабочих групп), первоначальное развертывание (установку Агента администрирования и программы защиты на пока еще не управляемые устройства) целесообразно выполнять при помощи групповых политик Active Directory. Развертывание выполняется с помощью штатной задачи удаленной инсталляции Kaspersky Security Center. Если размер сети велик, с целью уменьшения нагрузки на дисковую подсистему устройства с Сервером администрирования, целесообразно располагать папку общего доступа на специализированном файловом ресурсе.

Удаленная инсталляция рассылкой UNC-пути на автономный пакет

В случае если пользователи устройств сети организации имеют права локального администратора, еще одним способом первоначального развертывания является создание автономного пакета Агента администрирования (или даже "спаренного" пакета Агента администрирования совместно с программой защиты). После создания автономного пакета нужно отправить пользователям устройств сети ссылку на пакет, находящийся в папке общего доступа. Инсталляция запускается по ссылке.

Обновление из папки

В задаче обновления антивируса можно настроить обновление из папки общего доступа Сервера администрирования. Если задача назначена для большого количества устройств, целесообразно располагать папку общего доступа на специализированном файловом ресурсе.

Установка образов операционных систем

Установка образов операционных систем всегда выполняется с использованием папки общего доступа: устройства читают из папки образы операционных систем. Если

планируется развертывание образов на большом количестве устройств организации, то целесообразно располагать папку общего доступа на специализированном файловом ресурсе.

См. также

Развертывание Агента администрирования и программы защиты 222

Указание адреса Сервера администрирования

При установке Сервера администрирования можно задать адрес Сервера администрирования. Этот адрес по умолчанию используется при создании инсталляционных пакетов Агента администрирования. По умолчанию используется NetBIOS-имя устройства с Сервером администрирования. Если в сети организации настроена и правильно работает DNS, то следует здесь задать FQDN-имя устройства с Сервером администрирования. Если Сервер администрирования установлен в демилитаризованной зоне, то может быть целесообразным указать внешний адрес Сервера администрирования. В дальнейшем адрес Сервера администрирования можно будет изменить средствами Консоли администрирования, однако при этом он не изменится автоматически в уже созданных инсталляционных пакетах Агента администрирования.

См. также

Доступ из интернета: Сервер администрирования в демилитаризованной зоне 94

Задание сертификата Сервера администрирования

В случае необходимости можно задать Серверу администрирования специальный сертификат при помощи утилиты командной строки klsetsrvcert.

При замене сертификата все Агенты администрирования, ранее подключенные к Серверу администрирования по SSL, перестанут подключаться к Серверу с ошибкой "Ошибка аутентификации Сервера администрирования".

Следует учитывать, что сертификат Сервера администрирования часто помещают в пакеты Агента администрирования при их создании. В этом случае замена сертификата Сервера при помощи утилиты klsetsrvcert не приведет к замене сертификата Сервера администрирования в уже существующих пакетах Агента администрирования.

Целесообразно заменять сертификат сразу после инсталляции Сервера администрирования, до завершения мастера первоначальной настройки.

Подробную информацию об условиях, при которых необходима замена сертификата, смотрите в разделе Планирование развертывания Kaspersky Security Center (на стр. 83).

Для замены сертификата следует создать новый сертификат (например, средствами инфраструктуры открытых ключей организации) в формате PKCS#12 и передать его на вход утилиты klsetsrvcert (значения параметров утилиты см. в таблице ниже).

Синтаксис утилиты:

klsetsrvcert [-l LOGFILE] -t TYPE [-p PASSWORD] -i FILE

Таблица 19. Значения параметров утилиты klsetsrvcert

Параметр	Значение
-t TYPE	Тип сертификата, который следует заменить. Возможные значения параметра TYPE: • C – заменить сертификат для портов 13000 и 13291; • CR – заменить резервный сертификат для портов 13000 и 13291; • M – заменить сертификат для мобильных устройств порта 13292.
-i FILE	Контейнер с сертификатом в формате PKCS#12 (файл с расширением .p12 или .pfx).
-p PASSWORD	Пароль, при помощи которого защищен p12-контейнер с сертификатом.
-l LOGFILE	Файл вывода результатов. По умолчанию вывод осуществляется в стандартный поток вывода.

Этапы развертывания Сервера администрирования

В этом разделе описаны этапы развертывания Сервера администрирования.

Этапы развертывания описаны для двух вариантов работы с программой:

- развертывание Сервера администрирования внутри организации;
- развертывание Сервера администрирования для защиты сети организации-клиента.

> Если вам требуется развернуть Сервер администрирования внутри организации, которая включает в себя удаленные офисы, не входящие в сеть организации, вы можете следовать порядку развертывания системы защиты для сервис-провайдеров.

Kaspersky Security Center предоставляет возможность интеграции в платформу Microsoft Network Access Protection (NAP), которая позволяет регулировать доступ клиентских

устройств в сеть. Для того чтобы обеспечить проверку работоспособности операционной системы при совместной работе программы Kaspersky Security Center с Microsoft NAP, необходимо дополнительно установить компонент System Health Validator (см. раздел "Установка и настройка Kaspersky Security Center SHV" на стр. 175).

Далее в разделе описаны действия, входящие в перечисленные этапы развертывания защиты.

В этом разделе

Этапы развертывания Сервера администрирования внутри организации

► *Чтобы развернуть Сервер администрирования внутри организации, выполните следующие действия:*

1. Установите Kaspersky Security Center на рабочее место администратора.

2. Настройте параметры Сервера администрирования.

Этапы развертывания Сервера администрирования для защиты сети организации-клиента

Чтобы развернуть Сервер администрирования для защиты сети организации-клиента, установите Kaspersky Security Center на рабочее место администратора.

Обновление предыдущей версии Kaspersky Security Center

Вы можете установить Сервер администрирования версии 10 Service Pack 3 на устройство, на котором установлена предыдущая версия Сервера администрирования (начиная с версии 10 Service Pack 1). При обновлении до версии 10 Service Pack 3 данные и параметры предыдущей версии Сервера администрирования сохраняются.

► *Чтобы обновить Сервер администрирования предыдущей версии до версии 10 Service Pack 3, выполните следующие действия:*

1. Запустите исполняемый файл setup.exe для версии 10 Service Pack 3.

   Откроется окно с выбором программ "Лаборатории Касперского" для установки.

   В окне с выбором программ по ссылке **Установить Сервер администрирования Kaspersky Security Center 10** запустите мастер установки Сервера администрирования. Следуйте указаниям мастера.

   Внимательно прочитайте Лицензионное соглашение, которое заключается между вами и "Лабораторией Касперского", и Политику конфиденциальности. Если вы согласны со всеми пунктами Лицензионного соглашения и Политики конфиденциальности, в блоке **Я подтверждаю, что полностью прочитал, понимаю и принимаю** установите флажки:

   - **положения и условия настоящего Лицензионного соглашения**;
   - **Политику конфиденциальности, которая описывает обработку данных**.

   Установка программы будет продолжена после установки обоих флажков. Мастер установки предложит вам создать резервную копию данных Сервера администрирования для Kaspersky Security Center версии 10 Service Pack 1 и ниже.

   Kaspersky Security Center поддерживает восстановление данных из резервной копии данных Сервера администрирования, сформированной более ранней версией программы.

2. Если требуется создать резервную копию, в открывшемся окне **Создание резервной копии Сервера администрирования** установите флажок **Создать резервную копию Сервера администрирования**.

Резервная копия данных Сервера администрирования создается при помощи утилиты klbackup. Эта утилита входит в состав дистрибутива программы и располагается в корне папки установки Kaspersky Security Center.

3. Установите Сервер администрирования версии 10 Service Pack 3, следуя указаниям мастера установки.

   Не рекомендуется прерывать работу мастера установки. Прерывание процесса обновления на стадии установки Сервера администрирования может привести к неработоспособности обновляемой версии.

4. Для устройств, на которых был установлен Агент администрирования предыдущей версии, создайте и запустите задачу удаленной установки новой версии Агента администрирования (см. раздел "Установка программ с помощью задачи удаленной установки" на стр. 268).

   После выполнения задачи удаленной установки версия Агента администрирования будет обновлена.

Если при установке Сервера администрирования возникли проблемы, вы можете восстановить предыдущую версию Сервера администрирования, используя созданную перед обновлением резервную копию данных Сервера.

Если в сети установлен хотя бы один Сервер администрирования новой версии, обновление других Серверов администрирования в сети можно проводить с помощью задачи удаленной установки, в которой используется инсталляционный пакет Сервера администрирования.

Установка и удаление Kaspersky Security Center

В этом разделе описывается локальная установка компонентов Kaspersky Security Center. Доступны два типа установки:

- **Стандартная**. В этом случае будет установлен минимальный набор необходимых компонентов программы.

- **Выборочная**. В этом случае вы сможете выбрать отдельные компоненты для установки и настроить дополнительные параметры программы. Выборочную установку рекомендуется проводить опытным пользователям.

Если в сети установлен хотя бы один Сервер администрирования, Серверы на других устройствах сети могут быть установлены с помощью задачи удаленной установки методом форсированной установки (см. раздел "Установка программ с помощью задачи удаленной установки" на стр. 268). При формировании задачи удаленной установки следует использовать инсталляционный пакет Сервера администрирования.

Вы можете использовать один из двух типов установочных пакетов:

- ksc_10sp3_10.5.<номер сборки>_full_<язык локализации>.exe. Содержит полный набор компонентов для установки. Используйте этот пакет, если вы хотите установить все компоненты, необходимые для полной функциональности Kaspersky Security Center, или обновить существующие версии этих компонентов.

- ksc_10sp3_10.5.<номер сборки>_lite_<язык локализации>.exe. Содержит минимальный набор компонентов, необходимый для работы Kaspersky Security Center. Например, этот пакет не содержит плагинов управления программой Kaspersky Endpoint Security 10 для Windows.

  Используйте этот пакет установки, если:

  - вы хотите обновить Сервер администрирования с предыдущей версии;

  - у вас уже установлены компоненты, необходимые для полной функциональности Kaspersky Security Center, и вы хотите продолжить пользоваться существующими версиями этих компонентов;

  - вы хотите использовать Kaspersky Security Center с ограниченной функциональностью;

  - вы собираетесь использовать Kaspersky Security Center в организациях, где ограничен интернет-трафик и дистрибутивы загружаются отдельно.

В этом разделе

Подготовка к установке

Перед началом установки нужно убедиться, что аппаратное и программное обеспечение устройства соответствует требованиям, предъявляемым к Серверу администрирования и Консоли администрирования.

Kaspersky Security Center хранит информацию в базе данных SQL-сервера. Для этого необходимо самостоятельно установить базу данных SQL-сервера (подробнее о выборе СУБД (см. раздел "О выборе СУБД для Сервера администрирования" на стр. 88)). Для хранения информации можно использовать и другие SQL-серверы. Они должны быть установлены в сети до начала установки Kaspersky Security Center. Для установки Kaspersky Security Center необходимо наличие прав локального администратора на устройстве, где осуществляется установка.

Вместе с компонентом Сервер администрирования на устройство будет установлена серверная версия Агента администрирования. Его совместная установка с обычной версией Агента администрирования невозможна. Если серверная версия Агента администрирования уже установлена на вашем устройстве, требуется удалить ее и запустить установку Сервера администрирования повторно.

Учетные записи для работы ч

В таблицах ниже приведена информация о том, как влияет выбор системы управления базами данных (СУБД) на свойства учетных записей для работы с СУБД.

Локальной СУБД называется СУБД, установленная на том же устройстве, что и Сервер администрирования. Удаленной СУБД называется СУБД, установленная на другом устройстве.

Задавайте все права, необходимые для учетной записи Сервера администрирования, до запуска службы Сервера администрирования.

SQL Server

Таблица 20. СУБД: SQL Server (в том числе и Express Edition) с аутентификацией SQL Server

Расположение СУБД	Локальная	Удаленная
Кто создает базу данных KAV	Администратор вручную или инсталлятор	Администратор вручную или инсталлятор
Учетная запись, от имени которой работает инсталлятор	Локальная	Доменная
Права учетной записи, от имени которой работает инсталлятор	• Системные: права локального администратора. • SQL Server: учетной записи инсталлятора не требуется доступ к SQL Server.	• Системные: права локального администратора. • SQL Server: учетной записи инсталлятора не требуется доступ к SQL Server.
Учетная запись службы Сервера администрирования	Локальная или доменная	Доменная
Права учетной записи службы Сервера администрирования	• Системные: необходимые права присвоит инсталлятор. • SQL Server: учетной записи службы Сервера администрирования не требуется доступ к SQL Server.	• Системные: необходимые права присвоит инсталлятор. • SQL Server: учетной записи службы Сервера администрирования не требуется доступ к SQL Server.
Дополнительно	Администратор явным образом задает в инсталляторе внутреннюю учетную запись SQL Server, которая требует наличия роли sysadmin	Администратор явным образом задает в инсталляторе внутреннюю учетную запись SQL Server, которая требует наличия роли sysadmin

Таблица 21. СУБД: SQL Server (в том числе и Express Edition) с аутентификацией Windows

Расположение СУБД	Локальная	Локальная	Удаленная	Удаленная
Кто создает базу данных KAV	Инсталлятор	Администратор вручную	Инсталлятор	Администратор вручную
Учетная запись, от имени которой работает инсталлятор	Локальная или доменная	Локальная или доменная	Доменная	Доменная
Права учетной записи, от имени которой работает инсталлятор	• Системные: права локального администратора. • SQL Server: роль sysadmin.	• Системные: права локального администратора. • SQL Server: для базы данных KAV схема dbo, роли db_datareader и db_datawriter для каждой из баз данных KAV, master и tempdb.	• Системные: права локального администратора. • SQL Server: роль sysadmin.	• Системные: права локального администратора. • SQL Server: для базы данных KAV схема dbo, роли db_datareader и db_datawriter для каждой из баз данных KAV, master и tempdb.

Учетная запись Сервера администрирования	• Автоматически созданная вида KL-AK-*. • Выбранная администратором локальная. • Выбранная администратором доменная.	• Автоматически созданная вида KL-AK-*. • Выбранная администратором локальная. • Выбранная администратором доменная.	Доменная	Доменная
Права учетной записи службы Сервера администрирования	• Системные: необходимые права присвоит инсталлятор. • SQL Server: необходимые права присвоит инсталлятор.	• Системные: необходимые права присвоит инсталлятор. • SQL Server: администратор должен присвоить учетной записи роль db_owner для базы данных KAV и роли db_datareader и db_datawriter для каждой из баз данных master и tempdb.	• Системные: необходимые права присвоит инсталлятор. • SQL Server: необходимые права присвоит инсталлятор.	• Системные: необходимые права присвоит инсталлятор. • SQL Server: администратор должен присвоить учетной записи роль db_owner для БД KAV, роли db_datareader и db_datawriter для каждой из баз данных master и tempdb.

Таблица 22.

MySQL

Таблица 23. СУБД: MySQL

Расположение СУБД	Локальная или удаленная	Локальная или удаленная
Кто создает базу данных KAV	Инсталлятор	Администратор вручную
Учетная запись, от имени которой работает инсталлятор	Локальная или доменная	Локальная или доменная
Права учетной записи, от имени которой работает инсталлятор	• Системные: права локального администратора. • MySQL Server: учетной записи инсталлятора не требуется доступ к MySQL.	• Системные: права локального администратора. • MySQL Server: учетной записи инсталлятора не требуется доступ к MySQL.
Учетная запись службы Сервера администрирования	Локальная или доменная	Локальная или доменная
Права учетной записи службы Сервера администрирования	• Системные: необходимые права присвоит инсталлятор. • MySQL Server: учетной записи службы Сервера администрирования не требуется доступ к MySQL.	• Системные: необходимые права присвоит инсталлятор. • MySQL Server: учетной записи службы Сервера администрирования не требуется доступ к MySQL.
Дополнительно	Администратор явным образом задает в инсталляторе внутреннюю учетную запись SQL Server, которая требует доступа root	Администратор явным образом задает в инсталляторе внутреннюю учетную запись SQL Server, которая требует GRANT ALL для базы данных KAV

Стандартная установка

Стандартная установка – это установка Сервера администрирования, при которой используются заданные по умолчанию пути для файлов программы, устанавливается набор плагинов по умолчанию и не включается поддержка мобильных устройств.

► *Чтобы установить Сервер администрирования Kaspersky Security Center на локальное устройство,*

запустите исполняемый файл ksc_10sp3_10.5.<номер сборки>_full_<язык локализации>.exe.

Откроется окно с выбором программ "Лаборатории Касперского" для установки. В окне с выбором программ по ссылке **Установить Сервер администрирования Kaspersky Security Center 10** запустите мастер установки Сервера администрирования. Следуйте указаниям мастера.

Далее описаны шаги мастера установки программы, а также действия, которые вы можете выполнить на каждом из этих шагов.

В этом разделе

Шаг 1. Просмотр Лицензионного соглашения и Политики конфиденциальности

На этом шаге мастера установки требуется ознакомиться с Лицензионным соглашением, которое заключается между вами и "Лабораторией Касперского" и Политикой конфиденциальности.

Вам также может быть предложено ознакомиться с Лицензионными соглашениями и Политиками конфиденциальности на доступные в дистрибутиве Kaspersky Security Center плагины управления программами.

Внимательно прочитайте Лицензионное соглашение и Политику конфиденциальности. Если вы согласны со всеми пунктами Лицензионного соглашения и Политики конфиденциальности, в блоке **Я подтверждаю, что полностью прочитал, понимаю и принимаю** установите флажки:

- **положения и условия настоящего Лицензионного соглашения**;
- **Политику конфиденциальности, которая описывает обработку данных**.

Установка программы на ваше устройство будет продолжена после установки обоих флажков.

Если вы не согласны с Лицензионным соглашением или Политикой конфиденциальности, то отмените установку программы, нажав на кнопку **Отмена**.

Шаг 2. Выбор типа установки

В окне выбора типа установки укажите тип **Стандартная**.

Стандартная установка рекомендуется, если вы хотите ознакомиться с программой Kaspersky Security Center, например, протестировать ее работу на небольшом участке сети вашей организации. При стандартной установке вы настраиваете только параметры базы данных. Параметры Сервера администрирования не настраиваются, для них используются заданные по умолчанию значения. Стандартная установка не позволяет выбрать устанавливаемые плагины управления, устанавливается заданный по умолчанию набор плагинов. При стандартной установке не создаются инсталляционные пакеты для мобильных устройств, однако вы можете создать их позднее в Консоли администрирования.

Шаг 3. Выбор размера сети

Укажите размер сети, в которой устанавливается Kaspersky Security Center. В зависимости от количества устройств в сети мастер настраивает параметры установки и отображение интерфейса программы.

В таблице ниже перечислены параметры установки программы и отображения интерфейса при выборе разных размеров сети.

Таблица 24. Зависимость параметров установки от выбора размеров сети

Параметры	1–100 устройств	100–1000 устройств	1000–5000 устройств	Более 5000 устройств
Отображение в дереве консоли узла подчиненных и виртуальных Серверов администрирования и всех параметров, связанных с подчиненными и виртуальными Серверами	отсутствует	отсутствует	присутствует	присутствует
Отображение разделов **Безопасность** в окнах свойств Сервера и групп администрирования	отсутствует	отсутствует	присутствует	присутствует
Распределение времени запуска задачи обновления на клиентских устройствах случайным образом	отсутствует	в интервале 5 минут	в интервале 10 минут	в интервале 10 минут

При подключении Сервера администрирования к серверу базы данных MySQL и SQL Express не рекомендуется использовать программу для управления более чем 5000 устройств.

Шаг 4. Выбор базы данных

На этом шаге мастера установки требуется выбрать ресурс Microsoft SQL Server (SQL Express) или MySQL, который будет использоваться для размещения информационной базы данных Сервера администрирования.

> Если вы устанавливаете Kaspersky Security Center на сервер, выполняющий роль контроллера домена только для чтения (RODC), для него не предусмотрена возможность установки Microsoft SQL Server (SQL Express). В этом случае для правильной установки Kaspersky Security Center рекомендуется использовать ресурс MySQL.

Структура базы данных Сервера администрирования описана в файле klakdb.chm, который расположен в папке установки программы Kaspersky Security Center (этот файл в виде архива доступен на портале "Лаборатории Касперского": klakdb.zip (http://media.kaspersky.com/utilities/CorporateUtilities/klakdb.zip)).

См. также

Выбор СУБД 121

Шаг 5. Настройка параметров SQL-сервера

На этом шаге мастера установки выполняется настройка параметров SQL-сервера.

В зависимости от выбранной базы данных возможны следующие варианты настройки параметров SQL-сервера:

- Если на предыдущем этапе вы выбрали вариант **Microsoft SQL Server (SQL Express)**, укажите следующие параметры:
  - В поле **Имя SQL-сервера** укажите имя SQL-сервера, установленного в сети. При помощи кнопки **Обзор** вы можете открыть список всех SQL-серверов, установленных в сети. По умолчанию поле не заполнено.

Если Сервер администрирования запускается под учетной записью локального администратора или под учетной записью системы, кнопка **Обзор** недоступна.

Если в сети организации установлен SQL-сервер с настроенной поддержкой AlwaysON, в поле **Имя SQL-сервера** укажите имя прослушивателя группы доступности.

- В поле **Имя базы данных** задайте имя базы данных, которая была создана для размещения информации Сервера администрирования. По умолчанию указано значение *KAV*.

- Если на предыдущем этапе был выбран вариант **MySQL**, укажите следующие параметры:

  - В поле **Имя SQL-сервера** укажите имя установленного SQL-сервера. По умолчанию используется IP-адрес устройства, на который устанавливается Kaspersky Security Center.

  - В поле **Порт** укажите порт для подключения Сервера администрирования к базе данных SQL-сервера. По умолчанию используется порт 3306.

  - В поле **Имя базы данных** задайте имя базы данных, которая была создана для размещения информации Сервера администрирования. По умолчанию указано значение *KAV*.

Если на этом шаге вы хотите установить SQL-сервер на то устройство, с которого производите установку Kaspersky Security Center, нужно прервать установку и запустить ее снова после установки SQL-сервера. Поддерживаемые SQL-серверы перечислены в требованиях к системе.

Если вы хотите установить SQL-сервер на удаленное устройство, прерывать работу мастера установки Kaspersky Security Center не требуется. Установите SQL-сервер и вернитесь к установке Kaspersky Security Center.

Шаг 6. Выбор режима аутентификации

Определите режим аутентификации, который будет использоваться при подключении Сервера администрирования к SQL-серверу.

В зависимости от выбранной базы данных вы можете выбрать следующие режимы аутентификации:

- Для SQL Express или Microsoft SQL Server выберите один из следующих вариантов:
  - **Режим аутентификации Microsoft Windows**. В этом случае при проверке прав будет использоваться учетная запись для запуска Сервера администрирования.
  - **Режим аутентификации SQL-сервера**. В случае выбора этого варианта для проверки прав будет использоваться указанная в окне учетная запись. Заполните поля **Учетная запись** и **Пароль**.

    После того как как вы начали вводить пароль, отображается кнопка **Показать пароль**. Чтобы посмотреть введенный пароль, нажмите на кнопку **Показать пароль** и удерживайте ее необходимое вам время.

  Если база данных Сервера администрирования находится на другом устройстве и учетная запись Сервера администрирования не имеет доступа к серверу базы данных, то при установке или обновлении Сервера администрирования следует использовать режим аутентификации SQL-сервера. Это может происходить в случае, когда устройство с базой данных находится не в домене, или Сервер администрирования установлен под учетной записью Локальная система.

- Для сервера MySQL укажите учетную запись и пароль.

Шаг 7. Распаковка и установка файлов на жесткий диск

По окончании настройки параметров установки компонентов Kaspersky Security Center вы можете запустить установку файлов на жесткий диск.

Если для запуска установки требуются дополнительные программы, мастер установки сообщит об этом перед началом установки Kaspersky Security Center в окне **Установка обязательных компонентов**. Необходимые программы будут установлены автоматически после нажатия на кнопку **Далее**.

В последнем окне мастера установки вам будет предложено запустить Консоль администрирования. При первом запуске Консоли вы можете выполнить первоначальную настройку программы (см. стр. 176).

По окончании работы мастера установки следующие компоненты программы будут установлены на жесткий диск, на котором установлена операционная система:

- Сервер администрирования (совместно с серверной версией Агента администрирования);
- Консоль администрирования;
- доступные в дистрибутиве плагины управления программами.

Кроме того, будет установлена программа Microsoft Windows Installer версии 4.5, если эта программа не была установлена ранее.

Выборочная установка

Выборочная установка – это установка Сервера администрирования, при которой вам предлагается выбрать компоненты для установки и указать папку, в которую будет установлена программа.

С помощью этого типа установки вы можете настроить параметры базы данных, параметры Сервера администрирования, установить компоненты, которые не включены в стандартную установку и плагины управления защитными программами "Лаборатории Касперского". Вы можете также включить поддержку мобильных устройств.

► *Чтобы установить Сервер администрирования Kaspersky Security Center на локальное устройство,*

запустите исполняемый файл ksc_10sp3_10.5.<номер сборки>_full_<язык локализации>.exe.

Откроется окно с выбором программ "Лаборатории Касперского" для установки. В окне с выбором программ по ссылке **Установить Сервер администрирования Kaspersky Security Center 10** запустите мастер установки Сервера администрирования. Следуйте указаниям мастера.

Далее описаны шаги мастера установки программы, а также действия, которые вы можете выполнить на каждом из этих шагов.

В этом разделе

Шаг 1. Просмотр Лицензионного соглашения и Политики конфиденциальности

На этом шаге мастера установки требуется ознакомиться с Лицензионным соглашением, которое заключается между вами и "Лабораторией Касперского" и Политикой конфиденциальности.

Вам также может быть предложено ознакомиться с Лицензионными соглашениями и Политиками конфиденциальности на доступные в дистрибутиве Kaspersky Security Center плагины управления программами.

Внимательно прочитайте Лицензионное соглашение и Политику конфиденциальности. Если вы согласны со всеми пунктами Лицензионного соглашения и Политики конфиденциальности, в блоке **Я подтверждаю, что полностью прочитал, понимаю и принимаю** установите флажки:

- **положения и условия настоящего Лицензионного соглашения**;
- **Политику конфиденциальности, которая описывает обработку данных**.

Установка программы на ваше устройство будет продолжена после установки обоих флажков.

Если вы не согласны с Лицензионным соглашением или Политикой конфиденциальности, то отмените установку программы, нажав на кнопку **Отмена**.

Шаг 2. Выбор типа установки

В окне выбора типа установки укажите тип **Выборочная**.

Выборочная установка позволяет настроить параметры Kaspersky Security Center, такие как путь к папке общего доступа, учетные записи и порты подключения к Серверу администрирования, и параметры базы данных. Выборочная установка позволяет указать, какие плагины управления программами "Лаборатории Касперского" будут установлены. При выборочной установке вы можете создать инсталляционные пакеты для мобильных устройств, указав соответствующую опцию.

Шаг 3. Выбор компонентов для установки

Выберите компоненты Сервера администрирования Kaspersky Security Center, которые вы хотите установить:

- **Поддержка мобильных устройств**. Установите этот флажок, если требуется создать инсталляционные пакеты для мобильных устройств во время работы мастера установки Kaspersky Security Center. Вы можете также создать инсталляционные пакеты для мобильных устройств вручную, после установки Сервера администрирования средствами Консоли администрирования.
- **Агент SNMP**. Получает статистическую информацию для Сервера администрирования по протоколу SNMP. Компонент доступен при установке программы на устройство с установленным компонентом SNMP.

  > После установки Kaspersky Security Center необходимые для получения статистической информации mib-файлы будут расположены в папке установки программы во вложенной папке SNMP.

Компоненты Агент администрирования и Консоль администрирования не отображаются в списке компонентов. Эти компоненты устанавливаются автоматически, их установку отменить нельзя.

На этом шаге мастера также следует указать папку для установки компонентов Сервера администрирования. По умолчанию компоненты устанавливаются в папку <Диск>:\Program Files\Kaspersky Lab\Kaspersky Security Center. Если папки с таким названием нет, она будет создана автоматически в процессе установки. Вы можете сменить папку назначения с помощью кнопки **Обзор**.

Шаг 4. Выбор размера сети

Укажите размер сети, в которой устанавливается Kaspersky Security Center. В зависимости от количества устройств в сети мастер настраивает параметры установки и отображение интерфейса программы.

В таблице ниже перечислены параметры установки программы и отображения интерфейса при выборе разных размеров сети.

Таблица 25. Зависимость параметров установки от выбора размеров сети

Параметры	1–100 устройств	100–1000 устройств	1000–5000 устройств	Более 5000 устройств
Отображение в дереве консоли узла подчиненных и виртуальных Серверов администрирования и всех параметров, связанных с подчиненными и виртуальными Серверами	отсутствует	отсутствует	присутствует	присутствует
Отображение разделов **Безопасность** в окнах свойств Сервера и групп администрирования	отсутствует	отсутствует	присутствует	присутствует
Распределение времени запуска задачи обновления на клиентских устройствах случайным образом	отсутствует	в интервале 5 минут	в интервале 10 минут	в интервале 10 минут

При подключении Сервера администрирования к серверу базы данных MySQL и SQL Express не рекомендуется использовать программу для управления более чем 5000 устройств.

Шаг 5. Выбор учетной записи для запуска Сервера администрирования

Выберите учетную запись, под которой Сервер администрирования будет запускаться как служба.

- **Создать учетную запись автоматически**. Программа создает локальную учетную запись KL-AK-*, под которой будет запускаться служба Сервера администрирования kladminserver.

  Вы можете выбрать этот вариант, если вы планируете разместить папку общего доступа (см. раздел "Шаг 10. Определение папки общего доступа" на стр. 154) и СУБД (см. раздел "Шаг 7. Выбор базы данных" на стр. 151) на том же устройстве, что и Сервер администрирования.

- **Выбрать учетную запись**. Служба Сервера администрирования (kladminserver) будет запускаться под выбранной вами учетной записью.

  Вам потребуется выбрать доменную учетную запись, например, если вы планируете использовать в качестве СУБД SQL-сервер любого выпуска, в том числе SQL-express (см. раздел "Шаг 7. Выбор базы данных" на стр. 151), расположенный на другом устройстве, и / или если вы планируете разместить папку общего доступа (см. раздел "Шаг 10. Определение папки общего доступа" на стр. 154) на другом устройстве.

  Kaspersky Security Center начиная с версии 10 Service Pack 3 поддерживает управляемые учетные записи службы и групповые управляемые учетные записи службы. Если такие учетные записи используются в вашем домене, вы можете выбрать одну из них в качестве учетной записи для службы Сервера администрирования:

  1. Нажмите на кнопку **Обзор**.
  2. В появившемся окне нажмите на кнопку **Object types**.
  3. Выберите тип **Service Accounts** и нажмите на кнопку **OK**.
  4. Выберите нужную учетную запись и нажмите на кнопку **OK**.

Выбранная вами учетная запись должна обладать различными правами в зависимости от того, какую СУБД вы планируете использовать (см. раздел "Учетные записи для работы ч" на стр. 132).

Из соображений безопасности не делайте учетную запись, под которой запускается Сервер администрирования, привилегированной.

Если в дальнейшем вы захотите изменить учетную запись Сервера администрирования, вы можете воспользоваться утилитой смены учетной записи Сервера администрирования (klsrvswch).

См. также

Учетные записи для работы ч 132

Изменения в системе после установки Сервера администрирования на устройство 168

Шаг 6. Выбор учетной записи для запуска служб Kaspersky Security Center

Выберите учетную запись, под которой будут запускаться службы Kaspersky Security Center на этом устройстве:

- **Создать учетную запись автоматически**. Kaspersky Security Center создает локальную учетную запись KlScSvc на этом устройстве в группе kladmins. Службы Kaspersky Security Center будут запускаться под созданной учетной записью.
- **Выбрать учетную запись**. Службы Kaspersky Security Center будут запускаться под выбранной вами учетной записью.

  Вам потребуется выбрать доменную учетную запись, например, если вы планируете сохранять отчеты в папке, расположенной на другом устройстве, или же если этого требует политика безопасности в вашей организации. Также вам может потребоваться выбрать доменную учетную запись при установке Сервера администрирования на отказоустойчивый кластер (см. раздел "Создание учетных

записей для служб Сервера администрирования на отказоустойчивом кластере" на стр. 120).

Из соображений безопасности не делайте учетную запись, под которой запускаются службы, привилегированной.

Под выбранной учетной записью будут запускаться службы прокси-сервера KSN (ksnproxy), прокси-сервера активации "Лаборатории Касперского" (klactprx) и портала авторизации "Лаборатории Касперского" (klwebsrv).

См. также

Изменения в системе после установки Сервера администрирования на устройство 168

Шаг 7. Выбор базы данных

На этом шаге мастера установки требуется выбрать ресурс Microsoft SQL Server (SQL Express) или MySQL, который будет использоваться для размещения информационной базы данных Сервера администрирования.

Если вы устанавливаете Kaspersky Security Center на сервер, выполняющий роль контроллера домена только для чтения (RODC), для него не предусмотрена возможность установки Microsoft SQL Server (SQL Express). В этом случае для правильной установки Kaspersky Security Center рекомендуется использовать ресурс MySQL.

Структура базы данных Сервера администрирования описана в файле klakdb.chm, который расположен в папке установки программы Kaspersky Security Center (этот файл в виде архива доступен на портале "Лаборатории Касперского": klakdb.zip (http://media.kaspersky.com/utilities/CorporateUtilities/klakdb.zip)).

Шаг 8. Настройка параметров SQL-сервера

На этом шаге мастера установки выполняется настройка параметров SQL-сервера.

В зависимости от выбранной базы данных возможны следующие варианты настройки параметров SQL-сервера:

- Если на предыдущем этапе вы выбрали вариант **Microsoft SQL Server (SQL Express)**, укажите следующие параметры:
  - В поле **Имя SQL-сервера** укажите имя SQL-сервера, установленного в сети. При помощи кнопки **Обзор** вы можете открыть список всех SQL-серверов, установленных в сети. По умолчанию поле не заполнено.

    > Если Сервер администрирования запускается под учетной записью локального администратора или под учетной записью системы, кнопка **Обзор** недоступна.

    > Если в сети организации установлен SQL-сервер с настроенной поддержкой AlwaysON, в поле **Имя SQL-сервера** укажите имя прослушивателя группы доступности.

  - В поле **Имя базы данных** задайте имя базы данных, которая была создана для размещения информации Сервера администрирования. По умолчанию указано значение *KAV*.

- Если на предыдущем этапе был выбран вариант **MySQL**, укажите следующие параметры:
  - В поле **Имя SQL-сервера** укажите имя установленного SQL-сервера. По умолчанию используется IP-адрес устройства, на который устанавливается Kaspersky Security Center.
  - В поле **Порт** укажите порт для подключения Сервера администрирования к базе данных SQL-сервера. По умолчанию используется порт 3306.

- В поле **Имя базы данных** задайте имя базы данных, которая была создана для размещения информации Сервера администрирования. По умолчанию указано значение *KAV*.

Если на этом шаге вы хотите установить SQL-сервер на то устройство, с которого производите установку Kaspersky Security Center, нужно прервать установку и запустить ее снова после установки SQL-сервера. Поддерживаемые SQL-серверы перечислены в требованиях к системе.

Если вы хотите установить SQL-сервер на удаленное устройство, прерывать работу мастера установки Kaspersky Security Center не требуется. Установите SQL-сервер и вернитесь к установке Kaspersky Security Center.

Шаг 9. Выбор режима аутентификации

Определите режим аутентификации, который будет использоваться при подключении Сервера администрирования к SQL-серверу.

В зависимости от выбранной базы данных вы можете выбрать следующие режимы аутентификации:

- Для SQL Express или Microsoft SQL Server выберите один из следующих вариантов:
  - **Режим аутентификации Microsoft Windows**. В этом случае при проверке прав будет использоваться учетная запись для запуска Сервера администрирования.
  - **Режим аутентификации SQL-сервера**. В случае выбора этого варианта для проверки прав будет использоваться указанная в окне учетная запись. Заполните поля **Учетная запись** и **Пароль**.

    После того как как вы начали вводить пароль, отображается кнопка **Показать пароль**. Чтобы посмотреть введенный пароль, нажмите на кнопку **Показать пароль** и удерживайте ее необходимое вам время.

Если база данных Сервера администрирования находится на другом устройстве и учетная запись Сервера администрирования не имеет доступа к серверу базы данных, то при установке или обновлении Сервера администрирования следует использовать режим аутентификации SQL-сервера. Это может происходить в случае, когда устройство с базой данных находится не в домене, или Сервер администрирования установлен под учетной записью Локальная система.

- Для сервера MySQL укажите учетную запись и пароль.

Шаг 10. Определение папки общего доступа

Определите место размещения и название папки общего доступа, которая будет использоваться для следующих целей:

- хранения файлов, необходимых для удаленной установки программ (файлы копируются на Сервер администрирования при создании инсталляционных пакетов);
- размещения обновлений, копируемых с источника обновлений на Сервер администрирования.

К этому ресурсу будет открыт общий доступ на чтение для всех пользователей.

Вы можете выбрать один из двух вариантов:

- **Создать папку общего доступа**. Создание новой папки. Укажите путь к папке в расположенном ниже поле.
- **Выбрать существующую папку общего доступа**. Выбор папки общего доступа из числа уже существующих.

Папка общего доступа может размещаться как локально на устройстве, с которого производится установка, так и удаленно, на любом из клиентских устройств, входящих в состав сети организации. Вы можете указать папку общего доступа с помощью кнопки **Обзор** или вручную, введя в соответствующем поле UNC-путь (например, \\server\Share).

По умолчанию создается локальная папка Share в папке, заданной для установки программных компонентов Kaspersky Security Center.

Шаг 11. Настройка параметров подключения к Серверу администрирования

Настройте параметры подключения к Серверу администрирования:

- **Номер порта**

  Номер порта, по которому выполняется подключение к Серверу администрирования.

  По умолчанию используется порт 14000.

- **Номер SSL-порта**

  Номер SSL-порта, по которому осуществляется защищенное подключение к Серверу администрирования с использованием протокола SSL.

  По умолчанию используется порт 13000.

- **Длина ключа шифрования**

Выберите длину ключа шифрования 1024 бита или 2048 бит.

Ключ шифрования длиной 1024 бита оказывает меньшую нагрузку на процессор, но считается устаревшим и по техническим характеристикам может не обеспечивать надежное шифрование. Также есть вероятность, что имеющееся оборудование несовместимо с SSL-сертификатами с длиной ключа 1024 бита.

Ключ шифрования длиной 2048 бит отвечает современным стандартам шифрования. Однако использование 2048-битного ключа шифрования может привести к дополнительной нагрузке на процессор.

По умолчанию вариант выбран вариант **2048 бит (большая безопасность)**.

Если Сервер администрирования работает под управлением Microsoft Windows XP с Service Pack 2, то встроенный сетевой экран блокирует TCP-порты с номерами 13000 и 14000. Поэтому для обеспечения доступа на устройстве, на котором установлен Сервер администрирования, эти порты нужно открыть вручную.

Шаг 12. Задание адреса Сервера администрирования

Задайте адрес Сервера администрирования. Вы можете выбрать один из следующих вариантов:

- **Имя DNS-домена**. Этот вариант используется в том случае, когда в сети присутствует DNS-сервер, и клиентские устройства могут получить с его помощью адрес Сервера администрирования.
- **NetBIOS-имя**. Этот вариант используется, если клиентские устройства получают адрес Сервера администрирования с помощью протокола NetBIOS, или в сети присутствует WINS-сервер.
- **IP-адрес**. Этот вариант используется, если Сервер администрирования имеет статический IP-адрес, который в дальнейшем не будет изменяться.

Шаг 13. Адрес Сервера для подключения мобильных устройств

Этот шаг мастера установки доступен в случае, если вы выбрали для установки компонент Поддержка мобильных устройств.

Укажите внешний адрес Сервера администрирования для подключения мобильных устройств, которые находятся за пределами локальной сети.

Шаг 14. Выбор плагинов управления программами

Выберите плагины управления программами "Лаборатории Касперского", которые требуется установить совместно с Kaspersky Security Center.

Для удобства поиска плагины разделены на группы в зависимости от типа защищаемых объектов.

Шаг 15. Распаковка и установка файлов на жесткий диск

По окончании настройки параметров установки компонентов Kaspersky Security Center вы можете запустить установку файлов на жесткий диск.

Если для запуска установки требуются дополнительные программы, мастер установки сообщит об этом перед началом установки Kaspersky Security Center в окне **Установка обязательных компонентов**. Необходимые программы будут установлены автоматически после нажатия на кнопку **Далее**.

В последнем окне мастера установки вам будет предложено запустить Консоль администрирования. При первом запуске Консоли вы можете выполнить первоначальную настройку программы (см. стр. 176).

Установка в неинтерактивном режиме

Сервер администрирования может быть установлен в неинтерактивном режиме, то есть без интерактивного ввода параметров установки.

► *Чтобы установить Сервер администрирования на локальном устройстве в неинтерактивном режиме,*

выполните команду

```
setup.exe /s /v"DONT_USE_ANSWER_FILE=1 EULA=1 PRIVATEPOLICY=1
<setup_parameters>"
```

где `setup_parameters` – список параметров и их значений, отделенных друг от друга пробелом (`PRO1=PROP1VAL PROP2=PROP2VAL`). Файл setup.exe расположен в папке Server внутри дистрибутива Kaspersky Security Center.

Имена и возможные значения параметров, которые можно использовать при установке Сервера администрирования в неинтерактивном режиме, приведены в таблице ниже.

Таблица 26. Параметры установки Сервера администрирования в неинтерактивном режиме

Имя параметра	Описание параметра	Возможные значения
EULA	Согласие с условиями Лицензионного соглашения	• 1 – согласны с условиями Лицензионного соглашения. • Другое значение или не задано – не согласны с условиями Лицензионного соглашения (установка не выполняется).
PRIVACYPOLICY	Согласие с условиями Политики конфиденциальности	• 1 – согласны с условиями Политики конфиденциальности. • Другое значение или не задано – не согласны с условиями Политики конфиденциальности (установка не выполняется).
INSTALLATIONMODETYPE	Тип установки Сервера администрирования	• Standard – стандартная установка. • Custom – выборочная установка.
INSTALLDIR	Путь к папке установки Сервера администрирования	Строковое значение.
ADDLOCAL	Список компонентов (через запятую) Сервера администрирования для установки	CSAdminKitServer, NAgent, CSAdminKitConsole, NSAC, MobileSupport, KSNProxy, SNMPAgent, GdiPlusRedist, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86 Минимальный достаточный для корректной установки Сервера администрирования список компонентов: `ADDLOCAL=CSAdminKitServer,CSAdminKitConsole,KSNProxy,Microsoft_VC90_CRT_x86,Microsoft_VC100_CRT_x86`

Имя параметра	Описание параметра	Возможные значения
NETRANGETYPE	Размер сети (количество устройств в сети)	• NRT_1_100 – от 1 до 100 устройств. • NRT_100_1000 – от 100 до 1000 устройств. • NRT_GREATER_1000 – более 1000 устройств.
SRV_ACCOUNT_TYPE	Способ задания учетной записи, под которой Сервер администрирования будет запускаться как служба	• SrvAccountDefault – учетная запись создается автоматически. • SrvAccountUser – учетная запись задается вручную; в этом случае следует задать значения параметров SERVERACCOUNTNAME и SERVERACCOUNTPWD.
SERVERACCOUNTNAME	Имя учетной записи, под которой Сервер администрирования будет запускаться как служба; значение параметра задается, если SRV_ACCOUNT_TYPE=SrvAccountUser	Строковое значение.

Имя параметра	Описание параметра	Возможные значения
SERVERACCOUNTPWD	Пароль учетной записи, под которой Сервер администрирования будет запускаться как служба; значение параметра задается, если SRV_ACCOUNT_TYPE=SrvAccountUser	Строковое значение.
SERVERCER	Длина ключа для сертификата Сервера администрирования (в битах)	• 1 – длина ключа для сертификата Сервера администрирования 2048 бит. • Значение не задано – длина ключа для сертификата Сервера администрирования 1024 бит.

Имя параметра	Описание параметра	Возможные значения
DBTYPE	Тип базы данных, которая будет использоваться для размещения информационной базы данных Сервера администрирования. Параметр является обязательным.	• MySQL – будет использоваться база данных MySQL; в этом случае следует задать значения параметров MYSQLSERVERNAME, MYSQLSERVERPORT,MYSQLDBNAME, MYSQLACCOUNTNAME, MYSQLACCOUNTPWD. • MSSQL – будет использоваться база данных Microsoft SQL Server (SQL Express); в этом случае следует задать значения параметров MSSQLSERVERNAME, MSSQLDBNAME, MSSQLAUTHTYPE.
MYSQLSERVERNAME	Полное имя SQL-сервера; значение параметра задается, если DBTYPE=MySQL	Строковое значение.
MYSQLSERVERPORT	Номер порта для подключения к SQL-серверу; значение параметра задается, если DBTYPE=MySQL	Строковое значение.

Имя параметра	Описание параметра	Возможные значения
MYSQLDBNAME	Имя базы данных, которая будет создана для размещения информации Сервера администрирования; значение параметра задается, если DBTYPE=MySQL	Строковое значение.
MYSQLACCOUNTNAME	Имя учетной записи для подключения к базе; значение параметра задается, если DBTYPE=MySQL	Строковое значение.
MYSQLACCOUNTPWD	Пароль учетной записи для подключения к базе; значение параметра задается, если DBTYPE=MySQL	Строковое значение.

Имя параметра	Описание параметра	Возможные значения
MSSQLSERVERNAME	Полное имя SQL-сервера; значение параметра задается, если DBTYPE=MySQL	Строковое значение.
MSSQLDBNAME	Имя базы данных; значение параметра задается, если DBTYPE=MySQL	Строковое значение.
MSSQLAUTHTYPE	Тип авторизации при подключении к SQL-серверу; значение параметра задается, если DBTYPE=MSSQL	• Windows – режим аутентификации Microsoft Windows. • SQLServer – режим аутентификации SQL-сервера; в этом случае следует задать значения параметров MSSQLACCOUNTNAME и MSSQLACCOUNTPWD.

Имя параметра	Описание параметра	Возможные значения
MSSQLACCOUNTNAME	Имя учетной записи для подключения к SQL-серверу; значение параметра задается, если MSSQLAUTHTYPE=SQLServer	Строковое значение.
MSSQLACCOUNTPWD	Пароль учетной записи для подключения к SQL-серверу; значение параметра задается, если MSSQLAUTHTYPE=SQLServer	Строковое значение.
CREATE_SHARE_TYPE	Способ задания папки общего доступа	• Create – создать новую папку общего доступа; в этом случае следует задать значения параметров SHARELOCALPATH и SHAREFOLDERNAME. • ChooseExisting – выбрать существующую папку; в этом случае следует задать значение параметра EXISTSHAREFOLDERNAME.

Имя параметра	Описание параметра	Возможные значения
SHARELOCALPATH	Полный путь к локальной папке; значение параметра задается, если CREATE_SHARE_TYPE=Create	Строковое значение.
SHAREFOLDERNAME	Сетевое имя папки общего доступа; значение параметра задается, если CREATE_SHARE_TYPE=Create	Строковое значение.
EXISTSHAREFOLDERNAME	Полный путь к существующей папке общего доступа; значение параметра задается, если CREATE_SHARE_TYPE=ChooseExisting	Строковое значение.

Имя параметра	Описание параметра	Возможные значения
SERVERPORT	Номер порта для подключения к Серверу администрирования	Числовое значение.
SERVERSSLPORT	Номер порта для защищенного подключения к Серверу администрирования с использованием протокола SSL	Числовое значение.
SERVERADDRESS	Адрес Сервера администрирования	Строковое значение.
MOBILESERVERADDRESS	Адрес Сервера администрирования для подключения мобильных устройств	Строковое значение.

Подробно параметры установки Сервера администрирования описаны в разделе Выборочная установка (на стр. 144).

Изменения в системе после установки Сервера администрирования на устройство

--Значок Консоли администрирования

В результате установки Консоли администрирования на вашем устройстве в меню **Пуск → Программы → Kaspersky Security Center** появится значок для ее запуска.

Службы Сервера администрирования и Агента администрирования

Сервер администрирования и Агент администрирования будут установлены на устройстве в качестве служб со свойствами, указанными в таблице ниже. В таблице также указаны атрибуты других служб, которые выполняются на устройстве после установки Сервера администрирования.

Таблица 27. Свойства служб Kaspersky Security Center

Компонент	Имя службы	Отображаемое имя службы	Учетная запись
Сервер администрирования	kladminserver	Сервер администрирования Kaspersky Security Center	Указанная пользователем или специальная, созданная при установке, непривилегированная учетная запись вида KL-AK-*
Агент администрирования	klnagent	Агент администрирования Kaspersky Security Center	Локальная система
Веб-сервер для работы Веб-консоли и организации внутреннего портала организации	klwebsrv	Веб-сервер "Лаборатории Касперского"	Специальная непривилегированная учетная запись KlScSvc
Прокси-сервер активации	klactprx	Прокси-сервер активации "Лаборатории Касперского"	Специальная непривилегированная учетная запись KlScSvc
Прокси-сервер KSN	ksnproxy	Прокси-сервер Kaspersky Security Network	Специальная непривилегированная учетная запись KlScSvc

Серверная версия Агента администрирования

Вместе с Сервером администрирования на устройство будет установлена серверная версия Агента администрирования. Она входит в состав Сервера администрирования, устанавливается и удаляется в его составе и может взаимодействовать только с локально установленным Сервером администрирования. Настраивать параметры подключения Агента к Серверу администрирования не требуется: настройка реализована программно с учетом того, что компоненты установлены на одном устройстве. Серверная версия Агента администрирования устанавливается с теми же атрибутами и выполняет те же функции управления программами, что и стандартный Агент администрирования. На эту версию будет действовать политика группы администрирования, в которую включено клиентское устройство Сервера администрирования. Для серверной версии Агента администрирования создаются все задачи, предусмотренные для Агента администрирования, за исключением задачи смены Сервера.

Отдельная установка Агента администрирования на устройство с Сервером администрирования невозможна.

Вы можете просматривать свойства служб Сервера и Агента администрирования, а также следить за их работой при помощи стандартных средств администрирования Microsoft Windows – Управление компьютером\Службы. Информация о работе службы Сервера администрирования сохраняется в системном журнале Microsoft Windows на устройстве, где установлен Сервер администрирования, в отдельной ветви журнала Kaspersky Event Log.

Не рекомендуется вручную запускать и отключать службы и менять учетные записи в настройках служб. При необходимости вы можете поменять учетную запись службы Сервера администрирования с помощью утилиты klsrvswch.

Учетные записи и группы пользователей

Инсталлятор Сервера администрирования создает по умолчанию следующие учетные записи:

- KL-AK-*: учетная запись службы Сервера администрирования.
- KlScSvc: учетная запись для прочих служб из состава Сервера администрирования.

- KlPxeUser: учетная запись для развертывания операционных систем.

Если на этапе работы инсталлятора вы выбирали другие учетные записи для службы Сервера администрирования и прочих служб, то будут использованы указанные вами учетные записи.

На устройстве, где установлен Сервер администрирования, также автоматически создаются локальные группы безопасности KLAdmins и KLOperators. Если Сервер администрирования устанавливается на контроллер домена, то автоматически создаются доменные группы безопасности KLAdmins и KLOperators.

При настройке почтовых уведомлений администратору может потребоваться завести учетную запись на почтовом сервере для ESMTP-аутентификации.

См. также

Учетные записи для работы ч 132

Удаление программы

Вы можете удалить Kaspersky Security Center стандартными средствами установки и удаления программ Microsoft Windows. Для удаления программы запускается мастер, в результате работы которого с устройства будут удалены все компоненты программы (включая плагины). Если во время работы мастера вы не задали удаление папки общего доступа (Share), то после завершения всех связанных с ней задач вы можете удалить ее вручную.

После удаления программы в системной временной папке могут оставаться файлы.

Мастер удаления программы предложит вам сохранить резервную копию Сервера администрирования.

При удалении программы с операционных систем Microsoft Windows 7 и Microsoft Windows 2008 возможно преждевременное завершение работы программы удаления. Чтобы избежать этого, отключите в операционной системе службу контроля учетных записей (UAC) и повторно запустите удаление программы.

Установка Консоли администрирования на рабочее место администратора

Вы можете установить Консоль администрирования отдельно на рабочее место администратора и управлять Сервером администрирования по сети с помощью этой Консоли. Консоль администрирования можно установить с помощью мастера установки или в неинтерактивном режиме.

Установка Консоли администрирования с помощью мастера установки

► *Чтобы установить Консоль администрирования на рабочее место администратора, выполните следующие действия:*

1. Запустите исполняемый файл setup.exe.

   Откроется окно с выбором программ "Лаборатории Касперского" для установки.

2. В окне с выбором программ по ссылке **Установить Консоль администрирования Kaspersky Security Center** запустите мастер установки Консоли администрирования. Следуйте указаниям мастера.

3. Выберите папку назначения. По умолчанию это <Диск>:\Program Files\Kaspersky Lab\Kaspersky Security Center Console. Если такой папки нет, она будет создана автоматически в процессе установки. Вы можете сменить папку назначения с помощью кнопки **Обзор**.

4. В завершающем окне мастера установки нажмите на кнопку **Начать**, чтобы начать процесс установки Консоли администрирования.

По окончании работы мастера Консоль администрирования будет установлена на рабочем месте администратора.

После установки Консоли администрирования следует подключиться к Серверу администрирования. Для этого нужно запустить Консоль администрирования и в открывшемся окне указать имя устройства или IP-адрес устройства, на котором установлен Сервер администрирования, а также параметры учетной записи для подключения к нему. После установления соединения с Сервером администрирования можно управлять системой антивирусной защиты с помощью этой Консоли администрирования.

Установка Консоли администрирования в неинтерактивном режиме

Консоль администрирования может быть установлена в неинтерактивном режиме, то есть без интерактивного ввода параметров установки.

► *Чтобы установить Консоль администрирования на локальном устройстве в неинтерактивном режиме,*

выполните команду

```
setup.exe /s /l /v"EULA=1 PRIVATEPOLICY=1"
```

Где ключ /s запускает установку в неинтерактивном (тихом) режиме. Ключ /l – полный путь к файлу инсталлятора. Например, `installer.exe /l c:\windows\temp\log.txt`. Ключ /v – предназначен для передачи инсталлятору значения дополнительного параметра.

Файл setup.exe расположен в папке Console внутри дистрибутива Kaspersky Security Center.

Запуск исполняемого файла с ключами `EULA=1` и `PRIVACYPOLICY=1` означает, что вы принимаете положения Лицензионного соглашения и Политики конфиденциальности соответственно. Текст Лицензионного соглашения и текст Политики конфиденциальности входят в комплект поставки Kaspersky Security Center. Согласие с положениями Лицензионного соглашения и Политики конфиденциальности является необходимым условием для установки программы или обновления предыдущей версии программы.

Вы можете удалить Консоль администрирования стандартными средствами установки и удаления программ Microsoft Windows.

Настройка подключения Консоли администрирования к Серверу администрирования

В предыдущих версиях Kaspersky Security Center Консоль администрирования подключалась к Серверу администрирования, используя SSL-порт TCP 13291, а также SSL-порт TCP 13000. Начиная с версии Kaspersky Security Center 10 Service Pack 2 SSL-порты, используемые программой, строго разделены, и использование портов не по назначению невозможно:

- SSL-порт TCP 13291 могут использовать только Консоль администрирования и объекты автоматизации утилиты klakaut.
- SSL-порт TCP 13000 могут использовать только Агент администрирования, подчиненный Сервер и главный Сервер администрирования, размещенный в демилитаризованной зоне.

Порт TCP 14000 может использоваться для подключения Консоли администрирования, агентов обновлений, подчиненных Серверов администрирования и объектов автоматизации утилиты klakaut, а также для получения данных с клиентских устройств.

В некоторых случаях может быть необходимо подключение Консоли администрирования по SSL-порту 13000:

- если предпочтительно использовать один и тот же SSL-порт как для Консоли администрирования, так и для других активностей (для получения данных с клиентских устройств, подключения агентов обновлений, подключения подчиненных Серверов администрирования),
- если объект автоматизации утилиты klakaut подключается к Серверу администрирования не напрямую, а через агент обновлений, размещенный в демилитаризованной зоне.

► *Чтобы разрешить подключение Консоли администрирования по порту 13000, выполните следующие действия:*

1. Откройте системный реестр устройства, на котором установлен Сервер администрирования, например, локально с помощью команды regedit в меню **Пуск** → **Выполнить**.

2. Перейдите в раздел:

   - для 64-разрядной системы:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\KLLIM

   - для 32-разрядной системы:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.core\.independent\KLLIM

3. Для ключа LP_ConsoleMustUsePort13291 (DWORD) установите значение 00000000.

   По умолчанию для этого ключа указано значение 1.

4. Перезапустите службу Сервера администрирования.

В результате Консоль администрирования сможет подключаться к Серверу администрирования, используя порт 13000.

Установка и настройка Kaspersky Security Center SHV

Kaspersky Security Center предоставляет возможность интеграции в платформу Microsoft Network Access Protection (NAP). Microsoft NAP позволяет регулировать доступ клиентских устройств в сеть. Microsoft NAP предполагает, что в сети выделен сервер с установленной операционной системой Microsoft Windows Server 2008, на который установлена служба PVS (Posture Validation Server), а на клиентских устройствах установлены NAP-совместимые операционные системы: Microsoft Windows Vista, Microsoft Windows XP с установленным Пакетом обновлений 3, Microsoft Windows 7.

При совместной работе программы Kaspersky Security Center с Microsoft NAP проверку работоспособности операционной системы осуществляет System Health Validator (далее – Kaspersky Security Center SHV).

► *Чтобы установить Kaspersky Security Center SHV на устройство локально, выполните следующие действия:*

1. Запустите исполняемый файл setup.exe.

   Откроется окно с выбором программ "Лаборатории Касперского" для установки.

   В окне с выбором программ по ссылке **Установить Kaspersky Security Center SHV** запустите мастер установки Kaspersky Security Center SHV. Следуйте указаниям мастера.

2. Определите папку назначения. По умолчанию это <Диск>:\Program Files\Kaspersky Lab\Kaspersky Security Center SHV. Если такой папки нет, она будет создана автоматически в процессе установки. Вы можете сменить папку назначения с помощью кнопки **Обзор**.

3. В завершающем окне мастера установки нажмите на кнопку **Начать**, чтобы начать процесс установки Kaspersky Security Center SHV.

По окончании работы мастера Kaspersky Security Center SHV будет установлен на вашем устройстве.

Вы можете удалить Kaspersky Security Center SHV стандартными средствами установки и удаления программ Microsoft Windows. При этом запускается мастер, в результате работы которого с устройства будут удалены все компоненты программы.

Мастер первоначальной настройки Сервера администрирования

В этом разделе представлена информация о работе мастера первоначальной настройки Сервера администрирования.

Программа Kaspersky Security Center позволяет настроить минимальный набор параметров, необходимых для построения системы централизованного управления защитой, с помощью

мастера первоначальной настройки. В процессе работы мастера вы можете внести в программу следующие изменения:

- Добавить ключи или ввести коды активации, которые можно автоматически распространять на устройства в группах администрирования.
- Настроить взаимодействие с Kaspersky Security Network (KSN). При разрешении использования KSN мастер включает службу прокси-сервера KSN, которая обеспечивает взаимодействие между KSN и устройствами.
- Настроить рассылку по электронной почте оповещений о событиях в работе Сервера администрирования и управляемых программ (чтобы уведомление прошло успешно, на Сервере администрирования и на всех устройствах-получателях должна быть запущена служба сообщений Messenger).
- Настроить параметры обновлений и закрытия уязвимостей программ, установленных на устройствах.
- Сформировать политику защиты рабочих станций и серверов, а также задачи поиска вирусов, получения обновлений и резервного копирования данных для верхнего уровня иерархии управляемых устройств.

  Мастер первоначальной настройки создает политики защиты только для тех программ, для которых они еще не присутствуют в папке **Управляемые устройства**. Мастер первоначальной настройки не создает задачи, если задачи с такими именами уже созданы для верхнего уровня иерархии управляемых устройств.

Программа автоматически предлагает запустить мастер первоначальной настройки после установки Сервера администрирования при первом подключении к Серверу. Вы также можете запустить мастер первоначальной настройки вручную в любое время.

► *Чтобы запустить мастер первоначальной настройки вручную, выполните следующие действия:*

1. В дереве консоли выберите узел **Сервер администрирования**.
2. В контекстном меню узла выберите пункт **Все задачи → Мастер первоначальной настройки Сервера администрирования**.

Мастер предложит произвести первоначальную настройку Сервера администрирования. Следуйте его указаниям.

В этом разделе

Шаг 1. Настройка дополнительных компонентов

Укажите, требуется ли вашей организации управление корпоративными мобильными устройствами. Выберите один из следующих вариантов:

- **Поддержка мобильных устройств не требуется**

  Выберите этот вариант, если вам не нужна функция поддержки мобильных устройств.

- **Включить поддержку мобильных устройств**

Выберите этот вариант, если вы хотите управлять мобильными устройствами сотрудников.

Шаг 2. Выбор способа активации программы

Выберите один из следующих вариантов активации Kaspersky Security Center:

- Введите код активации

  Код активации – это уникальная последовательность из двадцати латинских букв и цифр. Вы вводите код активации, чтобы добавить ключ, активирующий Kaspersky Security Center. Вы получаете код активации по указанному вами адресу электронной почты после приобретения Kaspersky Security Center или после заказа пробной версии Kaspersky Security Center.

  Чтобы активировать программу с помощью кода активации, требуется доступ в интернет для подключения к серверам активации "Лаборатории Касперского".

- Укажите файл ключа

  Файл ключа – это файл с расширением key, который вам предоставляет "Лаборатория Касперского". Файл ключа предназначен для добавления ключа, активирующего программу.

  Вы получаете файл ключа по указанному вами адресу электронной почты после приобретения Kaspersky Security Center или после заказа пробной версии Kaspersky Security Center.

  Чтобы активировать программу с помощью файла ключа, не требуется подключение к серверам активации "Лаборатории Касперского".

- Отложите активацию программы

  Программа будет работать в ограниченном режиме, без поддержки мобильных устройств и без функциональности системного администрирования.

Если вы выбрали отложенную активацию программы, вы можете добавить ключ позже в любое время.

► *Чтобы добавить ключ после завершения работы мастера первоначальной настройки, выполните следующие действия:*

1. В дереве консоли перейдите в раздел **Лицензии Лаборатории Касперского**.
2. Нажмите на кнопку **Добавить код активации или ключ**.

   Откроется мастер добавления ключа.
3. Следуйте указаниям мастера.

Шаг 3. Настройка параметров прокси-сервера

Настройте параметры доступа Kaspersky Security Center к интернету.

Установите флажок **Использовать прокси-сервер**, если вы хотите включить возможность использования прокси-сервера для подключения к интернету. Если флажок установлен, доступны поля ввода параметров. Настройте следующие параметры подключения к прокси-серверу:

- **Адрес**

  Адрес прокси-сервера для подключения Kaspersky Security Center к интернету.
- **Номер порта**

  Номер порта, по которому будет выполняться подключение Kaspersky Security Center к прокси-серверу.
- **Не использовать прокси-сервер для локальных адресов**

  При подключении к устройствам в локальной сети не будет использоваться прокси-сервер.

- **Аутентификация на прокси-сервере**

  Если флажок установлен, в полях ввода можно указать учетные данные для аутентификации на прокси-сервере. Поля ввода доступны, если установлен флажок **Использовать прокси-сервер**.

- **Имя пользователя** (поле доступно, если установлен флажок **Аутентификация на прокси-сервере**)

  Учетная запись пользователя, от имени которой будет выполняться подключение к прокси-серверу.

- **Пароль** (поле доступно, если установлен флажок **Аутентификация на прокси-сервере**)

  Пароль пользователя, через учетную запись которого выполняется подключение к прокси-серверу.

  После того как вы начали вводить пароль, отображается кнопка **Показать пароль**. Чтобы посмотреть введенный пароль, нажмите на кнопку **Показать пароль** и удерживайте ее необходимое вам время.

Шаг 4. Проверка обновлений для плагинов и инсталляционных пакетов

Настройте параметры проверки установленных плагинов и инсталляционных пакетов на актуальность. Выберите один из следующих вариантов:

- **Проверить актуальность плагинов и инсталляционных пакетов**

  Запуск проверки на актуальность. Если проверка обнаружит использование устаревших версий плагинов или инсталляционных пакетов, мастер предложит загрузить актуальные версии вместо устаревших.

- **Пропустить проверку**

  Продолжение работы без проверки плагинов и инсталляционных пакетов на актуальность. Этот вариант можно выбрать, например,

если у вас нет доступа в интернет или вы по какой-то причине хотите продолжить пользоваться устаревшей версией программы.

Пропуск проверки актуальности плагинов и инсталляционных пакетов может привести к некорректной работе программы.

Шаг 5. Настройка Kaspersky Security Network

Настройте параметры передачи информации о работе Kaspersky Security Center в базу знаний Kaspersky Security Network. Выберите один из следующих вариантов:

- **Я принимаю условия использования Kaspersky Security Network**

  Клиентские устройства под управлением Kaspersky Security Center в автоматическом режиме будут предоставлять "Лаборатории Касперского" информацию о работе установленных на них программ "Лаборатории Касперского". Сотрудничество с Kaspersky Security Network обеспечивает более быстрое обновление баз данных о вирусах и угрозах, что увеличивает скорость реагирования на возникающие угрозы безопасности.

- **Я не принимаю условия использования Kaspersky Security Network**

  Клиентские устройства под управлением Kaspersky Security Center не будут предоставлять "Лаборатории Касперского" информацию о работе установленных на них программ "Лаборатории Касперского".

Шаг 6. Настройка параметров отправки почтовых уведомлений

Настройте параметры рассылки оповещений о событиях, регистрируемых при работе программ "Лаборатории Касперского" на клиентских устройствах. Эти параметры будут использоваться в качестве значений по умолчанию в политиках программ.

Для настройки рассылки оповещений о возникающих событиях программ "Лаборатории Касперского" доступны следующие параметры:

- **Получатели (адреса электронной почты)**

  Адреса электронной почты пользователей, которым программа будет отправлять уведомления.

- **SMTP-серверы**

  Адреса почтовых серверов вашей организации, введенные через точку с запятой. В качестве адреса может использоваться IP-адрес или имя устройства в сети Windows (NetBIOS-имя).

- **Порт SMTP-сервера**

  Номер коммуникационного порта SMTP-сервера. По умолчанию указан порт 25.

- **Требуется ESMTP-аутентификация**

  Включение поддержки ESMTP-аутентификации. После установки флажка в полях **Имя пользователя** и **Пароль** можно указать параметры ESMTP-аутентификации. По умолчанию флажок снят, параметры ESMTP-аутентификации недоступны.

Вы можете проверить установленные параметры отправки почтовых уведомлений с помощью кнопки **Отправить пробное сообщение**.

Шаг 7. Настройка параметров управления обновлениями

Настройте параметры работы с обновлениями программ, установленных на клиентских устройствах.

В блоке параметров **Режим поиска и установки обновлений** вы можете выбрать один из режимов поиска и установки обновлений Kaspersky Security Center:

- **Искать требующиеся для установки обновления**

  Создается задача **Поиск уязвимостей и требуемых обновлений**.

  Этот вариант выбран по умолчанию.

- **Искать и устанавливать требующиеся обновления**

  Создаются задачи **Поиск уязвимостей и требуемых обновлений** и **Установка требуемых обновлений и закрытие уязвимостей**.

В блоке параметров **Служба Windows Update** вы можете выбрать один из способов синхронизации обновлений:

- **Использовать имеющийся в сети WSUS-сервер**

  Задача **Синхронизация обновлений Windows Update** не создается.

  Этот вариант выбран по умолчанию.

- **Использовать Сервер администрирования в роли WSUS-сервера**

  Создается задача **Синхронизация обновлений Windows Update**.

Шаг 8. Создание первоначальной конфигурации защиты

В окне **Создание первоначальной конфигурации защиты** отображается список создаваемых политик и задач.

Для перехода на следующий шаг мастера дождитесь окончания создания политик и задач.

Во время создания политик и задач откроется окно первоначальной настройки доверенной зоны Kaspersky Security Center. Программа предложит внести в доверенную зону проверенных "Лабораторией Касперского" производителей, чтобы исключить их программы из проверки для предотвращения случайной блокировки. Вы можете создать рекомендованные исключения сейчас или создать список исключений позже, выбрав в дереве консоли **Политики** → меню свойств Kaspersky Endpoint Security → **Продвинутая защита** → **Предотвращение вторжений** → **Настройка** → **Добавить**. Список исключений проверки доступен для редактирования в любой момент дальнейшей работы с программой.

Работа с доверенной зоной выполняется средствами программы Kaspersky Endpoint Security для Windows. Подробные инструкции по выполнению операций и описание особенностей функциональности шифрования приведены в онлайн-справке Kaspersky Endpoint Security для Windows https://help.kaspersky.com/KESWin/11/ru-RU/127968.htm.

Для завершения первоначальной настройки доверенной зоны и возвращения к мастеру нажмите **ОК**.

Нажмите на кнопку **Далее**. Она станет доступна, когда все необходимые политики и задачи будут созданы.

Шаг 9. Подключение мобильных устройств

Если ранее в настройках мастера вы выбрали включение поддержки мобильных устройств, настройте параметры подключения корпоративных мобильных устройств управляемой компании. Если вы указали, что поддержка мобильных устройств не требуется, то этот шаг будет пропущен.

► *Чтобы настроить порты подключения мобильных устройств, выполните следующие действия:*

1. Нажмите на кнопку **Настроить** справа от поля **Подключение мобильных устройств**.

2. В раскрывающемся списке выберите **Настроить порты**.

   Откроется окно свойств Сервера администрирования на разделе **Дополнительные порты**.

3. В разделе **Дополнительные порты** вы можете настроить параметры подключения мобильных устройств:

   - **SSL-порт для прокси-сервера активации**

     Номер SSL-порта для подключения Kaspersky Endpoint Security 10 для Windows к серверам активации "Лаборатории Касперского".

     По умолчанию используется порт 17000.

- **Открыть порт для мобильных устройств**

  Если флажок установлен, то открыт порт, по которому мобильные устройства будут подключаться к Серверу лицензирования. Вы можете задать номер порта и другие настройки в полях ниже.

  Если флажок снят, то открытого порта для подключения мобильных устройств нет, и поля **Порт для мобильных устройств** и **Порт активации мобильных клиентов** недоступны для редактирования.

  По умолчанию флажок установлен.

- **Порт для мобильных устройств**

  Номер порта, по которому мобильные устройства будут подключаться к Серверу администрирования и обмениваться с ним информацией. По умолчанию используется порт 13292.

  Вы можете назначить другой порт, если порт 13292 используется в каких-то других целях.

- **Порт активации мобильных клиентов**

  Порт подключения Kaspersky Endpoint Security для Android к серверам активации "Лаборатории Касперского".

  По умолчанию используется порт 17100.

- **Открыть порт для устройств с защитой на уровне UEFI**

  Если флажок установлен, то устройства с защитой на уровне UEFI могут подключаться к Серверу администрирования.

  По умолчанию флажок установлен.

- **Порт для устройств с защитой на уровне UEFI**

  Вы можете изменить номер порта, если установлен флажок **Открыть порт для устройств с защитой на уровне UEFI**. По умолчанию используется порт 13294.

4. Нажмите на кнопку **ОК**, чтобы сохранить изменения и вернуться к мастеру первоначальной настройки.

Вам потребуется настроить аутентификацию Сервера администрирования мобильными устройствами и аутентификацию мобильных устройств Сервером администрирования.

► *Чтобы настроить параметры аутентификации Сервера администрирования мобильными устройствами, выполните следующие действия:*

1. Нажмите на кнопку **Настроить** справа от поля **Подключение мобильных устройств**.

2. В раскрывающемся списке выберите **Настроить аутентификацию**.

   Откроется окно свойств Сервера администрирования на разделе **Сертификаты**.

3. Выберите вариант аутентификации для мобильных устройств в блоке параметров **Аутентификация Сервера мобильными устройствами** и для устройств со встроенной защитой на уровне UEFI в блоке параметров **Аутентификация Сервера устройствами с защитой на уровне UEFI**.

   Аутентификация Сервера администрирования при обмене информацией с клиентскими устройствами выполняется на основании сертификата.

   По умолчанию выбрано использование сертификата, созданного при установке Сервера администрирования.

   Чтобы добавить новый сертификат:

   a. Выберите вариант **Другой сертификат**.

   Появится кнопка **Выбрать**.

   b. Нажмите на кнопку **Выбрать**.

   c. В появившемся окне настройте параметры сертификата:

   - **Тип сертификата**
   - Срок активации:
     - **Немедленно**

     Текущий сертификат будет заменен новым сертификатом сразу после нажатия на кнопку **ОК**.

     Ранее подключенные мобильные устройства не смогут подключиться к

Серверу администрирования.

- **Через указанный срок (сут)**

Если выбран этот вариант, то будет сгенерирован резервный сертификат. Текущий сертификат будет заменен новым сертификатом через указанное количество дней. Дата, с которой резервный сертификат вступит в силу, отображается в разделе **Сертификаты**.

После того как текущий сертификат будет заменен новым сертификатом, ранее подключенные мобильные устройства не смогут подключиться к Серверу администрирования.

Вы можете нажать на кнопку **Свойства**, чтобы просмотреть параметры выбранного сертификата Сервера администрирования.

Чтобы перевыпустить сертификат, выпущенный средствами Сервера администрирования:

1. Нажмите на кнопку **Перевыпустить**.
2. В открывшемся окне настройте следующие параметры:

- Адрес подключения:

  - **Оставить адрес подключения прежним**

  Адрес Сервера администрирования, к которому подключаются мобильные устройства, останется прежним.

  Этот вариант выбран по умолчанию.

  - **Изменить адрес подключения на**

  Если необходимо, чтобы мобильные устройства подключались по другому адресу, укажите в поле требуемый адрес.

  При изменении адреса подключения мобильных устройств необходимо выпустить новый сертификат. Старый сертификат будет недействительным на подключенных мобильных устройствах. Ранее подключенные устройства не смогут подключиться к Серверу администрирования и перестанут быть управляемыми.

- Срок активации:

- **Немедленно**

  Текущий сертификат будет заменен новым сертификатом сразу после нажатия на кнопку **ОК**.

  Ранее подключенные мобильные устройства не смогут подключиться к Серверу администрирования.

- **Через указанный срок (сут)**

  Если выбран этот вариант, то будет сгенерирован резервный сертификат. Текущий сертификат будет заменен новым сертификатом через указанное количество дней. Дата, с которой резервный сертификат вступит в силу, отображается в разделе **Сертификаты**.

  После того как текущий сертификат будет заменен новым сертификатом, ранее подключенные мобильные устройства не смогут подключиться к Серверу администрирования.

3. Нажмите на кнопку **ОК**, чтобы сохранить изменения и вернуться к окну **Сертификаты**.

4. Нажмите на кнопку **ОК**, чтобы сохранить изменения и вернуться к мастеру первоначальной настройки.

► *Чтобы настроить выпуск, автоматическое обновление и шифрование сертификатов общего типа для идентификации мобильных устройств Сервером администрирования, выполните следующие действия:*

1. Нажмите на кнопку **Настроить** справа от поля **Идентификация мобильных устройств**.

   Откроется окно **Правила выпуска сертификатов** на разделе **Выпуск сертификатов общего типа**.

2. При необходимости настройте следующие параметры в блоке параметров **Параметры выпуска**:

   - **Срок действия сертификата, дней**

     Срок действия сертификата в днях. По умолчанию срок действия сертификата равен 365 дням. По истечении этого срока мобильное устройство не сможет подключаться к Серверу администрирования.

- **Источник сертификатов**

  Выбор источника сертификатов общего типа для мобильных устройств: сертификаты выпускает Сервер администрирования или сертификаты задаются вручную.

Вы можете изменить шаблон сертификата, если в разделе **Интеграция с PKI** настроена интеграция с инфраструктурой открытых ключей. В этом случае будут доступны следующие поля выбора шаблона:

- **Шаблон по умолчанию**

  Использование сертификата, выпущенного внешним источником сертификатов – центром сертификации – по шаблону, заданному по умолчанию.

  По умолчанию выбран этот вариант.

- **Другой шаблон**

  Выбор шаблона, на основании которого будут выпускаться сертификаты. Шаблоны сертификатов можно задать в домене. По кнопке **Обновить список** можно обновить список шаблонов сертификатов.

3. При необходимости задайте следующие параметры автоматического выпуска сертификатов в блоке параметров **Параметры автоматического обновления**:

   - **Обновлять, когда до истечения срока действия осталось (сут)**

     Количество дней до истечения срока действия текущего сертификата, за которое Сервер администрирования должен выпустить новый сертификат. Например, если в поле указано значение 4, Сервер администрирования выпустит новый сертификат за четыре дня до окончания срока действия текущего сертификата. По умолчанию указано значение 7.

   - **Автоматически перевыпускать сертификат, если это возможно**

     При наличии возможности сертификаты будут перевыпускаться

автоматически. Автоматический перевыпуск недоступен, если сертификат был задан вручную. Если флажок снят, сертификаты автоматически не перевыпускаются. По умолчанию флажок снят.

Сертификаты обновляются автоматически центром сертификации.

4. При необходимости настройте параметры расшифровки сертификатов при установке в блоке параметров **Защита паролем**.

   Установите флажок **Запрашивать пароль при установке сертификата**, чтобы при установке сертификата на мобильное устройство у пользователя запрашивался пароль. Пароль используется только один раз, при установке сертификата на мобильное устройство.

   Пароль будет автоматически сгенерирован средствами Сервера администрирования и отправлен по указанному вами адресу электронной почты. Вы можете указать адрес электронной почты пользователя либо свой собственный, если хотите затем передать пользователю пароль другим способом.

   Вы можете указать количество символов пароля для расшифровки сертификата с помощью ползунка.

   Функция запроса пароля необходима, например, для защиты общего сертификата в автономном пакете установки Kaspersky Endpoint Security для Android. Защита паролем не позволит злоумышленнику получить доступ к общему сертификату при краже автономного пакета установки с Веб-сервера Kaspersky Security Center.

   Если флажок снят, расшифровка сертификата при установке будет проводиться автоматически и у пользователя не будет запрашиваться пароль. По умолчанию флажок снят.

5. Нажмите на кнопку **ОК**, чтобы сохранить изменения и вернуться к окну мастера первоначальной настройки.

   Нажмите на кнопку **Отмена**, чтобы вернуться к мастеру первоначальной настройки без сохранения внесенных изменений.

► *Чтобы включить функцию перемещения мобильных устройств в нужную вам группу администрирования,*

в поле **Правила перемещения мобильных устройств** установите флажок **Обеспечить наличие правила перемещения**.

Если флажок **Обеспечить наличие правила перемещения** установлен, программа автоматически создает правило перемещения, которое перемещает следующие устройства в группу **Управляемые устройства**:

- с операционными системами Android, на которых установлен общий сертификат,
- с операционными системами iOS, на которых установлен Kaspersky Safe Browser и общий сертификат.

Если такое правило уже существует, то программа не создает правило.

По умолчанию флажок снят.

Шаг 10. Опрос сети

В информационном окне **Опрос сети** отображается информация о статусе опроса сети Сервером администрирования.

Вы можете просмотреть обнаруженные в сети Сервером администрирования устройства и получить справку по работе с окном **Опрос сети** по ссылкам в нижней части окна.

Шаг 11. Завершение работы мастера первоначальной настройки

В окне завершения работы мастера первоначальной настройки установите флажок **Запустить мастер развертывания защиты на рабочих станциях**, если вы хотите запустить автоматическую установку антивирусных программ и / или Агента администрирования на устройства в вашей сети.

Для завершения работы мастера нажмите на кнопку **Завершить**.

Настройка защиты в сети организации-клиента

После завершения инсталляции Сервера администрирования запускается Консоль администрирования, которая предлагает выполнить первоначальную настройку с помощью мастера. Во время работы мастера первоначальной настройки в корневой группе администрирования создаются следующие политики и задачи:

- политика Kaspersky Endpoint Security;
- групповая задача обновления Kaspersky Endpoint Security;
- групповая задача проверки устройства Kaspersky Endpoint Security;
- политика Агента администрирования;
- задача поиска уязвимостей (задача Агента администрирования);
- задача установки обновлений и закрытия уязвимостей (задача Агента администрирования).

Политики и задачи создаются с параметрами по умолчанию, которые могут оказаться неоптимальными или даже непригодными для данной организации. Поэтому следует просмотреть свойства созданных объектов и, в случае необходимости, внести изменения вручную.

В этом разделе содержится информация о ручной настройке политик, задач и других параметров Сервера администрирования, а также информация об агенте обновлений, построении структуры групп администрирования, иерархии задач, и других настройках.

В этом разделе

Ручная настройка политики Kaspersky Endpoint Security

Этот раздел содержит рекомендации по настройке параметров политики Kaspersky Endpoint Security, которую создает мастер первоначальной настройки Kaspersky Security Center. Настройка выполняется в окне свойств политики.

При изменении параметра следует помнить, что для того, чтобы значение параметра использовалось на рабочей станции, следует нажать на кнопку с "замком" над параметром.

В этом разделе

Настройка политики в разделе Базовая защита

Ниже описаны действия по дополнительной настройке, которую рекомендуется выполнить в окне свойств политики Kaspersky Endpoint Security в разделе **Базовая защита**.

Раздел Базовая защита, подраздел Сетевой экран

Следует проверить список сетей в свойствах политики. В списке могут отображаться не все сети.

► *Чтобы проверить список сетей, выполните следующие действия:*

1. В свойствах политики в разделе **Базовая защита** выберите подраздел **Сетевой экран**.
2. В блоке **Доступные сети** нажмите на кнопку **Настройка**.

   Откроется окно **Сетевой экран**. Список сетей отображается в этом окне на закладке **Сети**.

Раздел Базовая защита, подраздел Защита от файловых угроз

Включенная проверка сетевых дисков может создавать значительную нагрузку на сетевые диски. Целесообразнее осуществлять проверку непосредственно на файловых серверах.

► *Чтобы выключить проверку сетевых дисков, выполните следующие действия:*

1. В свойствах политики в разделе **Базовая защита** выберите подраздел **Защита от файловых угроз**.
2. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

3. В открывшемся окне **Защита от файловых угроз** на закладке **Общие** снимите флажок **Все сетевые диски**.

Настройка политики в разделе Дополнительные параметры

Ниже описаны действия по дополнительной настройке, которые рекомендуется выполнить в окне свойств политики Kaspersky Endpoint Security в разделе **Дополнительные параметры**.

Раздел Дополнительные параметры, подраздел Отчеты и хранилища

В блоке **Информировать Сервер администрирования** следует обратить внимание на следующие параметры:

- Флажок **О найденных уязвимостях** – этот параметр нужен главным образом для обеспечения обратной совместимости с более ранними версиями Kaspersky Security Center. Обнаружение уязвимостей встроено в Kaspersky Security Center начиная с версии 10. Поэтому, если используется Сервер администрирования и Агенты администрирования версии 10 и выше, этот флажок целесообразно снять.

- Флажок **О запускаемых программах** – если флажок установлен, в базе данных Сервера администрирования сохраняется информация о всех версиях всех модулей приложений на устройствах в сети организации. Указанная информация может занимать значительный объем в базе данных Kaspersky Security Center (десятки гигабайт). Поэтому в политике верхнего уровня флажок **О запускаемых программах** следует снять, если он оказался установлен.

Раздел Дополнительные параметры, подраздел Интерфейс

Если защита в сети организации должна управляться полностью централизованно через Консоль администрирования, то следует выключить отображение пользовательского интерфейса Kaspersky Endpoint Security на рабочих станциях (снять флажок **Отображать интерфейс программы** в разделе **Взаимодействие с пользователем**), а также включить защиту паролем (установить флажок **Включить защиту паролем** в разделе **Защита паролем**).

Раздел Дополнительные параметры, подраздел Параметры KSN

Целесообразно включить использование прокси-сервера KSN (установить флажок **Использовать прокси-сервер KSN**), так как это существенно повышает надежность обнаружения вредоносного программного обеспечения.

Настройка политики в разделе События

В разделе **События** следует отключить сохранение на Сервере администрирования всех событий, за исключением перечисленных ниже:

- На закладке **Информационное сообщение**:
  - Объект вылечен.
  - Объект удален.
  - Запуск программы запрещен в тестовом режиме.
  - Объект помещен на карантин.
  - Объект восстановлен из карантина.
  - Создана резервная копия объекта.
- На закладке **Предупреждение**:
  - Самозащита программы выключена.
  - Компоненты защиты выключены.
  - Некорректный резервный код активации.
  - Пользователь отказался от политики шифрования.
  - Жалоба на запрет запуска программы.
  - Жалоба на запрет доступа к устройству.
  - Жалоба на запрет доступа к веб-контенту.

    - Обнаружена программа, которая может быть использована злоумышленником.
- На закладке **Отказ функционирования**:
    - Ошибка в параметрах задачи. Параметры задачи не применены.
- На закладке **Критическое событие**:
    - Автозапуск программы выключен.
    - Доступ запрещен.
    - Запрещено.
    - Запуск программы запрещен.
    - Лечение невозможно.
    - Нарушено Лицензионное соглашение.
    - Невозможен запуск двух задач одновременно.
    - Обнаружен возможно зараженный объект.
    - Обнаружен вредоносный объект.
    - Обнаружена активная угроза. Требуется запуск процедуры лечения.
    - Обнаружена ранее открытая фишинговая ссылка.
    - Обнаружена ранее открытая вредоносная ссылка.
    - Обнаружена сетевая атака.
    - Обновлены не все компоненты.
    - Операция с устройством запрещена.
    - Ошибка активации.
    - Ошибка активации портативного режима.
    - Ошибка взаимодействия с Kaspersky Security Center.

- Ошибка деактивации портативного режима.
- Ошибка изменения состава программы.
- Ошибка применения шифрования / расшифровки файлов.
- Политика не может быть применена.
- Процесс завершен.
- Сетевая активность запрещена.
- Сетевая ошибка обновления.

Ручная настройка групповой задачи обновления Kaspersky Endpoint Security

> Информация в этом подразделе применима для Kaspersky Security Center 10 Maintenance Release 1 и более поздних версий.

Для групповых задач обновления Kaspersky Endpoint Security версий 10 и выше оптимальным и рекомендуемым является расписание **При загрузке обновлений в хранилище** при установленном флажке **Автоматически определять интервал для распределения запуска задачи**.

Для групповой задачи обновления Kaspersky Endpoint Security версии 8 следует явно указать период запуска (1 час или больше) и установить флажок **Автоматически определять интервал для распределения запуска задачи**.

Ручная настройка групповой задачи проверки устройства Kaspersky Endpoint Security

Мастер первоначальной настройки создает групповую задачу проверки устройства. По умолчанию для задачи выбрано расписание **Запускать по пятницам в 19:00** с автоматической рандомизацией и снят флажок **Запускать пропущенные задачи**.

Это означает, что если устройства организации выключаются по пятницам, например, в 18:30, то задача проверки устройства никогда не будет запущена. Следует настроить оптимальное расписание этой задачи исходя из принятого в организации регламента работы.

Ручная настройка расписания задачи поиска уязвимостей

Мастер первоначальной настройки создает для Агента администрирования групповую задачу поиска уязвимостей. По умолчанию для задачи выбрано расписание **Запускать по вторникам в 19:00** с автоматической рандомизацией и установлен флажок **Запускать пропущенные задачи**.

Если регламент работы организации предусматривает выключение устройств в это время, то задача поиска уязвимостей будет запущена после включения устройства (в среду утром). Такое поведение может быть нежелательным, так как поиск уязвимостей может вызывать повышенную нагрузку на процессор и дисковую подсистему устройства. Следует задать оптимальное расписание задачи поиска уязвимостей исходя из принятого в организации регламента работы.

Ручная настройка групповой задачи установки обновлений и закрытия уязвимостей

Мастер первоначальной настройки создает для Агента администрирования групповую задачу установки обновлений и поиска уязвимостей. По умолчанию настроен запуск задачи ежедневно в 1:00 с автоматической рандомизацией, флажок **Запускать пропущенные задачи** снят.

Если регламент работы организации предусматривает отключение устройств на ночь, то задача установки обновлений никогда не будет запущена. Следует задать оптимальное расписание задачи поиска уязвимостей исходя из принятого в организации регламента работы. Кроме того, следует учитывать, что в результате установки обновлений может потребоваться перезагрузка устройства.

Построение структуры групп администрирования и назначение агентов обновлений

Структура групп администрирования в Kaspersky Security Center выполняет следующие функции:

- Задание области действия политик.

  Существует альтернативный способ применения нужных наборов параметров на устройствах с помощью *профилей политик*. В этом случае область действия политик задается с помощью тегов, местоположения устройств в подразделениях Active Directory, членства в группах безопасности Active Directory и прочего (см. раздел "Иерархия политик, использование профилей политик" на стр. 209).

- Задание области действия групповых задач.

  Существует подход к заданию области действия групповых задач, не основанный на иерархии групп администрирования: использование задач для выборок устройств и наборов устройств.

- Задание прав доступа к устройствам, виртуальным и подчиненным Серверам администрирования.

- Назначение агентов обновлений.

При построении структуры групп администрирования следует учитывать топологию сети организации для оптимального назначения агентов обновлений. Оптимальное распределение агентов обновлений позволяет уменьшить сетевой трафик внутри сети организации.

В зависимости от организационной структуры организации и топологии сетей можно выделить следующие типовые конфигурации структуры групп администрирования:

- один офис;

- множество небольших изолированных офисов.

В этом разделе

Типовая конфигурация агентов обновлений: один офис

В типовой конфигурации "один офис" все устройства находятся в сети организации и "видят" друг друга. Сеть организации может состоять из нескольких выделенных "частей" (сетей или сегментов сети), связанных узкими каналами.

Возможны следующие способы построения структуры групп администрирования:

- Построение структуры групп администрирования с учетом топологии сети. Структура групп администрирования не обязательно должна точно отражать топологию сети. Достаточно того, чтобы выделенным частям сети соответствовали какие-либо группы администрирования. Можно использовать автоматическое назначение агентов обновлений, либо назначать агенты обновлений вручную.

- Построение структуры групп администрирования, не отражающей топологию сети. В этом случае следует отключить автоматическое назначение агентов обновлений, и в каждой выделенной части сети назначить одно или несколько устройств агентами обновлений на корневую группу администрирования, например, на группу **Управляемые устройства**. Все агенты обновлений окажутся на одном уровне и будут иметь одинаковую область действия "все устройства сети организации". Каждый Агент администрирования версии 10 Service Pack 1 или более поздней

версии в таком случае будет подключаться к тому агенту обновлений, маршрут к которому является самым коротким. Маршрут к агенту обновлений можно определить с помощью утилиты tracert.

Типовая конфигурация агентов обновлений: множество небольших изолированных офисов

Этой типовой конфигурации соответствует множество небольших удаленных офисов, возможно, связанных с главным офисом через интернет. Каждый из удаленных офисов находится за NAT, то есть подключение из одного удаленного офиса в другой невозможно – офисы изолированы друг от друга.

Конфигурацию следует обязательно отразить в структуре групп администрирования: для каждого из удаленных офисов следует создать отдельную группу администрирования (группы **Офис 1**, **Офис 2** на рисунке ниже).

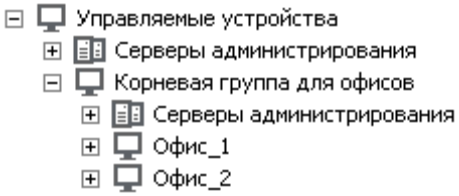


Рисунок 2. Удаленные офисы отражены в структуре групп администрирования

На каждую группу администрирования, соответствующую офису, нужно назначить один или несколько агентов обновлений. Агентами обновлений нужно назначать устройства удаленного офиса, имеющие достаточно места на диске (см. раздел "Оценка места на диске для агента обновлений" на стр. 404). Устройства, размещенные, например, в группе **Офис 1**, будут обращаться к агентам обновлений, назначенным на группу администрирования **Офис 1**.

Если некоторые пользователи физически перемещаются между офисами с ноутбуками, нужно в каждом удаленном офисе дополнительно к упомянутым выше агентам обновлений выбрать два и или более устройств и назначить их агентами обновлений на группу администрирования верхнего уровня (группа **Корневая группа для офисов** на рисунке выше).

Например, имеется ноутбук, размещенный в группе администрирования **Офис 1**, но физически переехавший в офис, соответствующий группе **Офис 2**. После перемещения Агент администрирования на ноутбуке попытается обратиться к агентам обновлений, назначенным на группу **Офис 1**, но эти агенты обновлений окажутся недоступны. Тогда Агент администрирования начнет обращаться к агентам обновлений, назначенным на группу **Корневая группа для офисов**. Так как удаленные офисы изолированы друг от друга, то из всех агентов обновлений, назначенных на группу администрирования **Корневая группа для офисов**, успешными будут лишь обращения к агентам обновлений, назначенным на группу **Офис 2**. То есть ноутбук, оставаясь в группе администрирования, соответствующей своему исходному офису, будет, тем не менее, использовать агента обновлений того офиса, в котором в данный момент находится физически.

Назначение устройства агентом обновлений и настройка шлюза соединений

Вы можете управлять устройствами организации-клиента, не имеющими прямой связи с виртуальным Сервером администрирования, через шлюз соединений.

Вы также можете вручную назначить устройство агентом обновлений для группы администрирования и настроить его как шлюз соединений в Консоли администрирования.

► *Чтобы назначить устройство агентом обновлений группы администрирования, выполните следующие действия:*

1. В дереве консоли выберите узел **Сервер администрирования**.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования в разделе **Агенты обновлений** нажмите на кнопку **Добавить**.

   В результате откроется окно **Добавление агента обновлений**.
4. В окне **Добавление агента обновлений** выполните следующие действия:

   a. Выберите устройство, которое будет выполнять роль агента обновлений, раскрыв список с помощью кнопки  , расположенной справа от кнопки **Добавить**. Доступны следующие способы добавления устройства:

- **Добавить устройство из группы**. Добавление устройства из папки **Управляемые устройства**.
- **Добавить шлюз соединений, находящийся в демилитаризованной зоне, по адресу**. Ввод адреса шлюза соединений.

  > Этот вариант следует использовать для добавления в качестве агента обновлений устройства, защищенного сетевым экраном, поскольку его невозможно напрямую включить в группу администрирования.

  При выборе устройства учитывайте особенности работы агентов обновлений и требования к устройству, которое выполняет роль агента обновлений.

b. Укажите набор устройств, на которые агент обновлений будет распространять обновления. Вы можете указать группу администрирования или описание сетевого местоположения.

5. Нажмите на кнопку **ОК**.

Добавленный агент обновлений отобразится в списке агентов обновлений в разделе **Агенты обновлений**.

> Первое устройство с установленным Агентом администрирования, которое подключится к виртуальному Серверу, будет автоматически назначено агентом обновлений и настроено в качестве шлюза соединений.

В результате добавления агента обновлений по IP-адресу Сервер администрирования обнаружит его при очередном сканировании сети и поместит в папку **Нераспределенные устройства**. Поскольку агент обновлений защищен межсетевым экраном, для его настройки требуется выполнить следующие действия:

1. Добавить это устройство в выбранную группу администрирования.
2. Снова открыть окно свойств Сервера администрирования на разделе **Агенты обновлений**.
3. Удалить устройство, добавленное по адресу, из списка агентов обновлений.

4. Добавить это же устройство из папки **Управляемые устройства** с помощью кнопки **Добавить** или **Добавить устройство из группы**.

5. В окне свойств этого агента обновлений в разделе **Дополнительно** проверить, установлены ли флажки **Шлюз соединений** и **Инициировать создание соединения с шлюзом со стороны Сервера администрирования**.

Локальная установка Агента администрирования на устройство, выбранное агентом обновлений

Чтобы устройство, выбранное агентом обновлений, могло напрямую связаться с виртуальным Сервером администрирования для выполнения роли шлюза соединений, на это устройство требуется локально установить Агент администрирования.

Порядок локальной установки Агента администрирования на устройство, выбранное агентом обновлений, совпадает с порядком локальной установки Агента администрирования на любое устройство сети.

Для устройства, выбранного агентом обновлений, должны быть выполнены следующие условия:

- В процессе локальной установки Агента администрирования в окне мастера установки **Сервер администрирования** в поле **Адрес сервера** требуется указать адрес виртуального Сервера администрирования, под управлением которого находится устройство. В качестве адреса устройства можно использовать IP-адрес или имя устройства в сети Windows.

  Используется следующая форма записи адреса виртуального Сервера: <Полный адрес физического Сервера администрирования, которому подчинен виртуальный Сервер>/<Имя виртуального Сервера администрирования>.

- Для выполнения роли шлюза соединений на устройстве должны быть открыты все порты, необходимые для связи с Сервером администрирования.

В результате установки на устройство Агента администрирования с указанными параметрами программа Kaspersky Security Center автоматически выполняет следующие действия:

- включает это устройство в группу **Управляемые устройства** виртуального Сервера администрирования;
- назначает это устройство агентом обновлений группы **Управляемые устройства** виртуального Сервера администрирования.

Необходимо и достаточно выполнить локальную установку Агента администрирования на устройстве, назначенное агентом обновлений группы **Управляемые устройства** в сети организации. На устройства, выполняющие роль агентов обновлений во вложенных группах администрирования, Агент администрирования можно установить удаленно, используя агент обновлений группы **Управляемые устройства** в качестве шлюза соединений.

См. также

Локальная установка Агента администрирования 300

Удаленная установка программ 265

Использование агента обновлений в качестве шлюза соединений

Если Сервер администрирования находится вне демилитаризованной зоны (DMZ), Агенты администрирования, находящиеся в демилитаризованной зоне, теряют возможность соединения с ним.

Для соединения Сервера администрирования с Агентами администрирования в качестве шлюза соединений можно использовать агент обновлений. Агент обновлений предоставляет Серверу администрирования порт для создания соединения. В момент запуска Сервер администрирования подключается к агенту обновлений и не разрывает соединение с ним в течение всего времени работы.

Получив сигнал от Сервера администрирования, агент обновлений посылает Агентам администрирования UDP-сигнал на подключение к Серверу администрирования. При

получении сигнала Агенты администрирования подключаются к агенту обновлений, который передает информацию между ними и Сервером администрирования.

Рекомендуется использовать в качестве шлюз соединений выделенное устройство и назначать на один шлюз соединений не более 500 клиентских устройств.

См. также

Назначение устройства агентом обновлений и настройка шлюза соединений..... 204

Локальная установка Агента администрирования 300

Создание иерархии групп администрирования, подчиненных виртуальному Серверу администрирования

После создания виртуального Сервера администрирования он по умолчанию содержит группу администрирования **Управляемые устройства**.

Процедура создания иерархии групп администрирования, подчиненных виртуальному Серверу администрирования, совпадает с процедурой создания иерархии групп администрирования, подчиненных физическому Серверу администрирования (см. раздел "Агент администрирования. Группа администрирования" на стр. 34).

В состав групп администрирования, подчиненных виртуальному Серверу администрирования, нельзя добавлять подчиненные и виртуальные Серверы администрирования. Это связано с ограничениями виртуальных Серверов администрирования (см. раздел "Агент администрирования. Группа администрирования" на стр. 34).

Иерархия политик, использование профилей политик

В этом разделе содержится информация об особенностях применения политик к устройствам в группах администрирования. В разделе также содержится информация о профилях политик, которые поддерживаются в Kaspersky Security Center начиная с версии 10 Service Pack 1.

В этом разделе

Иерархия политик

В Kaspersky Security Center политики предназначены для задания одинакового набора параметров на множестве устройств. Например, областью действия политики программы P, определенной для группы G, являются управляемые устройства с установленной программой P, размещенные в группе администрирования G и всех ее подгруппах, исключая те подгруппы, в свойствах которых снят флажок **Наследовать из родительской группы**.

Политика отличается от локальных параметров наличием "замков" возле содержащихся в ней параметров. Установленный "замок" в свойствах политики означает, что соответствующий ему параметр (или группа параметров) должен, во-первых, быть использован при формировании эффективных параметров, во-вторых, должен быть записан в нижележащую политику.

Формирование на устройстве действующих параметров можно представить следующим образом: из политики берутся значения параметров с неустановленным "замком", затем поверх них записываются значения локальных параметров, затем поверх полученных значений записываются взятые из политики значения параметров с установленным "замком".

Политики одной и той же программы действуют друг на друга по иерархии групп администрирования: параметры с установленным "замком" из вышележащей политики переписывают одноименные параметры из нижележащей политики.

Существует особый вид политики – политика для автономных пользователей. Эта политика вступает в силу на устройстве, когда устройство переходит в автономный режим. Политики для автономных пользователей не действуют по иерархии групп администрирования на другие политики.

> Политика для автономных пользователей не будет поддерживаться в будущих версиях Kaspersky Security Center. Вместо политик для автономных пользователей следует использовать профили политик.

Профили политик

Применение политик к устройствам исходя только из иерархии групп администрирования во многих случаях неудобно. Может возникнуть необходимость создать в разных группах администрирования нескольких копий политики, отличающихся одним-двумя параметрами, и в дальнейшем вручную синхронизировать содержимое этих политик.

Во избежание подобных проблем в Kaspersky Security Center, начиная с версии 10 Service Pack 1, поддерживаются *профили политики*. Профиль политики представляет собой именованное подмножество параметров политики, которое распространяется на устройства вместе с политикой и дополняет политику при выполнении некоторого условия – *условия активации профиля*. Профили содержат только те параметры, которые отличаются от "базовой" политики, действующей на клиентском устройстве (компьютере, мобильном устройстве). При активации профиля изменяются параметры политики, действовавшие на устройстве до активации профиля. Эти параметры принимают значения, указанные в профиле.

Профили политик сейчас имеют следующие ограничения:

- в политике может быть не более 100 профилей;
- профиль политики не может содержать другие профили;
- профиль политики не может содержать параметры уведомлений.

Состав профиля

Профиль политики содержит следующие составные части:

- Имя. Профили с одинаковыми именами действуют друг на друга по иерархии групп администрирования с общим правилами.
- Подмножество параметров политики. В отличие от политики, где содержатся все параметры, в профиле присутствуют лишь те параметры, которые действительно нужны (на которых установлен "замок").
- Условие активации – логическое выражение над свойствами устройства. Профиль активен (дополняет политику), только когда условие активации профиля становится истинным. В остальных случаях профиль неактивен и игнорируется. В логическом выражении могут участвовать следующие свойства устройства:
  - состояние автономного режима;
  - свойства сетевого окружения – имя активного правила подключения Агента администрирования (см. раздел "Настройка профилей соединения для автономных пользователей" на стр. 311);
  - наличие или отсутствие у устройства указанных тегов;
  - местоположение устройства в подразделении Active Directory: явное (устройство находится непосредственно в указанном подразделении) или неявное (устройство находится в подразделении, которое находится внутри указанного подразделения на любом уровне вложенности);
  - членство устройства в группе безопасности Active Directory (явное или неявное);
  - членство владельца устройства в группе безопасности Active Directory (явное или неявное).
- Флажок отключения профиля. Отключенные профили всегда игнорируются, условия их активации не проверяются на истинность.
- Приоритет профиля. Условия активации профилей независимы, поэтому одновременно могут активироваться сразу несколько профилей. Если активные профили содержат непересекающиеся наборы параметров, то никаких проблем не

возникает. Но если два активных профиля содержат разные значения одного и того же параметра, возникает неоднозначность. Неоднозначность устраняется при помощи приоритетов профилей: значение неоднозначной переменной будет взято из профиля с большим приоритетом (из того профиля, который располагается выше в списке профилей).

Поведение профилей при действии политик друг на друга по иерархии

Одноименные профили объединяются согласно правилам объединения политик. Профили верхней политики приоритетнее профилей нижней политики. Если в "верхней" политике запрещено изменение параметров (кнопка "замок" нажата), в "нижней" политике используются условия активации профиля из "верхней" политики. Если в "верхней" политике разрешено изменение параметров, то используются условия активации профиля из "нижней" политики.

Поскольку профиль политики может в условии активации содержать свойство **Устройство в автономном режиме**, профили полностью заменяют функциональность политик для автономных пользователей, которая в дальнейшем не будет поддерживаться.

Политика для автономных пользователей может содержать профили, но активация ее профилей может произойти не ранее, чем устройство перейдет в автономный режим.

Задачи

В зависимости от области действия задачи, в Kaspersky Security Center можно выделить следующие виды задач:

- Локальные задачи. Создаются непосредственно на управляемых устройствах. Локальные задачи могут быть изменены не только администратором средствами Консоли администрирования, но и пользователем удаленного устройства (например, в интерфейсе программы защиты). Если локальная задача была изменена одновременно и администратором, и пользователем на управляемом устройстве, то вступят в силу изменения, внесенные администратором как более приоритетные.

- Групповые задачи. Действуют на группу администрирования и все ее подгруппы. Групповые задачи также действуют (опционально) и на устройства, подключенные к размещенным в этой группе и подгруппах подчиненным и виртуальным Серверам администрирования.

- Задачи для наборов устройств. Действуют на ограниченный набор устройств, указанный при создании задачи.

- Задачи для выборок устройств. Действуют на устройства, входящие в указанную выборку. С течением времени область действия задачи изменяется по мере того, как изменяется множество устройств, входящих в выборку. Выборка устройств может быть построена на основе атрибутов устройств, в том числе на основе установленного на устройстве программного обеспечения, а также на основе присвоенных устройству тегов. Выборка является наиболее гибким способом задания области действия задачи.

  > Запуск по расписанию задач для выборок устройств всегда осуществляет Сервер администрирования. Такие задачи не запустятся на устройствах, не имеющих связи с Сервером администрирования. Задачи будут запускаться не по локальному времени устройства, а по локальному времени Сервера администрирования.

- Задачи кластера (массива серверов). Действуют на узлы данного кластера или массива серверов.

Правила перемещения устройств

Размещение устройств в группах администрирования целесообразно автоматизировать при помощи *правил перемещения устройств*. Правило перемещения состоит из трех основных частей: имени, условия выполнения (логического выражения над атрибутами устройства) и целевой группы администрирования. Правило перемещает устройство в целевую группу администрирования, если атрибуты устройства удовлетворяют условию выполнения правила.

Правила перемещения устройств имеют приоритеты. Сервер администрирования проверяет атрибуты устройства на соответствие условию выполнения каждого правила, в порядке убывания приоритета правил. Если атрибуты устройства удовлетворяют условию выполнения правила, то устройство перемещается в целевую группу, и на этом обработка правил для данного устройства прекращается. Если атрибуты устройства удовлетворяют сразу нескольким правилам, то устройство будет перемещено в целевую группу того правила, которое имеет больший приоритет (стоит в списке правил выше).

Правила перемещения устройств могут создаваться неявно. Например, в свойствах пакета или задачи удаленной установки может быть указана группа администрирования, в которую должно попасть устройство после установки на нем Агента администрирования. Также правила перемещения могут быть созданы администратором Kaspersky Security Center в явном виде, в списке правил перемещения. Список расположен в Консоли администрирования в свойствах группы **Нераспределенные устройства.**

Правило перемещения по умолчанию предназначено для однократного первоначального размещения устройств в группах администрирования. Правило перемещает только один раз устройства, находящиеся в группе **Нераспределенные устройства**. Если устройство однажды было перемещено этим правилом, правило не переместит его повторно, даже если вернуть устройство вручную в группу **Нераспределенные устройства**. Это рекомендуемый способ использования правил перемещения.

Можно перемещать устройства, уже размещенные в группах администрирования. Для этого в свойствах правила нужно снять флажок **Перемещать только устройства, не размещенные в группах администрирования**.

Наличие правил перемещения, действующих на устройства, уже размещенные в группах администрирования, существенно увеличивает нагрузку на Сервер администрирования.

Можно создать правило перемещения, способное многократно действовать на одно и то же устройство.

Настоятельно рекомендуется избегать подхода к работе с управляемыми устройствами, при котором одно и то же устройство многократно перемещается из группы в группу, например, с целью применения к устройству особой политики, запуска специальной групповой задачи, обновления с определенного агента обновлений.

Подобные сценарии не поддерживаются, так как они крайне неэффективны по нагрузке на Сервер администрирования и по сетевому трафику, а также противоречат модели работы Kaspersky Security Center (особенно в области прав доступа, событий и отчетов). Следует искать другое решение, например, использовать профили политик (на стр. 210), задачи для выборок устройств (см. раздел "Задачи" на стр. 212), назначать агенты обновлений согласно методике (см. раздел "Построение структуры групп администрирования и назначение агентов обновлений" на стр. 201) и так далее.

Категоризация программного обеспечения

Основным средством контроля запуска приложений являются *категории "Лаборатории Касперского"* (далее также *KL-категории*). KL-категории облегчают администратору Kaspersky Security Center работу по поддержанию категоризации ПО и минимизируют объем трафика, передаваемого на управляемые устройства.

Пользовательские категории следует создавать только для программ, не подпадающих ни под одну KL-категорию (например, для программ, разработанных на заказ). Пользовательские категории создаются на основе дистрибутива программы (MSI) или на основе папки с дистрибутивами.

В случае если имеется большая пополняемая коллекция программного обеспечения, не категоризированного при помощи KL-категорий, может быть целесообразным создать автоматически обновляемую категорию. Такая категория будет автоматически пополняться контрольными суммами исполняемых файлов при изменении папки с дистрибутивами.

Нельзя создавать автоматически обновляемые категории программного обеспечения на основе папок Мои документы, %windir%, %ProgramFiles%. Файлы в этих папках часто меняются, что приводит к увеличению нагрузки на Сервер администрирования и к увеличению трафика в сети. Следует создать отдельную папку с коллекцией программного обеспечения и время от времени пополнять ее.

Необходимые условия для установки программ на устройства организации-клиента

Процесс удаленной установки программ на устройства организации-клиента совпадает с процессом удаленной установки программ внутри организации (см. раздел "Удаленная установка программ" на стр. 265).

Для установки программ на устройства организации-клиента необходимо выполнение следующих условий:

- Перед первой установкой программ на устройства организации-клиента требуется установить на них Агент администрирования.

  При настройке инсталляционного пакета Агента администрирования сервис-провайдером в программе Kaspersky Security Center в окне свойств инсталляционного пакета требуется настроить следующие параметры:

  - В разделе **Подключение** в строке **Адрес сервера** требуется указать тот же адрес виртуального Сервера администрирования, что и при локальной установке Агента администрирования на агент обновлений.

  - В разделе **Дополнительно** требуется установить флажок **Подключаться к Серверу администрирования через шлюз соединений**. В строке **Адрес шлюза соединений** нужно указать адрес агента обновлений. В качестве адреса устройства можно использовать IP-адрес или имя устройства в сети Windows.

- В качестве способа загрузки инсталляционного пакета Агента администрирования необходимо выбрать **Средствами операционной системы с помощью агентов обновлений**. Выбор способа загрузки осуществляется следующим образом:

  - При установке программ с помощью задач удаленной установки способ загрузки можно выбрать двумя способами:

    - при создании задачи удаленной установки в окне **Параметры**;

    - в окне свойств задачи удаленной установки в разделе **Параметры**.

  - При установке программ с помощью мастера удаленной установки способ загрузки можно выбрать в окне мастера **Параметры**.

- Учетная запись, под которой работает агент обновлений, должна иметь доступ к ресурсу Admin$ на клиентских устройствах.

Резервное копирование и восстановление параметров Сервера администрирования

Для резервного копирования параметров Сервера администрирования и используемой им базы данных предусмотрены задача резервного копирования и утилита klbackup. Резервная копия включает в себя все основные параметры и объекты Сервера администрирования: сертификаты Сервера администрирования, ключи для лицензий, структуру групп администрирования со всем содержимым, задачи, политики и так далее. Имея резервную копию, можно восстановить работу Сервера администрирования в кратчайшие сроки – от десятков минут до двух часов.

Ни в коем случае не следует отказываться от регулярного создания резервных копий Сервера администрирования с помощью штатной задачи резервного копирования.

В случае отсутствия резервной копии сбой может привести к безвозвратной потере сертификатов и всех параметров Сервера администрирования. Это повлечет необходимость заново настраивать Kaspersky Security Center, а также заново выполнять первоначальное развертывание Агента администрирования в сети организации.

Мастер первоначальной настройки программы создает задачу резервного копирования параметров Сервера администрирования с ежедневным запуском в четыре часа ночи. Резервные копии по умолчанию сохраняются в папке %ALLUSERSPROFILE%\Application Data\KasperskySC.

Если в качестве СУБД используется экземпляр Microsoft SQL Server, установленный на другом устройстве, следует изменить задачу резервного копирования: указать в качестве папки для хранения сделанных резервных копий UNC-путь, доступный на запись как службе Сервера администрирования, так и службе SQL Server. Это неочевидное требование является следствием особенности резервного копирования в СУБД Microsoft SQL Server.

Если в качестве СУБД используется локальный экземпляр Microsoft SQL Server, также целесообразно сохранять резервные копии на отдельном носителе, чтобы обезопасить их от повреждения одновременно с Сервером администрирования.

> Поскольку резервная копия содержит важные данные, в задаче резервного копирования и в утилите klbackup предусмотрена защита резервных копий паролем. По умолчанию задача резервного копирования создается с пустым паролем. Следует обязательно задать пароль в свойствах задачи резервного копирования. Несоблюдение этого требования приведет к тому, что ключи сертификатов Сервера администрирования и ключи для лицензий окажутся незашифрованными.

Помимо регулярного резервного копирования, следует также создавать резервную копию перед всеми значимыми изменениями, в том числе перед обновлением Сервера администрирования до новой версии и перед установкой патчей Сервера администрирования.

Для уменьшения размеров резервных копий целесообразно установить флажок **Сжимать резервные копии** (**Compress backup**) в параметрах SQL Server.

Восстановление из резервной копии выполняется с помощью утилиты klbackup на только что установленном и работоспособном экземпляре Сервера администрирования той версии, для которой была сделана резервная копия (или более новой).

Инсталляция Сервера администрирования, на которую выполняется восстановление, должна использовать СУБД того же типа (тот же SQL Server или MySQL) той же самой или более новой версии. Версия Сервера администрирования может быть той же самой (с аналогичным или более новым патчем) или более новой.

В этом разделе описаны типовые сценарии восстановления параметров и объектов Сервера администрирования.

В этом разделе

Использование снимка файловой системы для уменьшения времени резервного копирования

В Kaspersky Security Center 10 уменьшено по сравнению с более ранними версиями время простоя Сервера администрирования во время резервного копирования данных. Кроме того, в параметры задачи добавлена функция **Использовать снимок файловой системы при создании резервной копии данных**. Эта функция позволяет дополнительно уменьшить время простоя за счет того, что утилита klbackup создает при выполнении резервного копирования теневую копию диска (это занимает несколько секунд) и одновременно производит копирование базы данных (это занимает не более нескольких минут). Создав теневую копию диска и сделав копию базы данных, klbackup снова делает Сервер администрирования доступным для соединения.

Вы можете пользоваться функцией создания снимка файловой системы только при соблюдении двух условий:

- Папка общего доступа Сервера администрирования и папка %ALLUSERSPROFILE%\KasperskyLab находятся на одном логическом диске и локальны по отношению к Серверу администрирования.
- Внутри папки %ALLUSERSPROFILE%\KasperskyLab нет созданных вручную символических ссылок.

Не используйте функцию, если хотя бы одно из этих условий не выполняется. В ответ на попытку создать снимок файловой системы программа выдаст сообщение об ошибке.

Для использования функции необходимо иметь учетную запись с правами на создание снимков логического диска, на котором расположена папка %ALLUSERSPROFILE%. Учетная запись службы сервера администрирования не имеет таких прав.

► *Чтобы воспользоваться функцией создания снимка файловой системы для уменьшения времени резервного копирования, выполните следующие действия:*

1. В разделе **Задачи** выберите задачу резервного копирования.
2. В контекстном меню выберите пункт **Свойства**.
3. В отобразившемся окне свойств задачи выберите раздел **Параметры**.
4. Установите флажок **Использовать снимок файловой системы при создании резервной копии данных**.
5. В полях **Имя пользователя** и **Пароль** введите имя и пароль от учетной записи, имеющей право на создание снимков логического диска, на котором расположена папка %ALLUSERSPROFILE%.
6. Нажмите на кнопку **Применить**.

При следующих запусках задачи резервного копирования утилита klbackup будет создавать снимки файловой системы, и время простоя Сервера администрирования во время выполнения задачи уменьшится.

Вышло из строя устройство с Сервером администрирования

Если в результате сбоя вышло из строя устройство с Сервером администрирования, рекомендуется выполнить следующие действия:

- Новому Серверу назначить тот же самый адрес: NetBIOS-имя, FQDN-имя, статический IP – смотря по тому, что было задано при развертывании Агентов администрирования.
- Установить Сервер администрирования с использованием СУБД того же типа, той же или более новой версии. Можно установить ту же версию Сервера с тем же или

более новым патчем, или более новую версию. После установки не следует выполнять первоначальную настройку с помощью мастера.

- Из меню **Пуск** запустить утилиту резервного копирования klbackup и выполнить восстановление.

Повреждены параметры Сервера администрирования или база данных

Если Сервер администрирования стал неработоспособен в результате повреждения параметров или базы данных (например, из-за сбоя питания), рекомендуется использовать следующий сценарий восстановления:

1. Выполнить проверку файловой системы на пострадавшем устройстве.
2. Деинсталлировать неработоспособную версию Сервера администрирования.
3. Заново установить Сервер администрирования с использованием СУБД того же типа, той же или более новой версии. Можно установить ту же версию Сервера с тем же или более новым патчем, или более новую версию. После установки не следует выполнять первоначальную настройку с помощью мастера.
4. Из меню **Пуск** запустить утилиту резервного копирования klbackup и выполнить восстановление.

Недопустимо восстанавливать Сервер администрирования любым другим способом кроме штатной утилиты klbackup.

Во всех случаях восстановления Сервера с помощью стороннего программного обеспечения неизбежно произойдет рассинхронизация данных на узлах распределенной программы Kaspersky Security Center и, как следствие, неправильная работа программы.

Развертывание Агента администрирования и программы защиты

Для управления устройствами организации требуется установить на устройства Агент администрирования. Развертывание распределенного приложения Kaspersky Security Center на устройствах организации обычно начинается с установки на них Агента администрирования.

В этом разделе

Первоначальное развертывание

Если на устройстве уже установлен Агент администрирования, удаленная инсталляция приложений на такое устройство осуществляется с помощью самого Агента администрирования. При этом передача дистрибутива устанавливаемого приложения

вместе с заданными администратором инсталляционными параметрами осуществляется по каналам связи между Агентами администрирования и Сервером администрирования. Для передачи дистрибутива можно использовать промежуточные центры распространения в виде агентов обновлений, многоадресную рассылку и так далее. Подробные сведения об установке приложений на управляемые устройства, на которых уже установлен Агент администрирования, см. далее в этом разделе.

Первоначальную установку Агента администрирования на устройства на платформе Microsoft Windows можно осуществлять следующими способами:

- С помощью сторонних средств удаленной установки приложений.
- Путем клонирования образа жесткого диска с операционной системой и установленным Агентом администрирования: средствами, предоставляемыми Kaspersky Security Center для работы с образами дисков, или сторонними средствами.
- Через механизм групповых политик Microsoft Windows: с помощью штатных средств управления групповыми политиками Microsoft Windows или автоматизированно, с помощью соответствующей опции в задаче удаленной установки приложений Kaspersky Security Center.
- Принудительно с помощью соответствующих опций в задаче удаленной установки приложений Kaspersky Security Center.
- Путем рассылки пользователям устройств ссылок на автономные пакеты, сформированные Kaspersky Security Center. Автономные пакеты представляют собой исполняемые модули, содержащие в себе дистрибутивы выбранных программ с настроенными параметрами.
- Вручную, запуская инсталляторы программ на устройствах.

На платформах, отличных от Microsoft Windows, первоначальную установку Агента администрирования на управляемых устройствах следует осуществлять имеющимися сторонними средствами. Обновлять Агент администрирования до новой версии, а также устанавливать другие приложения "Лаборатории Касперского" на этих платформах можно с помощью задач удаленной установки приложений, используя уже имеющиеся на устройствах Агенты администрирования. Установка в этом случае происходит аналогично установке на платформе Microsoft Windows.

Выбирая способ и стратегию развертывания программ в управляемой сети, следует принимать во внимание ряд факторов (неполный список):

- конфигурацию сети организации (см. раздел "Типовые конфигурации Kaspersky Security Center" на стр. 89);
- общее количество устройств;
- наличие в сети организации устройств, не являющихся членами доменов Active Directory, и наличие унифицированных учетных записей с административными правами на таких устройствах;
- ширину канала между Сервером администрирования и устройствами;
- характер связи между Сервером администрирования и удаленными подсетями и ширину сетевых каналов внутри таких подсетей;
- используемые на момент начала развертывания параметры безопасности на удаленных устройствах (в частности, использование UAC и режима Simple File Sharing).

В этом разделе

Настройка параметров инсталляторов

Прежде чем приступать к развертыванию в сети программ "Лаборатории Касперского", следует определить параметры инсталляции – те параметры, которые настраиваются в ходе установки программы. При установке Агента администрирования требуется задать по крайней мере адрес для подключения к Серверу администрирования, а возможно и некоторые дополнительные параметры. В зависимости от выбранного способа установки параметры можно задавать различными способами. В простейшем случае (при интерактивной установке вручную на выбранное устройство) необходимые параметры можно задать с помощью пользовательского интерфейса инсталлятора.

Этот способ настройки параметров не подходит для неинтерактивной "тихой" установки программ на группы устройств. В типичном случае администратор должен централизованно

указать значения параметров, которые в дальнейшем могут быть использованы для неинтерактивной установки на выбранные устройства в сети.

Инсталляционные пакеты

Первый и основной способ настройки инсталляционных параметров приложений является универсальным и подходит для всех способов установки приложений: как средствами Kaspersky Security Center, так и с помощью большинства сторонних средств. Этот способ подразумевает создание в Kaspersky Security Center инсталляционных пакетов приложений.

Инсталляционные пакеты создаются следующими способами:

- автоматически из указанных дистрибутивов на основании входящих в их состав *описателей* (файлов с расширением kud, содержащих правила установки и анализа результата и другую информацию);
- из исполняемых файлов инсталляторов или инсталляторов в формате Microsoft Windows Installer (MSI) – для стандартных или поддерживаемых приложений.

Созданные инсталляционные пакеты представляют собой папки с вложенными подпапками и файлами. Помимо исходного дистрибутива, в состав инсталляционного пакета входят редактируемые параметры (включая параметры самого инсталлятора и правила обработки таких ситуаций, как необходимость перезагрузки операционной системы для завершения инсталляции), а также небольшие вспомогательные модули.

Значения параметров инсталляции, специфичные для конкретного поддерживаемого приложения, можно задавать в пользовательском интерфейсе Консоли администрирования при создании инсталляционного пакета. В случае удаленной установки приложений средствами Kaspersky Security Center инсталляционные пакеты доставляются на устройства таким образом, что при запуске инсталлятора приложения ему становятся доступны все заданные администратором параметры. При использовании сторонних средств установки приложений "Лаборатории Касперского" достаточно обеспечить доступность на устройстве всего инсталляционного пакета, то есть дистрибутива и его параметров. Инсталляционные пакеты создаются и хранятся Kaspersky Security Center в соответствующей подпапке папки общего доступа (см. раздел "Задание папки общего доступа" на стр. 122).

Не указывайте в параметрах инсталляционных пакетов данные привилегированных учетных записей.

О том, как именно можно воспользоваться этим способом настройки параметров для приложений "Лаборатории Касперского" перед их развертыванием сторонними средствами, см. в разделе "Развертывание с помощью механизма групповых политик Microsoft Windows (на стр. 231)".

Сразу после установки Kaspersky Security Center автоматически создается несколько инсталляционных пакетов, готовых к установке, в том числе пакеты Агента администрирования и программы защиты для платформы Microsoft Windows.

Несмотря на то, что ключ для лицензии на приложение можно задать в свойствах инсталляционного пакета, желательно не использовать этот способ распространения лицензий из-за широкой доступности инсталляционных пакетов на чтение. Следует использовать автоматически распространяемые ключи или задачи установки ключей.

Свойства MSI и файлы трансформации

Другим способом настроить параметры инсталляции на платформе Windows является задание свойств MSI и файлов трансформации. Этот способ может быть использован в следующих случаях:

- при установке через групповые политики Windows при помощи штатных средств Microsoft или иных сторонних инструментов для работы с групповыми политиками Windows;
- при установке с помощью сторонних средств, ориентированных на работу с инсталляторами в формате Microsoft Installer (см. раздел "Настройка параметров инсталляторов" на стр. 244).

Развертывание при помощи сторонних средств удаленной установки приложений

При наличии в организации каких-либо средств удаленной установки приложений (например, Microsoft System Center) целесообразно выполнять первоначальное развертывание при помощи этих средств.

Нужно выполнить следующие действия:

- Выбрать способ настройки параметров инсталляции, наиболее подходящий для используемого средства развертывания.
- Определить механизм синхронизации между изменением параметров инсталляционных пакетов через интерфейс Консоли администрирования и работой выбранных сторонних средств развертывания приложений из данных инсталляционных пакетов.
- В случае установки из папки общего доступа убедиться в достаточной производительности этого файлового ресурса.

См. также

Задание папки общего доступа 122

Настройка параметров инсталляторов 244

Общие сведения о задачах удаленной установки приложений Kaspersky Security Center

Kaspersky Security Center предоставляет разнообразные механизмы удаленной установки приложений, реализованные в виде задач удаленной установки приложений (принудительная установка, установка с помощью копирования образа жесткого диска, установка с помощью групповых политик Microsoft Windows). Создать задачу удаленной установки можно как для указанной группы администрирования, так и для набора устройств или для выборки устройств (такие задачи отображаются в Консоли администрирования в папке **Задачи**). При создании задачи можно выбрать инсталляционные пакеты (Агента

администрирования и / или другого приложения), подлежащие установке при помощи данной задачи, а также задать ряд параметров, определяющих способ удаленной установки. Кроме того, можно воспользоваться мастером удаленной установки приложений, в основе которого также лежит создание задачи удаленной установки приложений и мониторинг результатов.

> Задачи для групп администрирования действуют не только на устройства, принадлежащие этой группе, но и на все устройства всех подгрупп выбранной группы. Если в параметрах задачи включен соответствующий параметр, задача распространяется на устройства подчиненных Серверов администрирования, расположенных в данной группе или ее подгруппах.

Задачи для наборов устройств актуализируют список клиентских устройств при каждом запуске в соответствии с составом выборки устройств на момент запуска задачи. Если в выборке устройств присутствуют устройства, подключенные к подчиненным Серверам администрирования, задача будет запускаться и на этих устройствах. Подробнее об этих параметрах и способах установки будет рассказано далее в этом разделе.

> Для успешной работы задачи удаленной установки на устройствах, подключенных к подчиненным Серверам администрирования, следует при помощи задачи ретрансляции предварительно ретранслировать используемые задачей инсталляционные пакеты на соответствующие подчиненные Серверы администрирования.

Развертывание захватом и копированием образа жесткого диска устройства

Если нужно инсталлировать Агент администрирования на устройства, на которые также предстоит установить (или переустановить) операционную систему и прочее программное обеспечение, можно воспользоваться механизмом захвата и копирования образа жесткого диска устройства.

Развертывание путем захвата и копирования образа жесткого диска нужно выполнять следующим образом:

1. Создать "эталонное" устройство с установленной операционной системой и необходимым для работы набором программного обеспечения, включая Агент администрирования и программу защиты.

2. Захватить образ "эталонного" устройства и далее распространять этот образ на новые устройства посредством задачи Kaspersky Security Center.

   Для захвата и установки образов диска можно воспользоваться как имеющимися в организации сторонними средствами, так и функциональностью, предоставляемой (при наличии лицензии на Системное администрирование) Kaspersky Security Center (см. раздел "Установка образов операционных систем" на стр. 100).

Если для работы с образами диска используются сторонние инструменты, необходимо при развертывании на устройство из эталонного образа обеспечить удаление информации, с помощью которой Kaspersky Security Center идентифицирует управляемое устройство. В противном случае Сервер администрирования не сможет в дальнейшем корректно различать устройства, созданные путем копирования одного и того же образа.

При захвате образа диска средствами Kaspersky Security Center эта проблема решается автоматически.

Копирование образа жесткого диска сторонними инструментами

При использовании сторонних инструментов для захвата образа устройства с установленным Агентом администрирования следует воспользоваться одним из следующих методов:

- Рекомендуемый метод. При установке Агента администрирования на эталонное устройство выбрать вариант **Не запускать службу по завершении инсталляции** и захватить образ устройства до первого старта службы Агента администрирования (так как уникальная информация, идентифицирующая устройство, создается при первом подключении Агента администрирования к Серверу администрирования). В дальнейшем рекомендуется не допускать запуск службы Агента администрирования вплоть до выполнения операции захвата образа.

- На эталонном устройстве остановить службу Агента администрирования и запустить утилиту klmover с ключом -dupfix. Утилита klmover входит в состав инсталляционного пакета Агента администрирования. В дальнейшем не допускать запуск службы Агента администрирования вплоть до выполнения операции захвата образа.

- Обеспечить запуск утилиты klmover с ключом -dupfix до (это важно) первого запуска службы Агента администрирования на устройствах при первом старте операционной системы после развертывания образа. Утилита klmover входит в состав инсталляционного пакета Агента администрирования.

Если копирование образа жесткого диска было выполнено неправильно, см. раздел "Неверно выполнено копирование образа жесткого диска (на стр. 382)".

Можно применять альтернативный вариант развертывания Агента администрирования на новые устройства с использованием образов операционной системы:

- Захваченный образ не содержит установленный Агент администрирования.

- В список исполняемых файлов, запускаемых по завершении развертывания образа на устройствах, добавлен автономный пакет Агента администрирования, расположенный в папке общего доступа Kaspersky Security Center.

Этот вариант развертывания дает большую гибкость: можно использовать один образ операционной системы совместно с различными вариантами установки Агента и / или программы защиты, включая правила перемещения устройства, связанные с автономным пакетом. При этом несколько усложняется процесс развертывания, требуется обеспечить доступ к сетевой папке с автономными пакетами с устройства (см. раздел "Установка образов операционных систем" на стр. 100).

Развертывание с помощью механизма групповых политик Microsoft Windows

Первоначальное развертывание Агентов администрирования рекомендуется осуществлять с помощью групповых политик Microsoft Windows при выполнении следующих условий:

- устройства являются членами домена Active Directory;

- план развертывания позволяет дождаться штатной перезагрузки устройств до начала развертывания на них Агентов администрирования, или к устройствам можно принудительно применить групповую политику Windows.

Суть данного способа развертывания заключается в следующем:

- Дистрибутив приложения в формате Microsoft Installer (MSI-пакет) размещается в папке общего доступа (в папке, к которой имеют доступ на чтение учетные записи LocalSystem устройств).

- В групповой политике Active Directory создается объект установки данного дистрибутива.

- Область действия установки задается привязкой к organization unit и / или к группе безопасности, в которую входят устройства.

- При очередном входе устройства в домен (до входа в систему пользователей устройства) выполняется проверка наличия требуемого приложения среди установленных приложений. Если приложение отсутствует, происходит загрузка дистрибутива с заданного в политике ресурса и его установка.

Одним из преимуществ этого способа развертывания является то, что назначенные приложения устанавливаются на устройства при загрузке операционной системы еще до входа пользователя в систему. Даже если пользователь, имеющий необходимые права, удалит приложение, при следующей загрузке операционной системы оно будет установлено снова. Недостатком этого способа развертывания является то, что произведенные администратором изменения в групповой политике не вступят в силу до перезагрузки устройств (без применения дополнительных средств).

С помощью групповых политик можно устанавливать как Агент администрирования, так и другие приложения, инсталляторы которых имеют формат Windows Installer.

При выборе этого способа развертывания, помимо прочего, необходимо оценить нагрузку на файловый ресурс, с которого будет осуществляться копирование файлов на устройства при применении групповой политики Windows.

Работа с политиками Microsoft Windows с помощью задачи удаленной установки приложений Kaspersky Security Center

Самым простым способом инсталляции приложений при помощи групповых политик Microsoft Windows является установка флажка **Назначить установку инсталляционного пакета в групповых политиках Active Directory** в свойствах задачи удаленной установки приложений Kaspersky Security Center. В этом случае при запуске задачи Сервер администрирования самостоятельно выполнит следующие действия:

- Создаст необходимые объекты в групповой политике Microsoft Windows.
- Создаст специальные группы безопасности, в которые включит устройства, и назначит установку выбранных приложений для этих групп безопасности. Состав групп безопасности будет актуализироваться при каждом запуске задачи в соответствии с набором устройств на момент запуска.

Для обеспечения работоспособности данной функции следует указать в параметрах задачи учетную запись, имеющую права на редактирование групповых политик Active Directory.

Если с помощью одной задачи предполагается установить и Агент администрирования, и другое приложение, установка флажка **Назначить установку инсталляционного пакета в групповых политиках Active Directory** приведет к созданию в политике Active Directory объекта установки только для Агента администрирования. Второе выбранное в задаче приложение будет устанавливаться уже средствами Агента администрирования, как только он будет установлен на устройстве. Если по какой-то причине необходимо установить отличное от Агента администрирования приложение именно с помощью групповых политик Windows, то нужно создать задачу установки только для этого инсталляционного пакета (без пакета Агента администрирования). Не все приложения могут быть установлены с помощью групповых политик Microsoft Windows. О такой возможности вы можете узнать, обратившись к информации о способах установки приложения.

В случае, когда необходимые объекты создаются в групповой политике средствами Kaspersky Security Center, в качестве источника инсталляционного пакета будет использована папка общего доступа Kaspersky Security Center. При планировании развертывания следует соотнести скорость чтения из этой папки с количеством устройств и размером устанавливаемого дистрибутива. Возможно, будет целесообразно расположить папку общего доступа Kaspersky Security Center в мощном специализированном файловом хранилище (см. раздел "Задание папки общего доступа" на стр. 122).

Помимо простоты, автоматическое создание групповых политик Windows средствами Kaspersky Security Center имеет еще одно преимущество: при планировании установки Агента администрирования легко указать группу администрирования Kaspersky Security Center, в которую будут автоматически перемещаться устройства по завершении установки. Группу можно указать в мастере создания задачи или в окне параметров задачи удаленной установки.

При работе с групповыми политиками Windows средствами Kaspersky Security Center задание устройств для объекта групповой политики осуществляется путем создания группы безопасности. Kaspersky Security Center синхронизирует состав группы безопасности с текущим набором устройств задачи. При использовании иных средств для работы с групповыми политиками можно привязывать объекты групповых политик непосредственно к выбранным подразделениям Active Directory.

Самостоятельная установка приложений с помощью политик Microsoft Windows

Администратор может самостоятельно создать в групповой политике Windows объекты, необходимые для установки. В этом случае можно сослаться на пакеты, лежащие в папке общего доступа Kaspersky Security Center, или выложить пакеты на отдельный файловый сервер и сослаться на них.

Возможны следующие сценарии установки:

- Администратор создает инсталляционный пакет и настраивает его свойства в Консоли администрирования. Объект групповой политики ссылается на msi-файл этого сконфигурированного пакета, лежащего в папке общего доступа Kaspersky Security Center.

- Администратор создает инсталляционный пакет и настраивает его свойства в Консоли администрирования. Затем администратор копирует целиком подпапку EXEC этого пакета из папки общего доступа Kaspersky Security Center в папку на специализированном файловом ресурсе организации. Объект групповой политики ссылается на msi-файл этого сконфигурированного пакета, лежащего в подпапке на специализированном файловом ресурсе организации.

- Администратор загружает дистрибутив приложения (в том числе дистрибутив Агента администрирования) из интернета и выкладывает его на специализированный

файловый ресурс организации. Объект групповой политики ссылается msi-файл этого пакета, лежащего в подпапке на специализированном файловом ресурсе организации. Настройка параметров инсталляции осуществляется путем настройки свойств MSI или настройкой файлов трансформации MST (см. раздел "Настройка параметров инсталляторов" на стр. 244).

Принудительное развертывание с помощью задачи удаленной установки приложений Kaspersky Security Center

В случае если требуется начать развертывание Агентов администрирования или других необходимых приложений немедленно, без ожидания очередного входа устройств в домен, или же при наличии устройств, не являющихся членами домена Active Directory, можно использовать принудительную (форсированную) установку выбранных инсталляционных пакетов при помощи задачи удаленной установки приложений Kaspersky Security Center.

Устройства при этом могут задаваться явно (списком) либо выбором группы администрирования Kaspersky Security Center, которой они принадлежат, либо созданием выборки устройств по определенному условию. Момент начала установки определяется расписанием задачи. Если в свойствах задачи включен параметр **Запускать пропущенные задачи**, задача может запускаться сразу при включении устройств или при переносе их в целевую группу администрирования.

Данный способ установки осуществляется путем копирования файлов на административный ресурс admin$ каждого из устройств и удаленной регистрации на них вспомогательных служб. При этом должны выполняться следующие условия:

- Устройства должны быть доступны для подключения либо со стороны Сервера администрирования, либо со стороны агента обновлений.
- В сети должно корректно работать разрешение имен для устройств.
- На управляемых устройствах не должны быть отключены административные ресурсы общего доступа admin$.
- На устройствах должна быть запущена системная служба Server (по умолчанию данная служба запущена).

- На устройствах должны быть открыты следующие порты для удаленного доступа к устройствам средствами Windows: TCP 139, TCP 445, UDP 137, UDP 138.
- На устройствах должен быть выключен режим Simple File Sharing.
- На устройствах модель совместного доступа и безопасности для локальных учетных записей должна находиться в состоянии *Обычная – локальные пользователи удостоверяются как они сами* (*Classic – local users authenticate as themselves*), и ни в коем случае не в состоянии *Гостевая – локальные пользователи удостоверяются как гости* (*Guest only – local users authenticate as Guest*).
- Устройства должны быть членами домена, либо на устройствах должны быть заблаговременно созданы унифицированные учетные записи с административными правами.

Устройства, расположенные в рабочих группах, могут быть приведены в соответствие указанным выше требованиям при помощи утилиты riprep.exe, которая описана на портале Службы технической поддержки "Лаборатории Касперского".

При установке на новые устройства, еще не размещенные в группах администрирования Kaspersky Security Center, в свойствах задачи удаленной установки можно задать группу администрирования, в которую устройства будут перемещаться по завершении установки на них Агента администрирования.

> При создании групповой задачи необходимо помнить, что групповая задача действует на устройства всех вложенных подгрупп выбранной группы. Поэтому не следует дублировать задачи установки в подгруппах.

Можно использовать упрощенный способ создания задач принудительной установки приложений – автоматическую установку. Для этого в свойствах группы администрирования нужно выбрать в списке инсталляционных пакетов те пакеты, которые должны быть установлены на устройствах этой группы. В результате на всех устройствах этой группы и ее подгрупп будут автоматически установлены выбранные инсталляционные пакеты. Период, в течение которого будут установлены пакеты, зависит от пропускной способности сети и общего количества устройств в сети.

Принудительная установка может быть использована и в случае, если устройства не доступны Серверу администрирования непосредственно: например, устройства

расположены в изолированных сетях, или устройства расположены в локальной сети, а Сервер администрирования – в демилитаризованной зоне. Для работоспособности принудительной установки необходимо обеспечить наличие агентов обновлений в каждой такой изолированной сети.

Использование агентов обновлений в качестве локальных центров установки может быть удобно и для установки на устройства в подсетях, соединенных с Сервером администрирования узким каналом связи при наличии широкого канала связи между устройствами внутри подсети. Однако следует учитывать, что данный способ установки создает значительную нагрузку на устройства, назначенные агентами обновлений. Поэтому нужно выбирать в качестве агентов обновлений достаточно мощные устройства с быстрыми накопителями. Также необходимо, чтобы объем свободного места в разделе с папкой *%ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit* многократно превосходил суммарный объем дистрибутивов устанавливаемых приложений (см. раздел "Оценка места на диске для агента обновлений" на стр. 404).

Запуск автономных пакетов, сформированных Kaspersky Security Center

Описанные выше способы первоначального развертывания Агента администрирования и приложений могут быть реализованы не всегда из-за невозможности выполнить все необходимые условия. В таких случаях из подготовленных администратором инсталляционных пакетов с необходимыми параметрами установки средствами Kaspersky Security Center можно создать единый исполняемый файл, который называется *автономным пакетом установки*. Автономный пакет установки размещается в папке общего доступа Kaspersky Security Center.

При помощи Kaspersky Security Center можно разослать по электронной почте выбранным пользователям ссылку на этот файл в папке общего доступа с просьбой запустить файл (интерактивно или с ключом "тихой" установки "-s"). Автономный пакет установки можно прикрепить к сообщению электронной почты для пользователей устройств, не имеющих доступ к папке общего доступа Kaspersky Security Center. Администратор может скопировать автономный пакет на внешнее устройство и доставить пакет на нужное устройство с целью его последующего запуска.

Автономный пакет можно создать из пакета Агента администрирования, пакета другого (например, программы защиты) приложения или сразу из обоих пакетов. Если автономный

пакет создан из Агента администрирования и другого приложения, установка начнется с Агента администрирования.

При создании автономного пакета с Агентом администрирования можно указать группу администрирования, в которую будут автоматически перемещаться новые устройства (ранее не размещенные в группах администрирования) по завершении установки на них Агента администрирования.

Автономные пакеты могут работать интерактивно (по умолчанию), с отображением результата установки входящих в них приложений, или в "тихом" режиме (при запуске с ключом "-s"). "Тихий" режим может быть использован для установки из каких-либо скриптов (например, из скриптов, настраиваемых для запуска по завершении развертывания образа операционной системы, и тому подобное). Результат установки в "тихом" режиме определяется кодом возврата процесса.

Возможности ручной установки приложений

Администраторы или опытные пользователи могут устанавливать приложения вручную в интерактивном режиме. При этом можно использовать как исходные дистрибутивы, так и сформированные из них инсталляционные пакеты, расположенные в папке общего доступа Kaspersky Security Center. Инсталляторы по умолчанию работают в интерактивном режиме, запрашивая у пользователя все необходимые значения параметров. Но при запуске процесса setup.exe из корня инсталляционного пакета с ключом "-s" инсталлятор будет работать в "тихом" режиме с параметрами, заданными при настройке инсталляционного пакета.

> При запуске setup.exe из корня инсталляционного пакета, расположенного в папке общего доступа Kaspersky Security Center, сначала произойдет копирование пакета во временную локальную папку, затем из локальной папки будет запущен инсталлятор приложения.

Управление перезагрузкой устройств в задаче удаленной установки

Часто для завершения удаленной установки приложений (особенно на платформе Windows) требуется перезагрузка устройства.

Если используется задача удаленной установки приложений Kaspersky Security Center, в мастере создания задачи или в окне свойств созданной задачи (раздел **Перезагрузка ОС**) можно выбрать вариант действия при необходимости перезагрузки:

- **Не перезагружать устройство**. В этом случае автоматическая перезагрузка не будет выполнена. Для завершения установки потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами). Информация о необходимости перезагрузки будет сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач установки на серверы и другие устройства, для которых критически важна бесперебойная работа.

- **Перезагрузить устройство**. В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения установки. Этот вариант подходит для задач установки на устройства, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).

- **Спросить у пользователя**. В этом случае на экране клиентского устройства будет выводиться сообщение о том, что устройство должно быть перезагружено вручную. Для этого варианта можно настроить дополнительные параметры: текст сообщения для пользователя, периодичность сообщения, а также время, после которого перезагрузка будет выполнена принудительно (без подтверждения пользователя). Вариант **Спросить у пользователя** наиболее подходит для рабочих станций, пользователи которых должны иметь возможность выбрать наиболее подходящий момент для перезагрузки.

Целесообразность обновления баз в инсталляционном пакете программы защиты

Перед началом развертывания защиты необходимо учитывать возможность обновления антивирусных баз (включая модули автопатчей), распространяемых вместе с дистрибутивом программы защиты. Целесообразно перед началом развертывания принудительно обновить базы в составе инсталляционного пакета приложения (например, с помощью соответствующей команды в контекстном меню выбранного инсталляционного пакета). Это уменьшит количество перезагрузок, требующихся для завершения развертывания защиты на устройствах.

Выбор способа деинсталляции несовместимых приложений при установке программы защиты "Лаборатории Касперского"

Для установки программ защиты "Лаборатории Касперского" средствами Kaspersky Security Center может потребоваться удалить стороннее программное обеспечение, несовместимое с устанавливаемой программой. Существуют два основных способа выполнить эту задачу.

Автоматическое удаление несовместимых программ с помощью инсталлятора

Поддерживается при различных видах установки. Перед установкой программы защиты несовместимые с ней программы удаляются автоматически, если в окне свойств инсталляционного пакета программы защиты (раздел **Несовместимые программы**) установлен флажок **Удалять несовместимые программы автоматически**.

Удаление несовместимых программ с помощью отдельной задачи

Для удаления несовместимых программ используется задача **Удаленная деинсталляция программы**. Задачу следует запускать на устройствах перед задачей установки программы защиты. Например, в задаче установки можно выбрать расписание типа **По завершении другой задачи**, где другой задачей является задача **Удаленная деинсталляция программы**.

Этот способ удаления целесообразно использовать в случаях, если инсталлятор программы защиты не может успешно удалить какую-либо из несовместимых программ.

Использование средств удаленной установки приложений Kaspersky Security Center для запуска на управляемых устройствах произвольных исполняемых файлов

С помощью мастера создания инсталляционного пакета можно выбрать произвольный исполняемый файл и задать для него параметры командной строки. При этом в инсталляционный пакет можно поместить как сам выбранный файл, так и всю папку, в которой этот файл содержится. Затем следует создать задачу удаленной установки и выбрать созданный инсталляционный пакет.

В ходе работы задачи на устройствах будет запущен указанный при создании исполняемый файл с заданными параметрами командной строки.

Если используются инсталляторы в формате Microsoft Windows Installer (MSI), Kaspersky Security Center использует штатные возможности по анализу результата установки.

Если есть лицензия на Системное администрирование, при создании инсталляционного пакета для одного из поддерживаемых приложений, распространенных в корпоративной среде, Kaspersky Security Center также использует правила установки и анализа результатов установки, имеющиеся в его обновляемой базе.

В иных случаях для исполняемых файлов задача по умолчанию дожидается завершения запущенного процесса и всех порожденных им дочерних процессов. По завершении запущенных процессов задача будет завершена успешно независимо от кода возврата исходного процесса. Чтобы изменить такое поведение задачи, перед созданием задачи следует изменить вручную kud-файл, сформированный Kaspersky Security Center в папке созданного инсталляционного пакета.

Для того чтобы задача не ожидала завершения запущенного процесса, в секции [SetupProcessResult] нужно задать значение 0 для параметра Wait:

Пример:

[SetupProcessResult]

Wait=0

Для того чтобы на платформе Windows задача ожидала только завершения исходного процесса, но не порожденных им дочерних процессов, нужно в секции [SetupProcessResult] задать значение 0 для параметра WaitJob, например:

Пример:

[SetupProcessResult]

WaitJob=0

Для того чтобы задача завершалась успешно или с ошибкой в зависимости от кода возврата запущенного процесса, нужно перечислить успешные коды возврата в секции [SetupProcessResult_SuccessCodes], например:

Пример:

[SetupProcessResult_SuccessCodes]

0=

3010=

В этом случае любой код, отличный от перечисленных, будет означать ошибку.

Для того чтобы в результатах задачи отображалась строка с комментарием об успешном завершении задачи или сообщения об ошибках, нужно задать краткие описания ошибок, соответствующих кодам возврата процесса, в секциях [SetupProcessResult_SuccessCodes] и [SetupProcessResult_ErrorCodes], например:

Пример:

[SetupProcessResult_SuccessCodes]

0= Installation completed successfully

3010=A reboot is required to complete the installation

[SetupProcessResult_ErrorCodes]

1602=Installation cancelled by the user

1603=Fatal error during installation

Для того чтобы задействовать средства Kaspersky Security Center по управлению перезагрузкой устройства (если перезагрузка необходима для завершения операции), нужно дополнительно перечислить коды возврата процесса, означающие необходимость перезагрузки, в секции [SetupProcessResult_NeedReboot]:

Пример:

[SetupProcessResult_NeedReboot]

3010=

Мониторинг развертывания

Для контроля развертывания Kaspersky Security Center, а также для контроля наличия на управляемых устройствах программы защиты и Агента администрирования, следует обращать внимание на цветовой индикатор в блоке **Развертывание**. Индикатор расположен в рабочей области узла Сервер администрирования в главном окне Консоли администрирования. Индикатор отображает текущее состояние развертывания. Рядом с индикатором отображается количество устройств с установленными Агентами администрирования и программами защиты. При наличии активных задач установки отображается прогресс выполнения задач. При наличии ошибок установки отображается

количество ошибок с возможностью просмотреть детальную информацию об ошибке по ссылке.

Также можно воспользоваться диаграммой развертывания в рабочей области папки **Управляемые устройства** на закладке **Группы**. Диаграмма отражает процесс развертывания: количество устройств без Агента администрирования, с Агентом администрирования, с Агентом администрирования и программой защиты.

Более детальное описание хода развертывания (или работы конкретной задачи установки) можно увидеть в окне результатов выполнения соответствующей задачи удаленной установки. Окно результатов доступно из контекстного меню задачи (пункт **Результаты**). В окне отображаются два списка: в верхнем списке содержится список состояний задачи на устройствах, а в нижнем – список событий задачи на устройстве, которое в данный момент выбрано в верхнем списке.

Информация об ошибках при развертывании записываются в Kaspersky Event Log Сервера администрирования. Информация об ошибках также доступна в соответствующей выборке событий в узле Сервера администрирования на закладке **События**.

Настройка параметров инсталляторов

В разделе содержится информация о файлах инсталляторов Kaspersky Security Center и параметрах установки, а также рекомендации по установке Сервера администрирования и Агента администрирования в "тихом" режиме.

В этом разделе

Общая информация

Инсталляторы компонентов Kaspersky Security Center 10 – Сервера администрирования, Агента администрирования, Консоли администрирования – построены на технологии Windows Installer. Ядром инсталлятора является msi-пакет. Этот формат упаковки дистрибутива позволяет использовать все преимущества технологии Windows Installer: масштабируемость, возможность использовать систему патчевания, систему трансформации, возможность установки централизованно сторонними решениями, прозрачность регистрации в операционной системе.

Установка в тихом режиме (с файлом ответов)

В инсталляторах Сервера администрирования и Агента администрирования реализована возможность работы с файлом ответов (ss_install.xml), в котором записаны параметры для установки в тихом режиме без участия пользователя. Файл ss_install.xml расположен в той же папке, что и msi-пакет, и используется автоматически при установке в тихом режиме. Тихий режим установки включается ключом командной строки "/s".

Пример запуска:

```
setup.exe /s
```

Файл ss_install.xml представляет собой внутренний формат параметров инсталлятора Kaspersky Security Center. В составе дистрибутивов поставляется файл ss_install.xml с параметрами по умолчанию.

Не следует изменять файл ss_install.xml вручную. Этот файл изменяется средствами Kaspersky Security Center при изменении параметров установочных пакетов в Консоли администрирования.

Установка в тихом режиме (без файла ответов)

Агент администрирования можно установить при помощи одного только msi-пакета, задавая при этом значения свойств MSI стандартным образом. Такой сценарий позволяет устанавливать Агент администрирования, используя групповые политики. Для того чтобы не возникал конфликт между параметрами, заданными с помощью свойств MSI, и параметрами, заданными в файле ответов, предусмотрена возможность отключения файла ответов путем задания свойства DONT_USE_ANSWER_FILE=1. Ниже приведен пример запуска инсталлятора Агента администрирования с помощью msi-пакета.

Пример:

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

Также параметры инсталляции msi-пакета можно задать, подготовив предварительно файл трансформации (файл с расширением mst). Команда будет выглядеть следующим образом:

Пример:

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

В одной команде можно указать более одного файла трансформации.

Частичная настройка параметров установки через setup.exe

Запуская установку программ через setup.exe, можно передавать в msi-пакет значения любых свойств MSI.

Команда будет выглядеть следующим образом:

Пример:

/v"PROPERTY_NAME1=PROPERTY_VALUE1 PROPERTYNAME2=PROPERTYVALUE2"

Параметры установки Сервера администрирования

В таблице ниже описаны свойства MSI, которые можно настраивать при установке Сервера администрирования. Все параметры являются опциональными, кроме EULA и PRIVACYPOLICY.

Таблица 28. Параметры установки Сервера администрирования в неинтерактивном режиме

Свойство MSI	Описание	Возможные значения
EULA	Согласие с условиями лицензии (обязательный параметр).	• 1 – согласны с условиями Лицензионного соглашения. • Другое значение или не задано – не согласны с условиями Лицензионного соглашения (установка не выполняется).
PRIVACYPOLICY	Согласие с условиями Политики конфиденциальности (обязательный параметр).	• 1 – согласны с условиями Политики конфиденциальности. • Другое значение или не задано – не согласны с условиями Политики конфиденциальности (установка не выполняется).
INSTALLATIONMODETYPE	Тип установки Сервера администрирования.	• Стандартная. • Выборочная.

Свойство MSI	Описание	Возможные значения
INSTALLDIR	Папка установки программы.	Строковое значение.
ADDLOCAL	Список компонентов для установки (через запятую).	CSAdminKitServer, NAgent, CSAdminKitConsole, NSAC, MobileSupport, KSNProxy, SNMPAgent, GdiPlusRedist, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86. Минимальный достаточный для корректной установки Сервера администрирования список компонентов: `ADDLOCAL=CSAdminKitServer,CSAdminKitConsole,KSNProxy,Microsoft_VC90_CRT_x86,Microsoft_VC100_CRT_x86`
NETRANGETYPE	Размер сети.	• NRT_1_100 – от 1 до 100 устройств. • NRT_100_1000 – от 100 до 1000 устройств. • NRT_GREATER_1000 – более 1000 устройств.
SRV_ACCOUNT_TYPE	Способ задания пользователя для работы службы Сервера администрирования.	• SrvAccountDefault – учетная запись пользователя будет создана автоматически. • SrvAccountUser – учетная запись пользователя задана вручную.

Свойство MSI	Описание	Возможные значения
SERVERACCOUNTNAME	Имя пользователя для службы.	Строковое значение.
SERVERACCOUNTPWD	Пароль пользователя для службы.	Строковое значение.
DBTYPE	Тип базы данных.	• MySQL. • MSSQL.
MYSQLSERVERNAME	Полное имя mysql-сервера.	Строковое значение.
MYSQLSERVERPORT	Номер порта для подключения к mysql-серверу.	Числовое значение.
MYSQLDBNAME	Имя базы данных mysql-сервера.	Строковое значение.

Свойство MSI	Описание	Возможные значения
MYSQLACCOUNTNAME	Имя пользователя для подключения к базе mysql-сервера.	Строковое значение.
MYSQLACCOUNTPWD	Пароль пользователя для подключения к базе mysql-сервера.	Строковое значение.
MSSQLCONNECTIONTYPE	Тип использования базы данных MSSQL.	• InstallMSSEE – инсталлировать из пакета. • ChooseExisting –использовать установленный сервер.
MSSQLSERVERNAME	Полное имя экземпляра SQL Server.	Строковое значение.

Свойство MSI	Описание	Возможные значения
MSSQLDBNAME	Имя базы данных SQL Server.	Строковое значение.
MSSQLAUTHTYPE	Способ аутентификации при подключении к SQL Server.	• Windows. • SQLServer.
MSSQLACCOUNTNAME	Имя пользователя для подключения к SQL Server в режиме SQLServer.	Строковое значение.

Свойство MSI	Описание	Возможные значения
MSSQLACCOUNTPWD	Пароль пользователя для подключения к SQL Server в режиме SQLServer.	Строковое значение.

CREATE_SHARE_TYPE	Способ задания папки общего доступа.	• Create – создать новую папку общего доступа. В этом случае должны быть заданы свойства:
		  • SHARELOCALPATH – путь к локальной папке.
		  • SHAREFOLDERNAME – сетевое имя папки.
		• Пусто – должно быть задано свойство EXISTSHAREFOLDERNAME.

EXISTSHAREFOLDERNAME	Полный путь к существующей папке общего доступа.	Строковое значение.

Свойство MSI	Описание	Возможные значения
SERVERPORT	Номер порта для подключения к Серверу администрирования.	Числовое значение.
SERVERSSLPORT	Номер порта для установки SSL-соединения с Сервером администрирования.	Числовое значение.
SERVERADDRESS	Адрес Сервера администрирования.	Строковое значение.

Свойство MSI	Описание	Возможные значения
SERVERCERT2048BITS	Длина ключа для сертификата Сервера администрирования (в битах).	• 1 – длина ключа для сертификата Сервера администрирования составляет 2048 бит. • 0 – длина ключа для сертификата Сервера администрирования составляет 1024 бит. • Если параметр не задан, длина ключа для сертификата Сервера администрирования составляет 1024 бит.
MOBILESERVERADDRESS	Адрес Сервера администрирования для подключения мобильных устройств; игнорируется, если не выбран компонент MobileSupport.	Строковое значение.

См. также:

Параметры установки Агента администрирования 256

Установка Агента администрирования в неинтерактивном режиме 302

Параметры установки Агента администрирования

В таблице ниже описаны свойства MSI, которые можно настраивать при установке Агента администрирования. Все параметры являются опциональными, кроме SERVERADDRESS.

Таблица 29. Параметры установки Агента администрирования в неинтерактивном режиме

Свойство MSI	Описание	Возможные значения
DONT_USE_ANSWER_FILE	Читать параметры установки из файла ответов.	• 1 – читать; • другое значение или не задано – не читать.
INSTALLDIR	Путь к папке установки Агента администрирования.	Строковое значение.
SERVERADDRESS	Адрес Сервера администрирования (обязательный параметр).	Строковое значение.
SERVERPORT	Номер порта подключения к Серверу администрирования.	Числовое значение.
SERVERSSLPORT	Номер порта для защищенного подключения к Серверу администрирования с использованием протокола SSL.	Числовое значение.
USESSL	Использовать ли SSL-соединение.	• 1 – использовать; • другое значение или не задано – не использовать.
OPENUDPPORT	Открыть ли UDP-порт.	• 1 – открывать; • другое значение или не задано – не открывать.
UDPPORT	Номер UDP-порта.	Числовое значение.

Свойство MSI	Описание	Возможные значения
USEPROXY	Использовать ли прокси-сервер.	• 1 – использовать; • другое значение или не задано – не использовать.
PROXYADDRESS	Адрес прокси-сервера	Строковое значение.
PROXYPORT	Номер порта для подключения к прокси-серверу.	Числовое значение.
PROXYLOGIN	Учетная запись для подключения к прокси-серверу.	Строковое значение.
PROXYPASSWORD	Пароль учетной записи для подключения к прокси-серверу. Не указывайте в параметрах инсталляционных пакетов данные привилегированных учетных записей.	Строковое значение.
GATEWAYMODE	Режим использования шлюза соединения.	• 0 – не использовать шлюз соединений; • 1 – использовать данный Агент администрирования в качестве шлюза соединений; • 2 – подключаться к Серверу администрирования через шлюз соединений
GATEWAYADDRESS	Адрес шлюза соединений.	Строковое значение.

Свойство MSI	Описание	Возможные значения
CERTSELECTION	Способ получения сертификата.	• GetOnFirstConnection – получить сертификат от Сервера администрирования; • GetExistent – задать существующий сертификат. Если выбран этот вариант, должно быть задано свойство CERTFILE.
CERTFILE	Путь к файлу сертификата.	Строковое значение.
VMVDI	Включить динамический режим для VDI.	• 1 – включать; • другое значение или не задано – не включать.
LAUNCHPROGRAM	Запускать ли службу Агента администрирования после установки.	• 1 – запускать; • другое значение или не задано – не запускать.

Виртуальная инфраструктура

Kaspersky Security Center поддерживает работу с виртуальными машинами. Поддерживается установка Агента администрирования и программы защиты на каждую виртуальную машину и защита виртуальных машин на уровне гипервизора. В первом случае для защиты виртуальных машин может использоваться как обычная программа защиты, так и Kaspersky Security для виртуальных сред / Легкий агент. Во втором случае для защиты виртуальных машин используется Kaspersky Security для виртуальных сред / Защита без агента.

Начиная с версии 10 Maintenance Release 1, Kaspersky Security Center поддерживает откат виртуальных машин в предыдущее состояние (см. раздел "Поддержка отката файловой системы для устройств с Агентом администрирования" на стр. 263).

В этом разделе

Рекомендации по снижению нагрузки на виртуальные машины

В случае инсталляции Агента администрирования на виртуальную машину следует рассмотреть возможность отключения той части функциональности Kaspersky Security Center, которая малополезна для виртуальных машин.

При установке Агента администрирования на виртуальную машину или на шаблон, из которого в дальнейшем будут получены виртуальные машины, целесообразно выполнить следующие действия:

- если выполняется удаленная установка, в окне свойств инсталляционного пакета Агента администрирования (раздел **Дополнительно**) установить флажок **Оптимизировать параметры для VDI (Virtual Desktop Infrastructure)**;
- если выполняется интерактивная установка с помощью мастера, в окне мастера установить флажок **Оптимизировать параметры Агента администрирования для виртуальной инфраструктуры**.

Установка флажков изменит параметры Агента администрирования таким образом, чтобы по умолчанию (до применения политики) были выключены следующие функции:

- получение информации об установленном программном обеспечении;
- получение информации об аппаратном обеспечении;
- получение информации о наличии уязвимостей;
- получение информации о необходимых обновлениях.

Как правило, перечисленные функции не нужны на виртуальных машинах в силу того, что программное обеспечение и виртуальное аппаратное обеспечение на них единообразны.

Выключение функций обратимо. Если любая из выключенных функций все же нужна, ее можно включить при помощи политики Агента администрирования, или в локальных параметрах Агента администрирования. Локальные параметры Агента администрирования доступны из контекстного меню соответствующего устройства в Консоли администрирования.

Поддержка динамических виртуальных машин

Kaspersky Security Center поддерживает динамические виртуальные машины. Если в сети организации развернута виртуальная инфраструктура, то в некоторых случаях могут использоваться динамические (временные) виртуальные машины. Такие машины создаются с уникальными именами из заранее подготовленного администратором шаблона. Пользователь работает с созданной машиной некоторое время, а после выключения виртуальная машина удаляется из виртуальной инфраструктуры. Если в сети организации развернут Kaspersky Security Center, то виртуальная машина с установленным на ней Агентом администрирования добавляется в базу данных Сервера администрирования. После выключения виртуальной машины запись о ней должна быть также удалена и из базы данных Сервера администрирования.

Чтобы функциональность автоматического удаления записей о виртуальных машинах работала, при установке Агента администрирования на шаблон, из которого будут созданы динамические виртуальные машины, нужно установить флажок **Включить динамический режим для VDI**:

- в случае удаленной установки – в окне свойств инсталляционного пакета Агента администрирования (раздел **Дополнительно**);
- в случае интерактивной установки – в окне мастера установки Агента администрирования.

> Флажок **Включить динамический режим для VDI** не следует устанавливать при установке Агента администрирования на физические устройства.

Если нужно, чтобы события с динамических виртуальных машин сохранялись на Сервере администрирования некоторое время после удаления машин, то следует в окне свойств Сервера администрирования в разделе **Хранение событий** установить флажок **Хранить события после удаления устройств** и указать максимальное время хранения событий в днях.

Поддержка копирования виртуальных машин

Копирование виртуальной машины с установленным на нее Агентом администрирования или ее создание из шаблона с установленным Агентом администрирования эквивалентно развертыванию Агентов администрирования захватом и копированием образа жесткого диска. Поэтому, в общем случае, при копировании виртуальных машин нужно выполнять те же действия, что и при развертывании копированием образа диска (см. раздел "Развертывание захватом и копированием образа жесткого диска устройства" на стр. 229).

Однако в описанных ниже двух случаях Агент администрирования обнаруживает факт копирования автоматически. Поэтому выполнять сложные действия, описанные в разделе «Развертывание захватом и копированием жесткого диска устройства», не обязательно:

- При установке Агента администрирования был установлен флажок **Включить динамический режим для VDI**: после каждой перезагрузки операционной системы такая виртуальная машина будет считаться новым устройством, независимо от факта ее копирования.
- Используется один из следующих гипервизоров: VMware™, HyperV® или Xen®: Агент администрирования определит факт копирования виртуальной машины по изменившимся идентификаторам виртуального аппаратного обеспечения.

> Анализ изменений виртуального аппаратного обеспечения не абсолютно надежен. Прежде чем широко использовать данный метод, следует предварительно проверить его работоспособность на небольшом количестве виртуальных машин для используемой в организации версии гипервизора.

Поддержка отката файловой системы для устройств с Агентом администрирования

Kaspersky Security Center является распределенной программой. Откат файловой системы в предыдущее состояние на одном из устройств с установленным Агентом администрирования приведет к рассинхронизации данных и неправильной работе Kaspersky Security Center.

Откат файловой системы (или ее части) в предыдущее состояние может происходить в следующих случаях:

- при копировании образа жесткого диска;
- при восстановлении состояния виртуальной машины средствами виртуальной инфраструктуры;
- при восстановлении данных из резервной копии или точки восстановления.

Для Kaspersky Security Center критичны только те сценарии, при которых стороннее программное обеспечение на устройствах с установленным Агентом администрирования затрагивает папку %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\. Поэтому, при наличии возможности, следует всегда исключать эту папку из процедуры восстановления.

Поскольку в ряде организаций регламент работы предполагает выполнение отката состояния файловой системы устройств, в Kaspersky Security Center, начиная с версии 10 Maintenance Release 1 (Сервер администрирования и Агенты администрирования должны быть версии 10 Maintenance Release 1 или выше), была добавлена поддержка обнаружения отката файловой системы на устройствах с установленным Агентом администрирования. В случае обнаружения такие устройства автоматически переподключаются к Серверу администрирования с полной очисткой и полной синхронизацией данных.

В Kaspersky Security Center 10 Service Pack 3 поддержка обнаружения отката файловой системы включена по умолчанию.

Следует при любой возможности избегать отката папки %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\ на устройствах с установленным Агентом администрирования, так как полная повторная синхронизация данных требует большого количества ресурсов.

Для устройства с установленным Сервером администрирования откат состояния системы недопустим. Недопустимым также является откат в предыдущее состояние базы данных, используемой Сервером администрирования.

Восстановить состояние Сервера администрирования из резервной копии можно только при помощи штатной утилиты klbackup (см. раздел "Резервное копирование и восстановление параметров Сервера администрирования" на стр. 217).

Удаленная установка программ

В этом разделе описаны способы удаленной установки программ "Лаборатории Касперского" и их удаления с устройств сети.

> Перед началом установки программ на клиентские устройства требуется убедиться в том, что аппаратное и программное обеспечение устройств соответствует предъявляемым к нему требованиям.

В этом разделе рассмотрена удаленная установка программ через Консоль администрирования.

Связь Сервера администрирования с клиентскими устройствами обеспечивает Агент администрирования. Поэтому его необходимо установить на каждое клиентское устройство, которое будет подключено к системе удаленного централизованного управления.

> На устройстве, где установлен Сервер администрирования, может использоваться только серверная версия Агента администрирования. Она входит в состав Сервера администрирования и устанавливается и удаляется вместе с ним. Устанавливать Агент администрирования на это устройство не требуется.

Установка Агента администрирования осуществляется точно так же, как и установка программ, и может быть проведена как удаленно, так и локально. При централизованной установке программ защиты через Консоль администрирования вы можете установить Агент администрирования совместно с программами защиты.

Агенты администрирования могут различаться в зависимости от программ "Лаборатории Касперского", для совместной работы с которыми они должны быть установлены. В некоторых случаях возможна только локальная установка Агента администрирования (подробнее см. в Руководствах к соответствующим программам). Агент администрирования устанавливается на клиентское устройство один раз.

Управление программами "Лаборатории Касперского" через Консоль администрирования выполняется при помощи плагинов управления. Поэтому для получения доступа к управлению программой через Kaspersky Security Center плагин управления этой программой должен быть установлен на рабочее место администратора.

Вы можете выполнить удаленную установку программ с рабочего места администратора в главном окне программы Kaspersky Security Center.

> Некоторые программы "Лаборатории Касперского" можно установить на клиентские устройства только локально (подробнее см. в Руководствах к соответствующим программам). Удаленное управление этими программами с помощью Kaspersky Security Center доступно.

Для удаленной установки программного обеспечения следует создать задачу удаленной установки.

Сформированная задача удаленной установки будет запускаться на выполнение в соответствии со своим расписанием. Вы можете прервать процедуру установки, остановив выполнение задачи вручную.

> Если удаленная установка программы завершается с ошибкой, вы можете проверить, чем вызвана эта проблема, и устранить ее с помощью утилиты подготовки устройства к удаленной установке (см. раздел "Подготовка устройства к удаленной установке. Утилита riprep.exe" на стр. 291).

Вы можете отслеживать процесс установки программ защиты "Лаборатории Касперского" в сети с помощью отчета о развертывании.

Kaspersky Security Center поддерживает удаленное управление следующими программами компании «Лаборатория Касперского»:

- Для рабочих станций:
  - Kaspersky Endpoint Security 10 для Windows;
  - Kaspersky Endpoint Security 10 для Linux;
  - Kaspersky Endpoint Security 10 для Mac;
  - Kaspersky Embedded Systems Security для Windows.
- Для мобильных устройств:

- Kaspersky Security 10 для мобильных устройств (установка доступна при активации функциональности Управление мобильными устройствами);

- Для файловых серверов:
  - Kaspersky Endpoint Security 10 для Windows;
  - Антивирус Касперского 8.0 для Windows Servers Enterprise Edition;
  - Kaspersky Security 10 для Windows Server;
  - Антивирус Касперского 8.0 для Linux File Server;
  - Антивирус Касперского 10 для Linux File Server.
- Для виртуальных машин:
  - Kaspersky Security для виртуальных сред 3.0 Защита без агента;
  - Kaspersky Security для виртуальных сред 4.0 Защита без агента;
  - Kaspersky Security для виртуальных сред 3.0. Легкий агент;
  - Kaspersky Security для виртуальных сред 4.0. Легкий агент.
- Kaspersky Industrial Cyber Security:
  - Kaspersky Industrial Cyber Security for Nodes.

Вы можете получить сведения о последних версиях программ на веб-сайте Службы технической поддержки, на странице Kaspersky Security Center, в разделе Общие понятия (http://support.kaspersky.ru/12029).

Подробную информацию об управлении перечисленными программами через Kaspersky Security Center см. в Руководствах к соответствующим программам.

В этом разделе

Установка программ с помощью задачи удаленной установки

Kaspersky Security Center позволяет удаленно устанавливать программы на устройства с помощью задач удаленной установки. Задачи создаются и назначаются устройствам с помощью мастера. Чтобы быстрее и проще назначить задачу устройствам, вы можете указывать в окне мастера устройства удобным для вас способом:

- **Выбрать устройства, обнаруженные в сети Сервером администрирования**. В этом случае задача назначается набору устройств. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.
- **Задать адреса устройств вручную или импортировать из списка**. Вы можете задавать NetBIOS-имена, DNS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

- **Назначить задачу выборке устройств**. В этом случае задача назначается устройствам, входящим в состав ранее созданной выборки. Вы можете указать выборку, созданную по умолчанию, или вашу собственную выборку.

- **Назначить задачу группе администрирования**. В этом случае задача назначается устройствам, входящим в ранее созданную группу администрирования.

Для правильной работы задачи удаленной установки на устройстве, на котором не установлен Агент администрирования, необходимо открыть порты TCP 139 и 445, UDP 137 и 138. Эти порты по умолчанию открыты на всех устройствах, включенных в домен. Они открываются автоматически с помощью утилиты подготовки устройств к удаленной установке (см. раздел "Подготовка устройства к удаленной установке. Утилита riprep.exe" на стр. 291).

В этом разделе

Установка программы на выбранные устройства

► *Чтобы установить программу на выбранные устройства, выполните следующие действия:*

1. Подключитесь к Серверу администрирования, под управлением которого находятся нужные вам устройства.

2. В дереве консоли выберите папку **Задачи**.

3. Запустите процесс создания задачи по ссылке **Создать задачу**.

   В результате запускается мастер создания задачи. Следуйте его указаниям.

В окне **Тип задачи** мастера создания задачи в узле **Сервер администрирования Kaspersky Security Center 10** выберите тип задачи **Удаленная установка программы**.

В результате работы мастера создания задачи будет создана задача удаленной установки выбранной программы для выбранного набора устройств. Созданная задача отображается в рабочей области папки **Задачи**.

4. Запустите задачу вручную или дождитесь ее запуска в соответствии с расписанием, указанным вами в параметрах задачи.

В результате выполнения задачи удаленной установки выбранная программа будет установлена на выбранные устройства.

Установка программы на клиентские устройства группы администрирования

► *Чтобы установить программу на клиентские устройства группы администрирования, выполните следующие действия:*

1. Подключитесь к Серверу администрирования, под управлением которого находится нужная группа администрирования.

2. В дереве консоли выберите группу администрирования.

3. В рабочей области группы выберите закладку **Задачи**.

4. Запустите процесс создания задачи по ссылке **Создать задачу**.

   В результате запускается мастер создания задачи. Следуйте его указаниям.

   В окне **Тип задачи** мастера создания задачи в узле **Сервер администрирования Kaspersky Security Center 10** выберите тип задачи **Удаленная установка программы**.

   В результате работы мастера создания задачи будет создана групповая задача удаленной установки выбранной программы. Созданная задача отображается в рабочей области группы администрирования, на закладке **Задачи**.

5. Запустите задачу вручную или дождитесь ее запуска в соответствии с расписанием, указанным вами в параметрах задачи.

В результате выполнения задачи удаленной установки выбранная программа будет установлена на клиентские устройства группы администрирования.

Установка программы с помощью групповых политик Active Directory

Kaspersky Security Center позволяет устанавливать программы "Лаборатории Касперского" с помощью групповых политик Active Directory.

> Установка программ с помощью групповых политик Active Directory возможна только при использовании инсталляционных пакетов, в состав которых входит Агент администрирования.

► *Чтобы установить программу с помощью групповых политик Active Directory, выполните следующие действия:*

1. Запустите процесс создания групповой задачи удаленной установки или задачи удаленной установки для набора устройств.

2. В окне мастера создания задачи **Параметры** установите флажок **Назначить установку инсталляционного пакета в групповых политиках Active Directory**.

3. Запустите созданную задачу удаленной установки вручную или дождитесь ее запуска по расписанию.

В результате будет запущен следующий механизм удаленной установки:

1. После запуска задачи в каждом домене, которому принадлежат клиентские устройства из набора, будут созданы следующие объекты:

   - Групповая политика с именем **Kaspersky_AK{GUID}**.

   - Связанная с групповой политикой группа безопасности **Kaspersky_AK{GUID}**. Эта группа безопасности содержит клиентские устройства, на которые

распространяется задача. Состав группы безопасности определяет область действия групповой политики.

2. Установка программ на клиентские устройства осуществляется непосредственно из сетевой папки общего доступа программы Share. При этом в папке установки Kaspersky Security Center будет создана вложенная вспомогательная папка, содержащая файл с расширением msi для устанавливаемой программы.

3. При добавлении новых устройств в область действия задачи они будут добавлены в группу безопасности после следующего запуска задачи. Если в расписании задачи установлен флажок **Запускать пропущенные задачи**, устройства будут добавлены в группу безопасности сразу.

4. При удалении устройств из области действия задачи их удаление из группы безопасности произойдет при следующем запуске задачи.

5. При удалении задачи из Active Directory будут удалены политика, ссылка на политику и группа безопасности, связанная с задачей.

Если вы хотите использовать другую схему установки через Active Directory, вы можете настроить параметры установки вручную. Это может потребоваться, например, в следующих случаях:

- при отсутствии у администратора антивирусной безопасности прав на внесение изменений в Active Directory некоторых доменов;
- при необходимости размещения исходного дистрибутива на отдельном сетевом ресурсе;
- для привязки групповой политики к конкретным подразделениям Active Directory.

Доступны следующие варианты использования другой схемы установки через Active Directory:

- Если установку требуется осуществлять непосредственно из папки общего доступа Kaspersky Security Center, в свойствах групповой политики Active Directory следует указать файл с расширением msi, расположенный во вложенной папке exec в папке инсталляционного пакета нужной программы.

- Если инсталляционный пакет нужно разместить на другом сетевом ресурсе, следует скопировать в него все содержимое папки exec, так как помимо файла с расширением msi в ней содержатся конфигурационные файлы, сформированные при создании инсталляционного пакета. Чтобы ключ был установлен вместе с программой, в эту папку следует также скопировать файл ключа.

Установка программ на подчиненные Серверы администрирования

► *Чтобы установить программу на подчиненные Серверы администрирования, выполните следующие действия:*

1. Подключитесь к Серверу администрирования, под управлением которого находятся нужные вам подчиненные Серверы администрирования.

2. Убедитесь в том, что соответствующий устанавливаемой программе инсталляционный пакет находится на каждом из выбранных подчиненных Серверов администрирования. Если инсталляционного пакета нет на каком-либо из подчиненных Серверов, распространите его с помощью задачи распространения инсталляционного пакета (см. раздел "Распространение инсталляционных пакетов на подчиненные Серверы администрирования" на стр. 286).

3. Запустите создание задачи установки программы на подчиненные Серверы администрирования одним из следующих способов:

   - Если вы хотите сформировать задачу для подчиненных Серверов выбранной группы администрирования, запустите создание групповой задачи удаленной установки для этой группы (см. раздел "Установка программы на клиентские устройства группы администрирования" на стр. 270).

   - Если вы хотите сформировать задачу для набора подчиненных Серверов, запустите создание задачи удаленной установки для набора устройств (см. раздел "Установка программы на выбранные устройства" на стр. 269).

   В результате запустится мастер создания задачи удаленной установки. Следуйте его указаниям.

В окне **Тип задачи** мастера создания задачи в узле **Сервер администрирования Kaspersky Security Center 10** в папке **Дополнительно** выберите тип задачи **Удаленная установка программы на подчиненные Серверы администрирования**.

В результате работы мастера создания задачи будет создана задача удаленной установки выбранной программы на выбранные подчиненные Серверы администрирования.

4. Запустите задачу вручную или дождитесь ее запуска в соответствии с расписанием, указанным вами в параметрах задачи.

В результате выполнения задачи удаленной установки выбранная программа будет установлена на выбранные подчиненные Серверы администрирования.

Установка программ с помощью мастера удаленной установки

Для установки программ компании вы можете воспользоваться мастером удаленной установки. Мастер удаленной установки позволяет проводить удаленную установку программ как с использованием сформированных инсталляционных пакетов, так и с дистрибутивов.

Для правильной работы задачи удаленной установки на клиентском устройстве, на котором не установлен Агент администрирования, необходимо открыть следующие порты: TCP 139 и 445; UDP 137 и 138. Эти порты по умолчанию открыты для всех устройств, включенных в домен, и открываются автоматически с помощью утилиты подготовки устройства к удаленной установке (см. раздел "Подготовка устройства к удаленной установке. Утилита riprep.exe" на стр. 291).

► *Чтобы установить программу на выбранные устройства с помощью мастера удаленной установки, выполните следующие действия:*

1. В дереве консоли выберите папку **Инсталляционные пакеты**, вложенную в папку **Удаленная установка**.

2. В рабочей области папки выберите инсталляционный пакет программы, которую нужно установить.
3. В контекстном меню инсталляционного пакета выберите пункт **Установить программу**.

   Запустится мастер удаленной установки.
4. В окне **Выбор устройств для установки** можно сформировать список устройств, на которые будет установлена программа:

   - **Установить на группу управляемых устройств**

     Если выбран этот вариант, задача удаленной установки программы будет создана для группы устройств.

   - **Выбрать устройства для установки**

     Если выбран этот вариант, задача удаленной установки программы будет создана для набора устройств. В состав набора могут входить как устройства в составе групп, так и нераспределенные устройства.
5. В окне **Определение параметров задачи удаленной установки** настройте параметры удаленной установки программы.

   В блоке параметров **Форсировать загрузку инсталляционного пакета** выберите способ доставки на клиентские устройства файлов, необходимых для установки программы:

   - **С помощью Агента администрирования**

     Если флажок установлен, доставку инсталляционных пакетов на клиентские устройства выполняет установленный на клиентских устройствах Агент администрирования.

     Если флажок снят, доставка инсталляционных пакетов выполняется средствами Microsoft Windows.

     Рекомендуется установить флажок, если задача назначена для устройств с установленными Агентами администрирования.

     По умолчанию флажок установлен.

- **Средствами Microsoft Windows с помощью Сервера администрирования**

  Если флажок установлен, доставка файлов на клиентские устройства будет осуществляться средствами Microsoft Windows с помощью Сервера администрирования. Этот вариант можно выбрать, если на клиентском устройстве не установлен Агент администрирования, но клиентское устройство находится в той же сети, что и Сервер администрирования.

  По умолчанию флажок установлен.

- **Средствами Microsoft Windows с помощью агентов обновлений**

  Если флажок установлен, инсталляционные пакеты передаются на клиентские устройства средствами операционной системы через агенты обновлений. Этот вариант можно выбрать, если в сети есть хотя бы один агент обновлений.

Если установлен флажок **С помощью Агента администрирования**, файлы будут доставлены средствами операционной системы только в случае невозможности использования средств Агента администрирования.

  По умолчанию флажок установлен для задач удаленной установки, созданных на виртуальном Сервере администрирования.

Настройте дополнительные параметры:

- **Не устанавливать программу, если она уже установлена**

  Если флажок установлен, выбранная программа не устанавливается заново, если она уже установлена на клиентском устройстве.

  Если флажок снят, программа будет установлена в любом случае.

  По умолчанию флажок установлен.

- **Назначить установку инсталляционного пакета в групповых политиках Active Directory**

  Если флажок установлен, инсталляционный пакет будет

устанавливаться с помощью групповых политик Active Directory.

Флажок доступен если выбран инсталляционный пакет Агента администрирования.

По умолчанию флажок снят.

1. В окне **Выбор ключа** выберите ключ и способ его распространения:

   - **Автоматическое распространение (рекомендуется)**

     Если выбран этот вариант, ключ будет автоматически распространяться на те устройства, для которых он подходит:

     - если в свойствах ключа настроено автоматическое распространение;
     - если создана задача **Добавление ключа**.

   - **Распространение в составе инсталляционного пакета**

     Если выбран этот вариант, ключ распространяется на устройства вместе с инсталляционным пакетом.

> Не рекомендуется распространять ключ таким способом, так как по умолчанию к хранилищу пакетов настроен общий доступ на чтение.

Окно **Выбор ключа** отображается если в состав инсталляционного пакета не входит ключ.

Если в состав инсталляционного пакета входит ключ, отображается окно **Свойства ключа** с информацией о ключе.

1. В окне **Выбор действия в случае необходимости перезагрузки операционной системы в ходе установки** определите, перезагружать ли устройства, если в ходе установки программ на них потребуется перезагрузка операционной системы:

   - **Не перезагружать устройство**

     Если выбран этот вариант, устройство не будет перезагружаться после установки программы защиты.

По умолчанию выбран этот вариант.

- **Перезагрузить устройство**

  Если выбран этот вариант, устройство будет перезагружено после установки программы защиты.

- **Спросить у пользователя**

  Если выбран этот вариант, после установки программы защиты пользователю будет показано сообщение о необходимости перезагрузки устройства. По ссылке **Изменить** можно изменить текст сообщения, а также период отображения сообщения и время выполнения автоматической перезагрузки.

  По умолчанию выбран этот вариант.

- **Принудительно закрывать программы в заблокированных сеансах**

  Если флажок установлен, программы в заблокированных устройствах будут принудительно закрываться перед перезагрузкой.

  По умолчанию флажок снят.

2. В окне **Выбор учетных записей для доступа к устройствам** можно добавить учетные записи, которые будут использоваться для запуска задачи удаленной установки:

   - **Учетная запись не требуется (установлен Агент администрирования уже установлен)**

     Если выбран этот вариант, не требуется указывать учетную запись, от имени которой будет запускаться инсталлятор программы. Задача запускается под учетной записью, под которой работает служба Сервера администрирования.

     Если Агент администрирования не установлен на клиентских устройствах, вариант недоступен.

   - **Учетная запись требуется (для установки без помощи Агента администрирования)**

Если выбран этот вариант, можно указать учетную запись, от имени которой будет запускаться инсталлятор программы. Учетную запись можно указать в случае если Агент администрирования не установлен на устройствах, для которых назначена задача.

Вы можете указать несколько учетных записей, если ни одна из них не обладает необходимыми правами на всех устройствах, для которых назначена задача. В этом случае для запуска задачи используются последовательно, сверху вниз, все добавленные учетные записи.

Если ни одна учетная запись не добавлена, задача запускается под той учетной записью, под которой работает служба Сервера администрирования.

3. В окне **Запуск установки** нажмите на кнопку **Далее** для создания и запуска задачи удаленной установки на выбранных устройствах.

   Если в окне **Запуск установки** установлен флажок **Не запускать задачу после завершения работы мастера удаленной установки**, задача удаленной установки не будет запущена. Вы можете запустить эту задачу в дальнейшем вручную. Имя задачи соответствует имени инсталляционного пакета для установки программы: **Установка <Имя инсталляционного пакета>**.

► *Чтобы установить программу на устройства группы администрирования с помощью мастера удаленной установки, выполните следующие действия:*

1. Подключитесь к Серверу администрирования, под управлением которого находится нужная группа администрирования.

2. В дереве консоли выберите группу администрирования.

3. В рабочей области группы нажмите на кнопку **Выполнить действие** и в раскрывающемся списке выберите пункт **Установить программу**.

   В результате запустится мастер удаленной установки. Следуйте его указаниям.

4. На последнем шаге мастера нажмите на кнопку **Далее** для создания и запуска задачи удаленной установки на выбранных устройствах.

В результате работы мастера удаленной установки Kaspersky Security Center выполняет следующие действия:

- Создает инсталляционный пакет для установки программы (если он не был создан раньше). Инсталляционный пакет размещается в папке **Удаленная установка**, во вложенной папке **Инсталляционные пакеты** с именем, соответствующим названию и версии программы. Вы можете использовать этот инсталляционный пакет для установки программы в дальнейшем.

- Создает и запускает задачу удаленной установки для набора устройств или для группы администрирования. Сформированная задача удаленной установки размещается в папке **Задачи** или добавляется к задачам группы администрирования, для которой она была создана. Вы можете запускать эту задачу в дальнейшем вручную. Имя задачи соответствует имени инсталляционного пакета для установки программы: **Установка <Имя инсталляционного пакета>**.

Просмотр отчета о развертывании защиты

Для отслеживания процесса развертывания защиты в сети можно использовать отчет о развертывании защиты.

► *Чтобы просмотреть отчет о развертывании защиты, выполните следующие действия:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.

2. В рабочей области узла выберите закладку **Отчеты**.

3. В рабочей области закладки **Отчеты** выберите шаблон отчета **Отчет о развертывании защиты**.

В рабочей области будет сформирован отчет, содержащий информацию о развертывании защиты на всех устройствах сети.

Вы можете сформировать новый отчет о развертывании защиты и указать, информацию какого типа в него следует включать:

- для группы администрирования;

- для набора устройств;
- для выборки устройств;
- для всех устройств.

> В рамках Kaspersky Security Center считается, что на устройстве развернута защита в том случае, когда на нем установлена программа защиты и включена постоянная защита.

Удаленная деинсталляция программ

Kaspersky Security Center позволяет удаленно деинсталлировать программы с устройств с помощью задач удаленной деинсталляции. Задачи создаются и назначаются устройствам с помощью мастера. Чтобы быстрее и проще назначить задачу устройствам, вы можете указывать в окне мастера устройства удобным для вас способом:

- **Выбрать устройства, обнаруженные в сети Сервером администрирования**. В этом случае задача назначается набору устройств. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.
- **Задать адреса устройств вручную или импортировать из списка**. Вы можете задавать NetBIOS-имена, DNS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.
- **Назначить задачу выборке устройств**. В этом случае задача назначается устройствам, входящим в состав ранее созданной выборки. Вы можете указать выборку, созданную по умолчанию, или вашу собственную выборку.
- **Назначить задачу группе администрирования**. В этом случае задача назначается устройствам, входящим в ранее созданную группу администрирования.

В этом разделе

Удаленная деинсталляция программы с клиентских устройств группы администрирования

► *Чтобы удаленно деинсталлировать программу с клиентских устройств группы администрирования, выполните следующие действия:*

1. Подключитесь к Серверу администрирования, под управлением которого находится нужная группа администрирования.

2. В дереве консоли выберите группу администрирования.

3. В рабочей области группы выберите закладку **Задачи**.

4. Запустите процесс создания задачи по ссылке **Создать задачу**.

   В результате запускается мастер создания задачи. Следуйте его указаниям.

   В окне **Тип задачи** мастера создания задачи в узле **Сервер администрирования Kaspersky Security Center 10** в папке **Дополнительно** выберите тип задачи **Удаленная деинсталляция программы**.

   В результате работы мастера создания задачи будет создана групповая задача удаленной деинсталляции выбранной программы. Созданная задача отображается в рабочей области группы администрирования, на закладке **Задачи**.

5. Запустите задачу вручную или дождитесь ее запуска в соответствии с расписанием, указанным вами в параметрах задачи.

В результате выполнения задачи удаленной деинсталляции выбранная программа будет удалена с клиентских устройств группы администрирования.

Удаленная деинсталляция программы с выбранных устройств

► *Чтобы удаленно деинсталлировать программу с выбранных устройств, выполните следующие действия:*

1. Подключитесь к Серверу администрирования, под управлением которого находятся нужные вам устройства.

2. В дереве консоли выберите папку **Задачи**.

3. Запустите процесс создания задачи по кнопке **Создать задачу**.

   В результате запускается мастер создания задачи. Следуйте его указаниям.

   В окне **Тип задачи** мастера создания задачи в узле **Сервер администрирования Kaspersky Security Center 10** в папке **Дополнительно** выберите тип задачи **Удаленная деинсталляция программы**.

   В результате работы мастера создания задачи будет создана задача удаленной деинсталляции выбранной программы для выбранного набора устройств. Созданная задача отображается в рабочей области папки **Задачи**.

4. Запустите задачу вручную или дождитесь ее запуска в соответствии с расписанием, указанным вами в параметрах задачи.

В результате выполнения задачи удаленной установки выбранная программа будет удалена с выбранных устройств.

Работа с инсталляционными пакетами

При создании задач удаленной установки используются инсталляционные пакеты, которые содержат набор параметров, необходимых для установки программы.

Инсталляционные пакеты могут содержать в себе файл ключа. Не рекомендуется размещать в открытом доступе инсталляционные пакеты, содержащие в себе файл ключа.

Вы можете использовать один и тот же инсталляционный пакет многократно.

Сформированные для Сервера администрирования инсталляционные пакеты размещаются в дереве консоли в папке **Удаленная установка**, во вложенной папке **Инсталляционные пакеты**. На Сервере администрирования инсталляционные пакеты хранятся в заданной папке общего доступа в служебной папке Packages.

В этом разделе

Создание инсталляционного пакета

► *Чтобы создать инсталляционный пакет, выполните следующие действия:*

1. Подключитесь к нужному Серверу администрирования.
2. В дереве консоли в папке **Удаленная установка** выберите вложенную папку **Инсталляционные пакеты**.
3. Запустите процесс создания инсталляционного пакета одним из следующих способов:
   - в контекстном меню папки **Инсталляционные пакеты** выберите пункт **Создать → Инсталляционный пакет**;

- в контекстном меню списка инсталляционных пакетов выберите пункт **Создать → Инсталляционный пакет**;
- по ссылке **Создать инсталляционный пакет** в блоке управления списком инсталляционных пакетов.

В результате запустится мастер создания инсталляционного пакета. Следуйте его указаниям.

В процессе создания инсталляционного пакета для программы "Лаборатории Касперского" вам может быть предложено ознакомиться с Лицензионным соглашением на эту программу и Политикой конфиденциальности программы. Внимательно прочитайте Лицензионное соглашение. С текстом Политики конфиденциальности вы можете ознакомиться на сайте "Лаборатории Касперского" https://www.kaspersky.com/products-and-services-privacy-policy. Если вы согласны со всеми пунктами Лицензионного соглашения и Политики конфиденциальности, в блоке **Я подтверждаю, что полностью прочитал, понимаю и принимаю** установите флажки:

- **положения и условия настоящего Лицензионного соглашения**;
- **Политику конфиденциальности, которая описывает обработку данных**.

Установка программы на ваше устройство будет продолжена после установки обоих флажков. После этого создание инсталляционного пакета будет продолжено. Путь к файлу Лицензионного соглашения и Политики конфиденциальности задается в файле с расширением kud или kpd, входящем в состав дистрибутива программы, для которой создается инсталляционный пакет.

> При создании инсталляционного пакета для программы Kaspersky Endpoint Security для Mac вы можете выбрать язык Лицензионного соглашения и Политики конфиденциальности.

Во время создания инсталляционного пакета для программы из базы программ "Лаборатории Касперского" вы можете включить автоматическую установку общесистемных компонентов (пререквизитов), необходимых для установки этой программы. Мастер создания инсталляционного пакета отображает список всех возможных общесистемных компонентов для выбранной программы. Если инсталляционный пакет создается для патча (неполный дистрибутив), то в список

общесистемных компонентов будут включены все необходимые для развертывания патча составляющие, вплоть до версии с полным дистрибутивом. Впоследствии вы можете ознакомиться с этим списком в свойствах инсталляционного пакета.

После завершения работы мастера созданный инсталляционный пакет будет отображаться в рабочей области папки **Инсталляционные пакеты** в дереве консоли.

Инсталляционный пакет для удаленной установки Агента администрирования не нужно создавать вручную. Он формируется автоматически при установке программы Kaspersky Security Center и располагается в папке **Инсталляционные пакеты**. Если пакет для удаленной установки Агента администрирования был удален, то для его повторного формирования в качестве файла с описанием следует выбрать файл nagent10.kud, расположенный в папке NetAgent дистрибутива Kaspersky Security Center.

Не указывайте в параметрах инсталляционных пакетов данные привилегированных учетных записей.

При создании инсталляционного пакета Сервера администрирования в качестве файла с описанием следует выбрать файл sc10.kud, расположенный в корневой папке дистрибутива Kaspersky Security Center.

Распространение инсталляционных пакетов на подчиненные Серверы администрирования

► *Чтобы распространить инсталляционные пакеты на подчиненные Серверы администрирования, выполните следующие действия:*

1. Подключитесь к Серверу администрирования, под управлением которого находятся нужные вам подчиненные Серверы администрирования.

2. Запустите создание задачи распространения инсталляционного пакета на подчиненные Серверы администрирования одним из следующих способов:

   - Если вы хотите сформировать задачу для подчиненных Серверов выбранной группы администрирования, запустите создание групповой задачи для этой группы.

- Если вы хотите сформировать задачу для набора подчиненных Серверов, запустите создание задачи для набора устройств.

В результате запустится мастер создания задачи. Следуйте его указаниям.

В окне **Тип задачи** мастера создания задачи в узле **Сервер администрирования Kaspersky Security Center 10** в папке **Дополнительно** выберите тип задачи **Распространение инсталляционного пакета**.

В результате работы мастера создания задачи будет создана задача распространения выбранных инсталляционных пакетов на выбранные подчиненные Серверы администрирования.

3. Запустите задачу вручную или дождитесь ее запуска в соответствии с расписанием, указанным вами в параметрах задачи.

В результате выполнения задачи выбранные инсталляционные пакеты будут скопированы на выбранные подчиненные Серверы администрирования.

Распространение инсталляционных пакетов с помощью агентов обновлений

Для распространения инсталляционных пакетов в пределах группы администрирования вы можете использовать агенты обновлений.

После получения инсталляционных пакетов с Сервера администрирования агенты обновлений автоматически распространяют их на клиентские устройства с помощью многоадресной IP-рассылки. IP-рассылка новых инсталляционных пакетов в пределах группы администрирования производится один раз. Если в момент рассылки клиентское устройство было отключено от сети организации, то при запуске задачи установки Агент администрирования клиентского устройства автоматически скачивает необходимый инсталляционный пакет с агента обновлений.

Передача в Kaspersky Security Center информации о результатах установки программы

После создания инсталляционного пакета программы вы можете настроить инсталляционный пакет таким образом, чтобы диагностическая информация о результатах установки программы передавалась в Kaspersky Security Center. Для инсталляционных пакетов программ "Лаборатории Касперского" передача диагностической информации о результате установки программы настроена по умолчанию, дополнительная настройка не требуется.

► *Чтобы настроить передачу в Kaspersky Security Center диагностической информации о результате установки программы, выполните следующие действия:*

1. Перейдите в папку инсталляционного пакета, сформированного средствами Kaspersky Security Center для выбранной программы. Эта папка расположена в папке общего доступа, которая была указана при установке Kaspersky Security Center.

2. Откройте файл с расширением kpd или kud для редактирования (например, с помощью текстового редактора Блокнот Microsoft Windows).

   Файл имеет формат обычного конфигурационного ini-файла.

3. Добавьте в файл следующие строки:

   ```
   [SetupProcessResult]

   Wait=1
   ```

   Эта команда настраивает программу Kaspersky Security Center таким образом, чтобы она ожидала окончания установки программы, для которой сформирован инсталляционный пакет и анализировала код возврата программы установки. Если нужно отключить передачу диагностической информации, установите для ключа Wait значение 0.

4. Внесите описание кодов возврата успешной установки. Для этого добавьте в файл следующие строки:

   ```
   [SetupProcessResult_SuccessCodes]
   ```

<код возврата>=[<описание>]

<код возврата 1>=[<описание>]

…

В квадратных скобках приводятся необязательные ключи.

Синтаксис строк:

- <код возврата>. Любое число, соответствующее коду возврата программы установки. Количество кодов возврата может быть произвольным.
- <описание>. Текстовое описание результата установки. Описание может отсутствовать.

5. Внесите описание кодов возврата для установки, завершенной с ошибкой. Для этого добавьте в файл следующие строки:

   [SetupProcessResult_ErrorCodes]

   <код возврата>=[<описание>]

   <код возврата 1>=[<описание>]

   …

   Синтаксис строк соответствует синтаксису строк кодов возврата при успешной установке.

6. Закройте kpd- или kud-файл, сохранив внесенные изменения.

Информация о результатах установки программы, указанной пользователем, будет записываться в журналах Kaspersky Security Center и отображаться в списке событий, в отчетах и в результатах выполнения задач.

Получение актуальных версий программ

Kaspersky Security Center позволяет получать актуальные версии корпоративных программ, выложенные на интернет-серверах "Лаборатории Касперского".

► *Чтобы получить актуальные версии корпоративных программ "Лаборатории Касперского", выполните следующие действия:*

1. Откройте главное окно Kaspersky Security Center.

2. Откройте окно **Актуальные версии программ** по ссылке **Вышли новые версии программ "Лаборатории Касперского"** в блоке **Развертывание**.

   Ссылка **Вышли новые версии программ "Лаборатории Касперского"** становится доступна, когда Сервер администрирования обнаруживает очередную версию корпоративной программы на интернет-сервере "Лаборатории Касперского".

3. Выберите в списке нужную вам программу.

4. Загрузите дистрибутив программы по ссылке в строке **Веб-адрес дистрибутива**.

   Если для выбранной программы отображается кнопка **Загрузить программы и создать инсталляционные пакеты**, вы можете нажать на эту кнопку для загрузки дистрибутива программы и автоматического создания инсталляционного пакета. В этом случае Kaspersky Security Center загружает дистрибутив программы на Сервер администрирования в папку общего доступа, заданную при установке Kaspersky Security Center. Автоматически созданный инсталляционный пакет отображается в папке **Удаленная установка** дерева консоли, во вложенной папке **Инсталляционные пакеты**.

После закрытия окна **Актуальные версии программ** ссылка **Вышли новые версии программ "Лаборатории Касперского"** исчезает из блока **Развертывание**.

Вы можете создавать инсталляционные пакеты новых версий программ и работать с созданными инсталляционными пакетами в папке **Удаленная установка** дерева консоли, во вложенной папке **Инсталляционные пакеты**.

Вы также можете открыть окно **Актуальные версии программ** по ссылке **Просмотреть актуальные версии программ "Лаборатории Касперского"** в рабочей области папки **Инсталляционные пакеты**.

См. также

Подготовка устройства к удаленной установке. Утилита riprep.exe

Удаленная установка программы на клиентском устройстве может завершаться с ошибкой по следующим причинам:

- Задача ранее уже была успешно выполнена на этом устройстве. В этом случае ее повторное выполнение не требуется.
- Во время запуска задачи устройство было выключено. В этом случае требуется включить устройство и запустить задачу еще раз.
- Отсутствует связь между Сервером администрирования и Агентом администрирования, установленным на клиентском устройстве. Для определения причины проблемы вы можете воспользоваться утилитой удаленной диагностики устройства (klactgui).

- Если на устройстве не установлен Агент администрирования, при удаленной установке программы могут возникнуть следующие проблемы:
  - на клиентском устройстве включен параметр **Простой общий доступ к файлам**;
  - на клиентском устройстве не работает служба Server;
  - на клиентском устройстве закрыты необходимые порты;
  - у учетной записи, под которой выполняется задача, недостаточно прав.

  Для решения проблем, возникших при установке программы на клиентское устройство, на котором не установлен Агент администрирования, вы можете воспользоваться утилитой подготовки устройства к удаленной установке (riprep).

В этом разделе описывается утилита подготовки устройства к удаленной установке (riprep). Она расположена в папке установки Kaspersky Security Center на устройстве с установленным Сервером администрирования.

Утилита подготовки устройства к удаленной установке не работает под управлением операционной системы Microsoft Windows XP Home Edition.

В этом разделе

Подготовка устройства к удаленной установке в интерактивном режиме

► *Чтобы подготовить устройство к удаленной установке в интерактивном режиме, выполните следующие действия:*

1. На клиентском устройстве запустите файл riprep.exe.

2. В открывшемся главном окне утилиты подготовки к удаленной установке установите следующие флажки:

   - **Отключить простой общий доступ к файлам**.
   - **Запустить службу Server**.
   - **Открыть порты**.
   - **Добавить учетную запись**.
   - **Отключить контроль учетных записей (UAC)**. Этот параметр доступен для операционных систем Microsoft Windows Vista, Microsoft Windows 7 и Microsoft Windows Server 2008.

3. Нажмите на кнопку **Запустить**.

   В результате в нижней части главного окна утилиты отображаются этапы подготовки устройства к удаленной установке.

Если вы установили флажок **Добавить учетную запись**, при создании учетной записи будет выведен запрос на ввод имени учетной записи и пароля. В результате будет создана локальная учетная запись, принадлежащая группе локальных администраторов.

Если вы установили флажок **Отключить контроль учетных записей**, попытка отключения контроля учетных записей будет выполняться и в том случае, когда до запуска утилиты контроль учетных записей был отключен. После отключения контроля учетных записей будет выведен запрос на перезагрузку устройства.

Подготовка устройства к удаленной установке в неинтерактивном режиме

► *Чтобы подготовить устройство к удаленной установке в неинтерактивном режиме,*

на клиентском устройстве запустите файл riprep.exe из командной строки с необходимым набором ключей.

Синтаксис утилиты:

```
riprep.exe [-silent] [-cfg CONFIG_FILE] [-tl traceLevel]
```

Описание ключей:

- `-silent` – запуск утилиты в неинтерактивном режиме.
- `-cfg CONFIG_FILE` – определение конфигурации утилиты, где `CONFIG_FILE` – путь к файлу конфигурации (файл с расширением .ini).
- `-tl traceLevel` – задание уровня трассировки, где `traceLevel` – число от 0 до 5. Если ключ не задан, то используется значение 0.

В результате запуска утилиты в неинтерактивном режиме вы можете выполнить следующие задачи:

- отключение простого общего доступа к файлам;
- запуск службы Server на клиентском устройстве;
- открытие портов;
- создание локальной учетной записи;
- отключение контроля учетных записей (UAC).

Вы можете задать параметры подготовки устройства к удаленной установке в конфигурационном файле, указанном в ключе `-cfg`. Чтобы задать эти параметры, в конфигурационный файл нужно добавить следующую информацию:

- В разделе `Common` указать, какие задачи следует выполнять:
  - `DisableSFS` – отключение простого общего доступа к файлам (0 – задача выключена; 1 – задача включена).
  - `StartServer` – запуск службы Server (0 – задача выключена; 1 – задача включена).
  - `OpenFirewallPorts` – открытие необходимых портов (0 – задача выключена; 1 – задача включена).

- `DisableUAC` – отключение контроля учетных записей (0 – задача выключена; 1 – задача включена).
- `RebootType` – определение поведения при необходимости перезагрузки при отключении контроля учетных записей. Вы можете использовать следующие значения параметра:
  - 0 – никогда не перезагружать устройство;
  - 1 – перезагружать устройство, если до запуска утилиты контроль учетных записей был включен;
  - 2 – перезагружать устройство принудительно, если до запуска утилиты контроль учетных записей был включен;
  - 4 – всегда перезагружать устройство;
  - 5 – всегда принудительно перезагружать устройство.
- В разделе `UserAccount` указать имя учетной записи (`user`) и ее пароль (`Pwd`).

Пример содержимого конфигурационного файла:

```
[Common]
DisableSFS=0
StartServer=1
OpenFirewallPorts=1

[UserAccount]
user=Admin
Pwd=Pass123
```

По окончании работы утилиты в папке запуска создаются следующие файлы:

- riprep.txt – отчет о работе, в котором перечислены этапы работы утилиты с причинами их проведения;

- riprep.log – файл трассировки (создается, если заданный уровень трассировки больше 0).

Подготовка устройства с операционной системой Linux к удаленной установке Агента администрирования

► *Чтобы подготовить устройство с операционной системой Linux к удаленной установке Агента администрирования, выполните следующие действия:*

1. Выполните проверку конфигурации устройства:

   a. Проверьте, что возможно подключение к устройству с помощью SSH клиентской программы (например, программа PuTTY).

   Если вы не можете подключиться к устройству, откройте файл /etc/ssh/sshd_config и убедитесь, что следующие параметры имеют значения:

   ```
   PasswordAuthentication no

   ChallengeResponseAuthentication yes
   ```

   Сохраните файл (при необходимости) и перезапустите службу SSH, используя команду sudo service ssh restart.

   b. Отключите пароль запроса Sudo для учетной записи пользователя, которая используется для подключения к устройству.

   Используйте команду sudo visudo, чтобы открыть конфигурационный файл sudoers. В открытом файле укажите: username ALL = (ALL) NOPASSWD: ALL. В этом случае username является учетной записью пользователя, которая будет использоваться для подключения к устройству по протоколу SSH.

   c. Сохраните и закройте файл sudoers.

   d. Повторно подключитесь к устройству через SSH и проверьте, что служба Sudo не требует пароль с помощью команды sudo whoami.

2. Загрузите и создайте инсталляционный пакет:

a. Перед установкой на устройство убедитесь, что на нем установлены зависимости (программы, библиотеки) для данного пакета.

Вы можете самостоятельно посмотреть зависимости для каждого пакета, используя утилиты, специфичные для того дистрибутива Linux, на который будет устанавливаться пакет. С информацией об утилитах вы можете ознакомиться в документации к вашей операционной системе.

b. Загрузите инсталляционный пакет Агент администрирования.

c. Для создания пакета удаленной установки используйте файлы:

- klnagent.kpd;
- akinstall.sh;
- deb или rpm пакет Агента администрирования.

3. Создайте задачу удаленной установки программы с параметрами:

   - В окне **Параметры** мастера создания задачи установите флажок **Средствами операционной системы с помощью Сервера администрирования**. Снимите все остальные флажки.

   - В окне **Выбор учетной записи** для запуска задачи укажите параметры учетной записи, которая используется для подключения к устройству через SSH.

4. Запустите задачу удаленной установки программы.

Установка может завершиться ошибкой, если вы устанавливаете Агент администрирования с использованием протокола SSH на устройства с операционными системами Fedora версии ниже 20. В этом случае для успешной установки Агента администрирования в файле /etc/sudoers закомментируйте параметр Defaults requiretty. Подробное описание того, почему параметр Defaults requiretty может вызвать проблемы при подключении по SSH, вы можете найти на сайте системы отслеживания проблем Bugzilla (https://bugzilla.redhat.com/show_bug.cgi?id=1020147).

Локальная установка программ

В этом разделе описана процедура установки программ, которые могут быть установлены на устройства только локально.

Для проведения локальной установки программ на выбранном клиентском устройстве вам необходимо обладать правами администратора на этом устройстве.

► *Чтобы установить программы локально на выбранное клиентское устройство, выполните следующие действия:*

1. Установите на клиентское устройство Агент администрирования и настройте связь клиентского устройства с Сервером администрирования.

2. Установите на устройство необходимые программы согласно описаниям, изложенным в Руководствах к этим программам.

3. Установите на рабочее место администратора плагин управления для каждой из установленных программ.

Kaspersky Security Center также поддерживает возможность локальной установки программ с помощью автономного пакета установки.

Создание автономных пакетов установки доступно для следующих программ:

- Для рабочих станций:
  - Kaspersky Endpoint Security 10 для Windows;
  - Kaspersky Endpoint Security 10 для Linux;
  - Kaspersky Endpoint Security 10 для Mac;
  - Kaspersky Embedded Systems Security для Windows.
- Для мобильных устройств:
  - Kaspersky Security 10 для мобильных устройств (установка доступна при активации функциональности Управление мобильными устройствами).
- Для почтовых систем и серверов совместной работы:

- Kaspersky Security 8.0 для Linux Mail Server Maintenance Pack 1 (и выше);
- Kaspersky Secure Mail Gateway 1.0;
- Kaspersky Security для Microsoft Exchange Servers;
- Kaspersky Security для SharePoint Server.

- Для файловых серверов:
  - Kaspersky Endpoint Security 10 для Windows;
  - Антивирус Касперского 8.0 для Windows Servers Enterprise Edition;
  - Kaspersky Security 10 для Windows Server;
  - Антивирус Касперского 8.0 для Linux File Server.
  - Антивирус Касперского 10 для Linux File Server.
- Для виртуальных машин:
  - Kaspersky Security для виртуальных сред 3.0 Защита без агента;
  - Kaspersky Security для виртуальных сред 4.0 Защита без агента;
  - Kaspersky Security для виртуальных сред 3.0 Легкий агент;
  - Kaspersky Security для виртуальных сред 4.0 Легкий агент.
- Kaspersky Industrial Cyber Security:
  - Kaspersky Industrial Cyber Security for Networks;
  - Kaspersky Industrial Cyber Security for Nodes.

Вы можете получить сведения о последних версиях программ на веб-сайте Службы технической поддержки, на странице Kaspersky Security Center 10, в разделе Общие понятия (http://support.kaspersky.ru/12029).

В этом разделе

Локальная установка Агента администрирования

► *Чтобы установить Агент администрирования на устройство локально, выполните следующие действия:*

1. На устройстве запустите файл setup.exe из дистрибутива, полученного через интернет.

   Откроется окно с выбором программ "Лаборатории Касперского" для установки.

2. В окне с выбором программ по ссылке **Установить только Агент администрирования Kaspersky Security Center 10** запустите мастер установки Агента администрирования. Следуйте указаниям мастера.

   Во время работы мастера установки вы можете настроить дополнительные параметры Агента администрирования (см. ниже).

3. Чтобы использовать устройство в качестве шлюза соединений для выбранной группы администрирования, в окне **Шлюз соединений** мастера установки выберите вариант **Использовать в качестве шлюза соединений в демилитаризованной зоне**.

4. Чтобы настроить Агент администрирования при установке на виртуальную машину, выполните следующие действия:

a. Включите динамический режим Агента администрирования для Virtual Desktop Infrastructure (VDI). Для этого в окне мастера установки **Дополнительные параметры** установите флажок **Включить динамический режим для VDI**.

b. Оптимизируйте работу Агента администрирования для виртуальной инфраструктуры. Для этого в окне мастера установки **Дополнительные параметры** установите флажок **Оптимизировать параметры Агента администрирования Kaspersky Security Center для виртуальной инфраструктуры.**

В результате будет выключена проверка исполняемых файлов на наличие уязвимостей при запуске устройства. Также будет выключена передача на Сервер администрирования следующей информации:

- о реестре оборудования;
- о программах, установленных на устройстве;
- об обновлениях Microsoft Windows, которые необходимо установить на локальном клиентском устройстве;
- об уязвимостях программного обеспечения, обнаруженных на локальном клиентском устройстве.

В дальнейшем вы сможете включить передачу этой информации в свойствах Агента администрирования или в параметрах политики Агента администрирования.

По окончании работы мастера установки Агент администрирования будет установлен на устройстве.

Вы можете просматривать свойства службы Агента администрирования Kaspersky Security Center, запускать, останавливать и следить за работой Агента администрирования при помощи стандартных средств администрирования Microsoft Windows – Управление компьютером\Службы.

Установка Агента администрирования в неинтерактивном режиме

Агент администрирования может быть установлен в неинтерактивном режиме, то есть без интерактивного ввода параметров установки. Для неинтерактивной установки используется установочный msi-пакет Агента администрирования, расположенный в дистрибутиве программы Kaspersky Security Center в папке Packages\NetAgent\exec.

► *Чтобы установить Агент администрирования на локальном устройстве в неинтерактивном режиме,*

выполните команду

```
msiexec /i "Kaspersky Network Agent.msi"
/qn <setup_parameters>
```

где `setup_parameters` – список параметров и их значений, отделенных друг от друга пробелом (`PRO1=PROP1VAL PROP2=PROP2VAL`).

Имена и возможные значения параметров, которые можно использовать при установке Агента администрирования в неинтерактивном режиме, приведены в разделе Параметры установки Агента администрирования *(на стр.* 256*)*.

Удаленная установка Агента администрирования с помощью инсталляционного пакета или локальная установка в неинтерактивном режиме означает согласие с условиями Лицензионного соглашения на устанавливаемую программу и Политикой конфиденциальности этой программы. Просмотреть Лицензионное соглашение и Политику конфиденциальности на конкретную программу можно в комплекте поставки этой программы или на веб-сайте Службы технической поддержки "Лаборатории Касперского".

См. также

Параметры установки Агента администрирования 256

Параметры установки Сервера администрирования 247

Локальная установка плагина управления программой

► *Чтобы установить плагин управления программой,*

на устройстве, где установлена Консоль администрирования, запустите исполняемый файл klcfginst.exe, входящий в дистрибутивный пакет этой программы.

Файл klcfginst.exe входит в состав всех программ, которыми может управлять Kaspersky Security Center. Установка сопровождается мастером и не требует настройки параметров.

Установка программ в неинтерактивном режиме

► *Чтобы провести установку программы в неинтерактивном режиме, выполните следующие действия:*

1. Откройте главное окно программы Kaspersky Security Center
2. В папке дерева консоли **Удаленная установка** во вложенной папке **Инсталляционные пакеты** выберите инсталляционный пакет нужной программы или сформируйте для этой программы новый инсталляционный пакет.

   Инсталляционный пакет будет сохранен на Сервере администрирования в папке общего доступа в служебной папке Packages. При этом каждому инсталляционному пакету соответствует отдельная вложенная папка.

3. Откройте папку нужного инсталляционного пакета одним из следующих способов:

   - Скопируйте папку, соответствующую нужному инсталляционному пакету, с Сервера администрирования на клиентское устройство. Затем откройте скопированную папку на клиентском устройстве.
   - С клиентского устройства откройте на Сервере администрирования папку общего доступа, соответствующую нужному инсталляционному пакету.

Если папка общего доступа расположена на устройстве с установленной операционной системой Microsoft Windows Vista, необходимо установить значение **Отключен** для параметра **Управление учетными записями пользователей: все администраторы работают в режиме одобрения администратором** (**Пуск** → **Панель управления** → **Администрирование** → **Локальная политика безопасности** → **Параметры безопасности**).

4. В зависимости от выбранной программы выполните следующие действия:

   - Для Антивируса Касперского для Windows Workstations, Антивируса Касперского для Windows Servers и Kaspersky Security Center перейдите во вложенную папку exec и запустите исполняемый файл (файл с расширением exe) с ключом /s.

   - Для остальных программ "Лаборатории Касперского" запустите из открытой папки исполняемый файл (файл с расширением exe) с ключом /s.

   Запуск исполняемого файла с ключами `EULA=1` и `PRIVACYPOLICY=1` означает, что вы принимаете положения Лицензионного соглашения и Политики конфиденциальности соответственно. Текст Лицензионного соглашения и текст Политики конфиденциальности входят в комплект поставки Kaspersky Security Center. Согласие с положениями Лицензионного соглашения и Политики конфиденциальности является необходимым условием для установки программы или обновления предыдущей версии программы.

Установка программ с помощью автономных пакетов

Kaspersky Security Center позволяет формировать автономные пакеты установки программ. Автономный пакет установки представляет собой исполняемый файл, который можно разместить на Веб-сервере, отправить по почте или передать на клиентское устройство другим способом. Полученный файл можно запустить локально на клиентском устройстве для выполнения установки программы без участия Kaspersky Security Center.

► *Чтобы установить программу с помощью автономного пакета установки, выполните следующие действия:*

1. Подключитесь к нужному Серверу администрирования.
2. В папке дерева консоли **Удаленная установка** выберите вложенную папку **Инсталляционные пакеты**.
3. В рабочей области выберите инсталляционный пакет нужной программы.
4. Запустите процесс создания автономного пакета установки одним из следующих способов:
   - в контекстном меню инсталляционного пакета выберите пункт **Создать автономный пакет установки**;
   - по ссылке **Создать автономный пакет установки** в блоке работы с инсталляционным пакетом.

   В результате запускается мастер создания автономного пакета установки. Следуйте его указаниям.

   На завершающем шаге мастера выберите способ передачи автономного пакета установки на клиентское устройство.
5. Передайте автономный пакет установки программы на клиентское устройство.
6. Запустите автономный пакет установки на клиентском устройстве.

В результате программа будет установлена на клиентском устройстве с параметрами, указанными в автономном пакете.

При создании автономный пакет установки автоматически публикуется на Веб-сервере. Ссылка для загрузки автономного пакета отображается в списке созданных автономных пакетов установки. При необходимости вы можете отменить публикацию выбранного автономного пакета и снова опубликовать его на Веб-сервере. По умолчанию для загрузки автономных пакетов установки используется порт 8060.

Параметры инсталляционного пакета Агента администрирования

► *Чтобы настроить параметры инсталляционного пакета Агента администрирования, выполните следующие действия:*

1. В дереве консоли в папке **Удаленная установка** выберите вложенную папку **Инсталляционные пакеты**.

   Папка **Удаленная установка** по умолчанию вложена в папку **Дополнительно**.

2. В контекстном меню инсталляционного пакета Агента администрирования выберите пункт **Свойства**.

Откроется окно свойств инсталляционного пакета Агента администрирования.

Общие

Раздел **Общие** содержит общую информацию об инсталляционном пакете:

- название инсталляционного пакета;
- имя и версию программы, для которой сформирован инсталляционный пакет;
- размер инсталляционного пакета;
- дату создания инсталляционного пакета;
- путь к папке размещения инсталляционного пакета.

Параметры

В этом разделе можно настроить параметры, необходимые для обеспечения работоспособности Агента администрирования сразу после его установки.

В блоке параметров **Папка установки** можно выбрать папку на клиентском устройстве, в которую будет установлен Агент администрирования:

- **Устанавливать в папку по умолчанию**

  Если выбран этот вариант, Агент администрирования будет установлен в папку <Диск>:\Program Files\Kaspersky Lab\NetworkAgent.

Если такой папки нет, она будет создана автоматически.

Этот вариант выбран по умолчанию.

- **Устанавливать в заданную папку**

  Если выбран этот вариант, Агент администрирования будет установлен в папку, указанную в поле ввода.

В блоке параметров ниже можно задать пароль для задачи удаленной деинсталляции Агента администрирования:

- **Использовать пароль деинсталляции**

  Если флажок установлен, при нажатии на кнопку **Изменить** можно ввести пароль для удаления программы (доступно только для Агента администрирования на устройствах под управлением операционных систем семейства Windows).

  По умолчанию флажок снят.

- **Статус**

  Статус пароля: **Пароль установлен** или **Пароль не установлен**.

  По умолчанию пароль не установлен.

- **Устанавливать обновления и патчи для Сервера администрирования и Агента администрирования автоматически**

  Если флажок установлен, то загруженные обновления и патчи для Сервера администрирования, Агента администрирования, Консоли администрирования, Сервера мобильных устройств Exchange ActiveSync и Сервера iOS MDM будут устанавливаться автоматически (автоматическая установка доступна для Агента администрирования начиная с версии Kaspersky Security Center 10 Service Pack 2).

  Если флажок снят, то загруженные обновления и патчи будут установлены только после того, как вы измените их статус на *Одобрен*. Обновления и патчи со статусом *Не определено* не будут установлены.

  По умолчанию флажок установлен.

Подключение

В этом разделе можно настроить параметры подключения Агента администрирования к Серверу администрирования.

- **Адрес сервера**

  Адрес устройства, на котором установлен Сервер администрирования.

- **Номер порта**

  Номер порта, по которому будет выполняться подключение.

- **Номер SSL-порта**

  Номер порта, по которому будет выполняться подключение с использованием протокола SSL.

- **Использовать сертификат Сервера**

  Если флажок установлен, для аутентификации доступа Агента администрирования к Серверу администрирования будет использоваться файл сертификата, который можно указать при нажатии на кнопку **Обзор**.

  Если флажок не установлен, файл сертификата будет получен с Сервера администрирования при первом подключении Агента администрирования по адресу, указанному в поле **Адрес сервера**.

  Не рекомендуется снимать флажок, так как автоматическое получение сертификата Сервера администрирования Агентом администрирования при подключении к Серверу является небезопасным.

  По умолчанию флажок установлен.

- **Использовать SSL-соединение**

  Если флажок установлен, подключение к Серверу администрирования будет выполняться через защищенный порт с использованием SSL-протокола.

  По умолчанию флажок снят.

- **Использовать UDP-порт**

  Если флажок установлен, подключение Агента администрирования к Серверу администрирования будет выполняться через UDP-порт.

  По умолчанию флажок установлен.

- **Номер UDP-порта**

  В поле можно указать номер порта подключения Агента администрирования к Серверу администрирования по протоколу UDP.

  По умолчанию номер UDP-порта – 15000.

- **Открывать порты Агента администрирования в брандмауэре Microsoft Windows**

  Если флажок установлен, после установки Агента администрирования на клиентском устройстве в список исключений брандмауэра Microsoft Windows будет добавлен UDP-порт, необходимый для работы Агента администрирования.

  По умолчанию флажок установлен.

Дополнительно

В разделе **Дополнительно** можно настроить параметры использования шлюза соединений:

- **Использовать в качестве шлюза соединений в демилитаризованной зоне**

  Если флажок установлен, Агент администрирования будет использоваться в качестве шлюза соединений в демилитаризованной зоне.

  По умолчанию флажок снят.

- **Подключаться к Серверу администрирования через шлюз соединений**

  Если флажок установлен, Агент администрирования будет подключаться к Серверу администрирования через шлюз соединений.

  По умолчанию флажок снят.

- **Адрес шлюза соединений**

В поле ввода можно указать адрес устройства, который будет использоваться в качестве шлюза соединений.

Поле недоступно, когда снят флажок **Подключаться к Серверу администрирования через шлюз соединений**.

- **Включить динамический режим для VDI**

  Если флажок установлен, для Агента администрирования, установленого на виртуальной машине,будет включен динамический режим для Virtual Desktop Infrastructure (VDI).

  По умолчанию флажок снят.

- **Оптимизировать параметры для VDI**.

Если флажок установлен, в параметрах Агента администрирования выключены следующие функции:

- получение информации об установленном программном обеспечении;
- получение информации об аппаратном обеспечении;
- получение информации о наличии уязвимостей;
- получение информации о необходимых обновлениях.

  По умолчанию флажок снят.

Дополнительные компоненты

В этом разделе можно выбрать дополнительные компоненты для совместной установки с Агентом администрирования.

Теги

В разделе **Теги** отображается список ключевых слов (тегов), которые можно добавлять клиентским устройствам после установки на них Агента администрирования. Вы можете добавлять и удалять теги из списка, а также переименовывать теги.

Если рядом с тегом установлен флажок, тег будет автоматически добавлен управляемым устройствам при установке на них Агента

администрирования.

Если флажок рядом с тегом снят, тег не будет автоматически добавлен управляемым устройствам при установке на них Агента администрирования. Этот тег можно добавить устройствам вручную.

При удалении тега из списка тег автоматически снимается со всех устройств, которым он добавлен.

История ревизий

В этом разделе можно посмотреть историю ревизий инсталляционного пакета. Вы можете сравнивать ревизии, просматривать ревизии, сохранять ревизии в файл, добавлять и изменять описания ревизий.

Настройка профилей соединения для автономных пользователей

При работе автономных пользователей, использующих ноутбуки (далее также "устройства") может понадобиться изменить способ подключения к Серверу администрирования или переключиться между Серверами администрирования в зависимости от текущего положения устройства в сети.

Использование различных адресов одного и того же Сервера администрирования

Описанное ниже применимо только для Kaspersky Security Center 10 Service Pack 1 и выше.

Устройства с установленным Агентом администрирования могут в разные периоды времени подключаться к Серверу администрирования как из внутренней сети организации, так и из интернета. В этой ситуации может потребоваться, чтобы Агент администрирования использовал различные адреса для подключения к Серверу администрирования: внешний адрес Сервера при подключении из интернета и внутренний адрес Сервера при подключении из внутренней сети.

Для этого в свойствах политики Агента администрирования (раздел **Сеть**, вложенный раздел **Подключение**) нужно добавить профиль подключения к Серверу администрирования из интернета. В окне создания профиля необходимо снять флажок **Использовать только для получения обновлений** и установить флажок **Синхронизировать параметры подключения с параметрами Сервера, указанными в этом профиле**. Если для доступа к Серверу администрирования используется шлюз соединений (например, в конфигурации Kaspersky Security Center вида Доступ из интернета: Агент администрирования в качестве шлюза соединений в демилитаризованной зоне (на стр. 95)), в профиле подключения следует указать адрес шлюза соединений в соответствующем поле.

Переключение между Серверами администрирования в зависимости от текущей сети

> Описанное ниже применимо для Kaspersky Security Center 10 Service Pack 2 Maintenance Release 1 и выше.

Если в организации несколько офисов с различными Серверами администрирования и между ними перемещается часть устройств с установленным Агентом администрирования, то необходимо, чтобы Агент администрирования подключался к Серверу администрирования локальной сети того офиса, в котором находится устройство.

В этом случае в свойствах политики Агента администрирования следует создать профиль подключения к Серверу администрирования для каждого из офисов, за исключением домашнего офиса, в котором расположен исходный домашний Сервер администрирования. В профилях подключения следует указать адреса соответствующих Серверов администрирования и установить либо снять флажок **Использовать только для получения обновлений**:

- установить флажок, если требуется, чтобы Агент администрирования синхронизировался с домашним Сервером администрирования, а локальный Сервер использовался только для загрузки обновлений;
- снять флажок, если необходимо, чтобы Агент администрирования полностью управлялся локальным Сервером администрирования.

Далее необходимо настроить условия переключения на созданные профили: не менее одного условия для каждого из офисов, исключая "домашний офис". Смысл каждого такого

условия заключается в обнаружении в сетевом окружении деталей, присущих одному из офисов. Если условие становится истинным, происходит активация соответствующего профиля. Если ни одно из условий не является истинным, Агент администрирования переключается на домашний Сервер администрирования.

См. также

Предоставление доступа к Серверу администрирования из интернета 92

Доступ из интернета: Агент администрирования в качестве шлюза соединений в демилитаризованной зоне 95

Развертывание систем управления мобильными устройствами

В этом разделе описано развертывание систем управления мобильных устройств по протоколам Exchange ActiveSync, iOS MDM и Kaspersky Endpoint Security.

В этом разделе

Развертывание системы управления по протоколу Exchange ActiveSync

Kaspersky Security Center позволяет управлять мобильными устройствами, которые подключаются к Серверу администрирования по протоколу Exchange ActiveSync. Мобильными устройствами Exchange ActiveSync (EAS-устройствами) называются мобильные устройства, подключенные к Серверу мобильных устройств Exchange ActiveSync и находящиеся под управлением Сервера администрирования.

Протокол Exchange ActiveSync поддерживают следующие операционные системы:

- Windows Mobile;
- Windows CE;

- Windows Phone® 7;
- Windows Phone 8;
- Android;
- Bada;
- BlackBerry® 10;
- iOS®;
- Symbian.

> Набор параметров управления устройством Exchange ActiveSync зависит от операционной системы, под управлением которой находится мобильное устройство. С особенностями поддержки протокола Exchange ActiveSync для конкретной операционной системы можно ознакомиться в документации для этой операционной системы.

Развертывание системы управления мобильными устройствами по протоколу Exchange ActiveSync выполняется в следующей последовательности:

1. Администратор устанавливает на выбранное клиентское устройство Сервер мобильных устройств Exchange ActiveSync (см. раздел "Установка Сервера мобильных устройств Exchange ActiveSync" на стр. 316).
2. Администратор создает в Консоли администрирования профиль (профили) управления EAS-устройствами и добавляет профиль к почтовым ящикам пользователей Exchange ActiveSync.

   > *Профиль управления мобильными устройствами Exchange ActiveSync* – это политика ActiveSync, которая используется на сервере Microsoft Exchange для управления мобильными устройствами Exchange ActiveSync. Почтовому ящику Microsoft Exchange можно назначить только один профиль управления EAS-устройствами.

   Пользователи мобильных EAS-устройств подключаются к своим почтовым ящикам Exchange. Профиль управления накладывает ограничения на мобильные устройства

(см. раздел "Подключение мобильных устройств к Серверу мобильных устройств Exchange ActiveSync" на стр. 318).

В этом разделе

Установка Сервера мобильных устройств Exchange ActiveSync

Сервер мобильных устройств Exchange ActiveSync устанавливается на клиентское устройство с установленным сервером Microsoft Exchange. Рекомендуется устанавливать Сервер мобильных устройств Exchange ActiveSync на сервер Microsoft Exchange с ролью Client Access. Если в одном домене несколько серверов Microsoft Exchange с ролью Client Access объединены в массив (Client Access Array), то рекомендуется устанавливать Сервер мобильных устройств Exchange ActiveSync в режиме кластера на каждый сервер Microsoft Exchange в массиве.

► *Чтобы установить Сервер мобильных устройств Exchange ActiveSync на локальном устройстве, выполните следующие действия:*

1. Запустите исполняемый файл setup.exe.

   Откроется окно с выбором программ "Лаборатории Касперского" для установки.

2. В окне с выбором программ по ссылке **Установить Сервер мобильных устройств Exchange ActiveSync** запустите мастер установки Сервера мобильных устройств Exchange ActiveSync.

3. В окне **Настройка установки** выберите тип установки Сервера мобильных устройств Exchange ActiveSync:

   - Если вы хотите установить Сервер мобильных устройств Exchange ActiveSync с использованием параметров по умолчанию, выберите вариант **Стандартная установка** и нажмите на кнопку **Далее**.

   - Если вы хотите задать вручную значения параметров установки Сервера мобильных устройств Exchange ActiveSync, выберите вариант **Расширенная установка** и нажмите на кнопку **Далее**. Затем выполните следующие действия:

     a. В окне **Папка назначения** выберите папку назначения. По умолчанию это <Диск>:\Program Files\Kaspersky Lab\Mobile Device Management for Exchange. Если такой папки нет, она будет создана автоматически в процессе установки. Вы можете сменить папку назначения с помощью кнопки **Обзор**.

     b. В окне **Режим установки** выберите режим установки Сервера мобильных устройств Exchange ActiveSync: обычный режим или режим кластера.

     c. В окне **Выбор учетной записи** выберите учетную запись, которая будет использоваться для управления мобильными устройствами:

        - **Создать учетную запись и ролевую группу автоматически**. Учетная запись будет создана автоматически.
        - **Указать учетную запись**. Учетную запись следует выбрать вручную. С помощью кнопки **Выбрать** укажите пользователя, чья учетная запись будет использоваться, и пароль. Выбранный пользователь должен входить в группу с правами на управление мобильными устройствами через ActiveSync.

     d. В окне **Настройка IIS** разрешите или запретите автоматическую настройку параметров веб-сервера Internet Information Services (IIS).

> Если вы запретили автоматическую настройку параметров IIS, включите вручную механизм аутентификации "Windows authentication" в параметрах IIS для виртуальной директории PowerShell. Если механизм аутентификации "Windows authentication" не будет включен, установленный Сервер мобильных устройств Exchange ActiveSync будет неработоспособен. Информацию о работе с параметрами IIS можно прочитать в документации для этого веб-сервера.

e. Нажмите на кнопку **Далее**.

4. В открывшемся окне проверьте значения параметров установки Сервера мобильных устройств Exchange ActiveSync и нажмите на кнопку **Установить**.

В результате работы мастера будет выполнена установка Сервера мобильных устройств Exchange ActiveSync на локальное устройство. Сервер мобильных устройств Exchange ActiveSync будет отображаться в папке **Управление мобильными устройствами** дерева консоли.

Подключение мобильных устройств к Серверу мобильных устройств Exchange ActiveSync

Перед подключением мобильных устройств должен быть настроен Microsoft Exchange Server для возможности соединения устройств по протоколу ActiveSync.

Чтобы подключить мобильное устройство к Серверу мобильных устройств Exchange ActiveSync, пользователь с мобильного устройства подключается к своему почтовому ящику Microsoft Exchange, используя ActiveSync. При подключении пользователь в клиенте ActiveSync должен указать параметры подключения, например, адрес электронной почты, пароль электронной почты.

Мобильное устройство пользователя, подключенное к серверу Microsoft Exchange, отображается в папке **Мобильные устройства**, вложенной в папку **Управление мобильными устройствами** дерева консоли.

После подключения мобильного устройства Exchange ActiveSync к Серверу мобильных устройств Exchange ActiveSync администратор может управлять подключенным мобильным устройством Exchange ActiveSync.

Настройка веб-сервера Internet Information Services

При использовании Microsoft Exchange Server версий 2010 и 2013 в настройках веб-сервера Internet Information Services (IIS) необходимо активировать механизм аутентификации Windows для виртуальной директории Windows PowerShell™. Активация этого механизма аутентификации выполняется автоматически, если в мастере установки Сервера мобильных устройств Exchange ActiveSync установлен флажок **Автоматическая настройка IIS** (поведение по умолчанию).

В противном случае необходимо активировать механизм аутентификации самостоятельно.

► *Чтобы активировать механизм аутентификации Windows для виртуальной директории PowerShell вручную, выполните следующие действия:*

1. В консоли Internet Information Services Manager откройте свойства виртуальной директории PowerShell.
2. Перейдите в раздел **Authentication**.
3. Выберите **Windows authentication**, нажмите на кнопку **Enable**.
4. Откройте дополнительные параметры **Advanced Settings**.
5. Установите флажок **Enable Kernel-mode authentication**.
6. В раскрывающемся списке **Extended Protection** выберите **Required**.

При использовании Microsoft Exchange Server версии 2007 настройка веб-сервера IIS не требуется.

Локальная установка Сервера мобильных устройств Exchange ActiveSync

Для локальной установки Сервера мобильных устройств Exchange ActiveSync

администратор должен выполнить следующие действия:

1. Из дистрибутива Kaspersky Security Center скопировать содержимое папки \Server\Packages\MDM4Exchange\ на клиентское устройство.

2. Запустить исполняемый файл setup.exe.

Локальная установка подразумевает два типа инсталляции:

- Стандартная установка – упрощенная установка, не требующая со стороны администратора настройки каких-либо параметров, рекомендуется в большинстве случаев;

- Расширенная установка – установка, требующая от администратора настройки следующих параметров:

  - путь для установки Сервера мобильных устройств Exchange ActiveSync;

  - режим работы Сервера мобильных устройств Exchange ActiveSync: обычный или в режиме кластера (см. раздел "Способы развертывания Сервера мобильных устройств Exchange ActiveSync" на стр. 103);

  - возможность указания учетной записи, под которой будет работать служба Сервера мобильных устройств Exchange ActiveSync (см. раздел "Учетная запись для работы службы Exchange ActiveSync" на стр. 104);

  - включение / выключение автоматической настройки веб-сервера IIS.

Мастер установки Сервера мобильных устройств Exchange ActiveSync следует запускать под учетной записью, обладающей необходимыми правами (см. раздел "Необходимые права для развертывания Сервера мобильных устройств Exchange ActiveSync" на стр. 104).

Удаленная установка Сервера мобильных устройств Exchange ActiveSync

► *Для настройки удаленной установки Сервера мобильных устройств Exchange ActiveSync администратор должен выполнить следующие действия:*

1. В дереве Консоли администрирования Kaspersky Security Center выбрать папку **Удаленная установка**, в ней вложенную папку **Инсталляционные пакеты**.

2. Во вложенной папке **Инсталляционные пакеты** открыть свойства пакета **Сервер мобильных устройств Exchange ActiveSync**.

3. Перейти в раздел **Параметры**.

   В разделе содержатся те же параметры, что и для локальной установки программы.

После настройки удаленной установки можно приступить к установке Сервера мобильных устройств Exchange ActiveSync.

► *Для установки Сервера мобильных устройств Exchange ActiveSync необходимо выполнить следующие действия:*

1. В дереве Консоли администрирования Kaspersky Security Center выбрать папку **Удаленная установка**, в ней вложенную папку **Инсталляционные пакеты**.

2. Во вложенной папке **Инсталляционные пакеты** выбрать пакет **Сервер мобильных устройств Exchange ActiveSync**.

3. Открыть контекстное меню пакета и выбрать пункт **Установить программу**.

4. В открывшемся мастере удаленной установки выбрать одно устройство (или несколько устройств при установке в режиме кластера).

5. В поле **Запускать инсталлятор программы под указанной учетной записью** указать учетную запись, под которой будет запущен процесс установки на удаленном устройстве.

   Учетная запись должна обладать необходимыми правами (см. раздел "Необходимые права для развертывания Сервера мобильных устройств Exchange ActiveSync" на стр. 104).

Развертывание системы управления по протоколу iOS MDM

Kaspersky Security Center позволяет управлять мобильными устройствами на платформе iOS. Мобильными устройствами iOS MDM называются мобильные устройства iOS, подключенные к Серверу iOS MDM и находящиеся под управлением Сервера администрирования.

Подключение мобильных устройств к Серверу iOS MDM выполняется в следующей последовательности:

1. Администратор устанавливает на выбранное клиентское устройство Сервер iOS MDM. Установка Сервера iOS MDM выполняется штатными средствами операционной системы.

2. Администратор получает сертификат Apple Push Notification Service (APNs-сертификат) (см. раздел "Получение APNs-сертификата" на стр. 337).

   APNs-сертификат позволяет Серверу администрирования подключаться к серверу APNs для отправки push-уведомлений на мобильные устройства iOS MDM.

3. Администратор устанавливает на Сервере iOS MDM APNs-сертификат (см. раздел "Установка сертификата APNs на Сервер iOS MDM" на стр. 342).

4. Администратор формирует iOS MDM-профиль для пользователя мобильного устройства iOS.

   iOS MDM-профиль содержит набор параметров подключения мобильных устройств iOS к Серверу администрирования.

5. Администратор выписывает пользователю общий сертификат (см. раздел "Выписка и установка общего сертификата на мобильное устройство" на стр. 345).

   Общий сертификат необходим для подтверждения того, что мобильное устройство принадлежит пользователю.

6. Пользователь переходит по ссылке, высланной администратором, и загружает установочный пакет на мобильное устройство.

   Установочный пакет содержит сертификат и iOS MDM-профиль.

   После загрузки iOS MDM-профиля и синхронизации с Сервером администрирования мобильное устройство iOS MDM отображается в папке **Мобильные устройства**, вложенной в папку **Управление мобильными устройствами** дерева консоли.

7. Администратор добавляет конфигурационный профиль на Сервер iOS MDM и после подключения мобильного устройства устанавливает на него конфигурационный профиль.

Конфигурационный профиль содержит набор параметров и ограничений для мобильного устройства iOS MDM, например, параметры установки приложений и использования различных функций мобильного устройства, параметры работы с электронной почтой и календарем. Конфигурационный профиль позволяет настраивать мобильные устройства iOS MDM в соответствии с политиками безопасности организации.

8. При необходимости администратор добавляет на Сервер iOS MDM provisioning-профили, а затем устанавливает provisioning-профили на мобильные устройства.

   Provisioning-профиль – это профиль, который используется для управления приложениями, распространяемыми не через App Store®. Provisioning-профиль содержит информацию о лицензии и привязан к конкретному приложению.

В этом разделе

Установка Сервера iOS MDM

► *Чтобы установить Сервер iOS MDM на локальное устройство, выполните следующие действия:*

1. Запустите исполняемый файл setup.exe.

   Откроется окно с выбором программ "Лаборатории Касперского" для установки.

   В окне с выбором программ по ссылке **Установить Сервер iOS MDM** запустите мастер установки Сервера iOS MDM.

2. Выберите папку назначения.

Папка назначения по умолчанию <Диск>:\Program Files\Kaspersky Lab\Mobile Device Management for iOS. Если такой папки нет, она будет создана автоматически в процессе установки. Вы можете изменить папку назначения с помощью кнопки **Обзор**.

3. В окне мастера **Параметры подключения к Серверу iOS MDM** в поле **Внешний порт подключения к службе iOS MDM** укажите внешний порт для подключения мобильных устройств к службе iOS MDM.

   Внешний порт 5223 используется мобильными устройствами для связи с APNs-сервером. Убедитесь, что в сетевом экране открыт порт 5223 для подключения к диапазону адресов 17.0.0.0/8.

   Для подключения устройства к Серверу iOS MDM по умолчанию используется порт 443. Если порт 443 уже используется другим сервисом или приложением, то его можно изменить, например, на порт 9443.

   Сервер iOS MDM использует внешний порт 2195 для отправки уведомлений на APNs-сервер.

   APNs-серверы работают в режиме сбалансированной нагрузки. Мобильные устройства не всегда подключаются к одним и тем же IP-адресам для получения уведомлений. Диапазон адресов 17.0.0.0/8 назначен компании Apple, поэтому рекомендуется указать весь этот диапазон как разрешенный в параметрах сетевого экрана.

4. Если вы хотите вручную настроить порты для взаимодействия между компонентами программы, установите флажок **Настроить локальные порты вручную**, а затем укажите значения следующих параметров:

   - **Порт подключения к Агенту администрирования**. Укажите в поле порт подключения службы iOS MDM к Агенту администрирования. По умолчанию используется порт 9799.
   - **Порт подключения к службе iOS MDM**. Укажите в поле локальный порт подключения Агента администрирования к службе iOS MDM. По умолчанию используется порт 9899.

Рекомендуется использовать значения по умолчанию.

5. В окне мастера **Внешний адрес Сервера мобильных устройств** в поле **Веб-адрес удаленного соединения с Сервером мобильных устройств** укажите адрес клиентского устройства, на котором будет установлен Сервер iOS MDM.

   Этот адрес будет использоваться для подключения управляемых мобильных устройств к службе iOS MDM. Клиентское устройство должно быть доступно для подключения к нему iOS MDM-устройств.

   Вы можете указать адрес клиентского устройства в одном из следующих форматов:

   - FQDN-имя устройства (например, mdm.example.com);
   - NetBIOS-имя устройства;
   - IP-адрес устройства.

   Не следует включать в строку с адресом URL-схему и номер порта: эти значения будут добавлены автоматически.

В результате работы мастера Сервер iOS MDM будет установлен на локальное устройство. Сервер iOS MDM отображается в папке **Управление мобильными устройствами** дерева консоли.

Установка Сервера iOS MDM в неинтерактивном режиме

Kaspersky Security Center позволяет устанавливать Сервер iOS MDM на локальное устройство в неинтерактивном режиме, то есть без интерактивного ввода параметров установки.

► *Чтобы установить Сервер iOS MDM на локальное устройство в неинтерактивном режиме,*

выполните команду

```
.\exec\setup.exe /s /v"DONT_USE_ANSWER_FILE=1 EULA=1
```

```
PRIVACYPOLICY=1 <setup_parameters>”
```

где `setup_parameters` – перечень параметров и их значений, отделенных друг от друга пробелом (`PRO1=PROP1VAL PROP2=PROP2VAL`). Файл setup.exe расположен в папке Server внутри дистрибутива программы Kaspersky Security Center.

Имена и возможные значения параметров, которые можно использовать при установке Сервера iOS MDM в неинтерактивном режиме, приведены в таблице ниже. Параметры можно указывать в любом порядке.

Таблица 30. Параметры установки Сервера iOS MDM в неинтерактивном режиме

Имя параметра	Описание параметра	Возможные значения
EULA	Согласие с условиями Лицензионного соглашения. Параметр является обязательным.	• 1 – согласны с условиями Лицензионного соглашения. • Другое значение или не задано – не согласны с условиями Лицензионного соглашения (установка не выполняется).
PRIVACYPOLICY	Согласие с условиями Политики конфиденциальности. Параметр является обязательным.	• 1 – согласны с условиями Политики конфиденциальности. • Другое значение или не задано – не согласны с условиями Политики конфиденциальности (установка не выполняется).
DONT_USE_ANSWER_FILE	Использовать xml-файл с параметрами установки Сервера iOS MDM или нет. xml-файл идет в комплекте с инсталляционным пакетом или находится на Сервере администрирования. Дополнительно путь к файлу указывать не нужно. Параметр является обязательным.	• 1 – не использовать xml-файл с параметрами. • Другое значение или не задано – использовать xml-файл с параметрами.

Имя параметра	Описание параметра	Возможные значения
INSTALLDIR	Папка установки Сервера iOS MDM. Параметр не является обязательным.	Строковое значение, например, `INSTALLDIR=\"C:\install\".`
CONNECTORPORT	Локальный порт подключения службы iOS MDM к Агенту администрирования. По умолчанию используется порт 9799. Параметр не является обязательным.	Числовое значение.
LOCALSERVERPORT	Локальный порт подключения Агента администрирования к службе iOS MDM. По умолчанию используется порт 9899. Параметр не является обязательным.	Числовое значение.

Имя параметра	Описание параметра	Возможные значения
EXTERNALSERVERPORT	Порт для подключения устройства к Серверу iOS MDM. По умолчанию используется порт 443. Параметр не является обязательным.	Числовое значение.
EXTERNAL_SERVER_URL	Внешний адрес клиентского устройства, на котором будет установлен Сервер iOS MDM. Этот адрес будет использоваться для подключения управляемых мобильных устройств к службе iOS MDM. Клиентское устройство должно быть доступно для подключения к нему iOS MDM. Адрес не должен включать URL-схему и номер порта: эти значения будут добавлены автоматически. Параметр не является обязательным.	• FQDN-имя устройства (например, mdm.example.com). • NetBIOS-имя устройства. • IP-адрес устройства.

Имя параметра	Описание параметра	Возможные значения
WORKFOLDER	Рабочая папка Сервера iOS MDM. Если рабочая папка не указана, данные будут записаны в папку по умолчанию. Параметр не является обязательным.	Строковое значение, например, `WORKFOLDER=\"C:\work\".`
MTNCY	Использование Сервера iOS MDM несколькими виртуальными Серверами. Параметр не является обязательным.	• 1 – Сервер iOS MDM будет использоваться несколькими виртуальными Серверами администрирования. • другое значение или не задано – Сервер iOS MDM не будет использоваться несколькими виртуальными Серверами администрирования.

Пример:

```
\exec\setup.exe /s /v"EULA=1 PRIVACYPOLICY=1 DONT_USE_ANSWER_FILE=1
EXTERNALSERVERPORT=9443 EXTERNAL_SERVER_URL=\"www.test-mdm.com\""
```

Параметры установки Сервера iOS MDM подробно описаны в разделе "Установка Сервера iOS MDM (на стр. 324)".

Схемы развертывания Сервера iOS MDM

Количество установленных копий Сервера iOS MDM может быть выбрано как исходя из наличия доступного аппаратного обеспечения, так и в зависимости от общего количества обслуживаемых мобильных устройств.

Следует учесть, что на одну установку Kaspersky Device Management для iOS рекомендуется не более 50 000 мобильных устройств. С целью уменьшения нагрузки все множество устройств можно распределить между несколькими серверами с установленным Сервером iOS MDM.

Аутентификация iOS MDM-устройств осуществляется при помощи сертификатов пользователей (профиль, устанавливаемый на устройство, содержит сертификат того пользователя, которому оно принадлежит). Поэтому возможны две схемы развертывания Сервера iOS MDM:

- упрощенная схема;
- схема развертывания с использованием принудительного делегирования Kerberos Constrained Delegation (KCD).

Ниже рассмотрены обе схемы развертывания.

См. также:

Упрощенная схема развертывания

При развертывании Сервера iOS MDM по упрощенной схеме мобильные устройства напрямую подключаются к веб-сервису iOS MDM. При этом для аутентификации устройств могут быть использованы только пользовательские сертификаты, выпущенные Сервером администрирования. Интеграция с Public Key Infrastructure (PKI) для пользовательских сертификатов невозможна (см. раздел "Типовая конфигурация: Kaspersky Device Management для iOS в демилитаризованной зоне" на стр. 108).

Схема развертывания с использованием принудительного делегирования Kerberos (KCD)

Для использования схемы развертывания с принудительным делегированием Kerberos Сервер администрирования и Сервер iOS MDM должны располагаться во внутренней сети организации.

Эта схема развертывания предполагает:

- интеграцию с Microsoft Forefront Threat Management Gateway (далее TMG);
- использование для аутентификации мобильных устройств принудительного делегирования Kerberos Constrained Delegation;
- интеграцию с инфраструктурой открытых ключей (PKI) для использования пользовательских сертификатов.

При использовании этой схемы развертывания следует учесть следующее:

- В Консоли администрирования в настройках веб-сервиса iOS MDM необходимо установить флажок **Обеспечить совместимость с Kerberos Constrained Delegation**.
- В качестве сертификата веб-сервиса iOS MDM следует указать особый (кастомизированный) сертификат, заданный на TMG при публикации веб-сервиса iOS MDM.
- Пользовательские сертификаты для iOS-устройств должны выписываться доменным Центром сертификации (Certification authority, далее CA). Если в домене несколько корневых CA, то пользовательские сертификаты должны быть выписаны CA, указанным при публикации веб-сервиса iOS MDM на TMG.

  Обеспечить соответствие пользовательского сертификата указанному требованию возможно несколькими способами:

  - Указать пользовательский сертификат в мастере создания iOS MDM-профиля и в мастере установки сертификатов.
  - Интегрировать Сервер администрирования с доменным PKI и настроить соответствующий параметр в правилах выписки сертификатов:

1. В дереве консоли откройте папку **Управление мобильными устройствами** и выберите вложенную папку **Сертификаты**.
2. В рабочей области папки **Сертификаты** по кнопке **Настроить правила выписки сертификатов** откройте окно **Правила выпуска сертификатов**.
3. В разделе **Интеграция с PKI** настройте интеграцию с инфраструктурой открытых ключей.
4. В разделе **Выпуск сертификатов общего типа** укажите источник сертификатов.

См. разделы:

- Типовая конфигурация: Сервер iOS MDM в локальной сети организации (на стр. 109);
- Интеграция с Public Key Infrastructure (на стр. 357).

Рассмотрим пример настройки ограниченного делегирования KCD со следующими допущениями:

- веб-сервис iOS MDM запущен на 443 порте;
- имя устройства с TMG – tmg.mydom.local;
- имя устройства с веб-сервисом iOS MDM – iosmdm.mydom.local;
- имя внешней публикации веб-сервиса iOS MDM – iosmdm.mydom.global.

Service Principal Name для http/iosmdm.mydom.local

В домене требуется прописать Service Principal Name (SPN) для устройства с веб-сервисом iOS MDM (iosmdm.mydom.local):

setspn -a http/iosmdm.mydom.local iosmdm

Настройка доменных свойств устройств с TMG (tmg.mydom.local)

Для делегирования трафика доверить устройство с TMG (tmg.mydom.local) службе, определенной по SPN (http/iosmdm.mydom.local).

► *Чтобы доверить устройство с TMG службе, определенной по SPN (http/iosmdm.mydom.local), администратор должен выполнить следующие действия:*

1. В оснастке Microsoft Management Console "Active Directory Users and Computers" необходимо выбрать устройство с установленным TMG (tmg.mydom.local).

2. В свойствах устройство на закладке **Delegation** для переключателя **Trust this computer for delegation to specified service only** выбрать вариант **Use any authentication protocol**.

3. В список **Services to which this account can present delegated credentials** добавить SPN http/iosmdm.mydom.local.

Особый (кастомизированный) сертификат для публикуемого веб-сервиса (iosmdm.mydom.global)

Требуется выписать особый (кастомизированный) сертификат для веб-сервиса iOS MDM на FQDN iosmdm.mydom.global и указать его взамен сертификата по умолчанию в настройках веб-сервиса iOS MDM в Консоли администрирования.

Следует учесть, что в контейнере с сертификатом (файл с расширением p12 или pfx) также должна присутствовать цепочка корневых сертификатов (публичные части).

Публикации веб-сервиса iOS MDM на TMG

На TMG для трафика, идущего со стороны мобильного устройства на 443 порт iosmdm.mydom.global, необходимо настроить KCD на SPN http/iosmdm.mydom.local с использованием сертификата, выписанного для FQDN iosmdm.mydom.global. При этом следует учесть, что как на публикации, так и на публикуемом веб-сервисе должен быть один и тот же серверный сертификат.

Использование Сервера iOS MDM несколькими виртуальными Серверами

► *Чтобы включить использование Сервера iOS MDM несколькими виртуальными Серверами администрирования, выполните следующие действия:*

1. Откройте системный реестр клиентского устройства, на котором установлен Сервер iOS MDM, например, локально с помощью команды regedit в меню **Пуск** → **Выполнить**.

2. Перейдите в раздел:

   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0

3. Для ключа ConnectorFlags (DWORD) установите значение 02102482.

4. Перейдите в раздел:

   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1103\1.0.0.0

5. Для ключа ConnInstalled (DWORD) установите значение 00000001.

6. Перезапустите службу Сервера iOS MDM.

Задавать значения ключей необходимо в указанной последовательности.

Получение APNs-сертификата

После создания Certificate Signing Request (далее CSR-запрос) на первом шаге мастера получения APNs-сертификата приватная часть будущего сертификата (private key) сохраняется в оперативной памяти устройства. Поэтому все шаги мастера должны быть завершены в рамках одной сессии работы с программой.

► *Чтобы получить APNs-сертификат, выполните следующие действия:*

1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Серверы мобильных устройств**.

2. В рабочей области папки **Серверы мобильных устройств** выберите Сервер iOS MDM.

3. В контекстном меню Сервера iOS MDM выберите пункт **Свойства**.

   Откроется окно свойств Сервера iOS MDM.

4. В окне свойств Сервера iOS MDM выберите раздел **Сертификаты**.

5. В разделе **Сертификаты** в блоке параметров **Сертификат Apple Push Notification** нажмите на кнопку **Запросить новый**.

   Запустится мастер получения APNs-сертификата, откроется окно **Запросить новый**.

6. Создайте Certificate Signing Request (далее CSR-запрос). Для этого выполните следующие действия:

   a. Нажмите на кнопку **Создать CSR**.

   b. В открывшемся окне **Создание CSR** укажите название запроса, название компании и департамента, город, область и страну.

   c. Нажмите на кнопку **Сохранить** и укажите имя файла, в котором будет сохранен CSR-запрос.

   Приватная часть (private key) будущего сертификата будет сохранена в памяти устройства.

7. Отправьте созданный файл с CSR-запросом на подпись в "Лабораторию Касперского" через ваш CompanyAccount.

   > Подписание CSR-запроса доступно только после загрузки на портал CompanyAccount ключа, разрешающего использование функциональности Управление мобильными устройствами.

   После обработки вашего электронного запроса вы получите файл CSR-запроса, подписанный "Лабораторией Касперского".

8. Отправьте подписанный файл CSR-запроса на веб-сайт Apple Inc. https://identity.apple.com/pushcert, используя произвольный Apple ID.

   > Не рекомендуется использовать персональный Apple ID. Создайте отдельный Apple ID, чтобы использовать его как корпоративный. Созданный Apple ID привяжите к почтовому ящику организации, а не отдельного сотрудника.

   После обработки CSR-запроса в Apple Inc. вы получите публичную часть APNs-сертификата. Сохраните полученный файл на диск.

9. Экспортируйте APNs-сертификат вместе с приватным ключом, созданным при формировании CSR-запроса, в файл формата PFX. Для этого выполните следующие действия:

   a. В окне **Запрос нового APNs-сертификата** нажмите на кнопку **Завершить CSR**.

   b. В открывшемся окне **Открыть** выберите файл с публичной частью сертификата, полученный после обработки CSR-запроса в Apple Inc., и нажмите на кнопку **Открыть**.

   Запустится экспорт сертификата.

   c. В открывшемся окне введите пароль для приватного ключа, нажмите на кнопку **ОК**.

   Заданный пароль будет использоваться для установки APNs-сертификата на Сервер iOS MDM.

   d. В открывшемся окне **Сохранение APNs-сертификата** укажите имя файла для сохранения APNs-сертификата, выберите папку, в которую он будет сохранен, и нажмите на кнопку **Сохранить**.

Приватная и публичная части сертификата будут объединены, APNs-сертификат будет сохранен в файл формата PFX. После этого можно установить полученный APNs-сертификат на Сервер iOS MDM (см. раздел "Установка сертификата APNs на Сервер iOS MDM" на стр. 342).

Подробнее о создании файла CSR-запроса и отправке его в Apple Inc. можно прочитать в Базе знаний на веб-сайте Службы технической поддержки “Лаборатории Касперского” http://support.kaspersky.ru/11077.

См. также

Обновление APNs-сертификата..... 340

Обновление APNs-сертификата

► *Чтобы обновить APNs-сертификат, выполните следующие действия:*

1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Серверы мобильных устройств**.
2. В рабочей области папки **Серверы мобильных устройств** выберите Сервер iOS MDM.
3. В контекстном меню Сервера iOS MDM выберите пункт **Свойства**.

   Откроется окно свойств Сервера iOS MDM.
4. В окне свойств Сервера iOS MDM выберите раздел **Сертификаты**.
5. В разделе **Сертификаты** в блоке параметров **Сертификат Apple Push Notification** нажмите на кнопку **Обновить**.

   Запустится мастер обновления APNs-сертификата, откроется окно **Обновление APNs-сертификата**.
6. Создайте Certificate Signing Request (далее CSR-запрос). Для этого выполните следующие действия:

   a. Нажмите на кнопку **Создать CSR**.

   b. В открывшемся окне **Создание CSR** укажите название запроса, название компании и департамента, город, область и страну.

c. Нажмите на кнопку **Сохранить** и укажите имя файла, в котором будет сохранен CSR-запрос.

Приватная часть (private key) будущего сертификата будет сохранена в памяти устройства.

7. Отправьте созданный файл с CSR-запросом на подпись в "Лабораторию Касперского" через ваш CompanyAccount.

> Подписание CSR-запроса доступно только после загрузки на портал CompanyAccount ключа, разрешающего использование функциональности Управление мобильными устройствами.

После обработки вашего электронного запроса вы получите файл CSR-запроса, подписанный "Лабораторией Касперского".

8. Отправьте подписанный файл CSR-запроса на веб-сайт Apple Inc. https://identity.apple.com/pushcert, используя произвольный Apple ID.

> Не рекомендуется использовать персональный Apple ID. Создайте отдельный Apple ID, чтобы использовать его как корпоративный. Созданный Apple ID привяжите к почтовому ящику организации, а не отдельного сотрудника.

После обработки CSR-запроса в Apple Inc. вы получите публичную часть APNs-сертификата. Сохраните полученный файл на диск.

9. Запросите публичную часть сертификата. Для этого выполните следующие действия:

   a. Перейдите на портал Apple Push Certificates https://identity.apple.com/pushcert. Для авторизации на портале потребуется Apple Id, полученный при первичном запросе сертификата.

   b. В списке сертификатов выберите сертификат, APSP-имя которого (имя в формате "APSP: <номер>") совпадает с APSP-именем сертификата, используемого Сервером iOS MDM, и нажмите на кнопку **Обновить**.

APNs-сертификат будет обновлен.

c. Сохраните созданный порталом сертификат.

10. Экспортируйте APNs-сертификат вместе с приватным ключом, созданным при формировании CSR-запроса, в файл формата PFX. Для этого выполните следующие действия:

    a. В окне **Обновление APNs-сертификата** нажмите на кнопку **Завершить CSR**.

    b. В открывшемся окне **Открыть** выберите файл с публичной частью сертификата, полученный после обработки CSR-запроса в Apple Inc., и нажмите на кнопку **Открыть**.

    Запустится экспорт сертификата.

    c. В открывшемся окне введите пароль для приватного ключа, нажмите на кнопку **ОК**.

    Заданный пароль будет использоваться для установки APNs-сертификата на Сервер iOS MDM.

    d. В открывшемся окне **Обновление APNs-сертификата** укажите имя файла для сохранения APNs-сертификата, выберите папку, в которую он будет сохранен, и нажмите на кнопку **Сохранить**.

Приватная и публичная части сертификата будут объединены, APNs-сертификат будет сохранен в файл формата PFX.

См. также

Получение APNs-сертификата 337

Установка сертификата APNs на Сервер iOS MDM

После получения APNs-сертификата необходимо установить APNs-сертификат на Сервер iOS MDM.

► *Чтобы установить APNs-сертификат на Сервер iOS MDM, выполните следующие действия:*

1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Серверы мобильных устройств**.

2. В рабочей области папки **Серверы мобильных устройств** выберите Сервер iOS MDM.

3. В контекстном меню Сервера iOS MDM выберите пункт **Свойства**.

   Откроется окно свойств Сервера iOS MDM.

4. В окне свойств Сервера iOS MDM выберите раздел **Сертификаты**.

В разделе **Сертификаты** в блоке параметров **Сертификат Apple Push Notification** нажмите на кнопку **Установить**.

1. Выберите файл формата PFX, содержащий APNs-сертификат.

2. Введите пароль приватного ключа, указанный при экспорте APNs-сертификата (см. раздел "Получение APNs-сертификата" на стр. 337).

В результате APNs-сертификат будет установлен на Сервер iOS MDM. Информация о сертификате будет отображаться в окне свойств Сервера iOS MDM в разделе **Сертификаты**.

Настройка доступа к сервису Apple Push Notification

Для корректной работы веб-сервиса iOS MDM, а также для обеспечения своевременного реагирования мобильных устройств на команды администратора, в параметрах Сервера iOS MDM следует указать сертификат Apple Push Notification Service (далее APNs-сертификат).

О том, как получить APNs-сертификат см. статью в Базе знаний на веб-сайте Службы технической поддержки http://support.kaspersky.ru/11077.

Взаимодействуя с сервисом Apple Push Notification (далее APNs), веб-сервис iOS MDM подключается к внешнему адресу gateway.push.apple.com по порту 2195 (исходящий). Поэтому веб-сервису iOS MDM необходимо предоставить доступ к порту TCP 2195 для

диапазона адресов 17.0.0.0/8. Со стороны iOS устройства – доступ к порту TCP 5223 для диапазона адресов 17.0.0.0/8.

Если доступ к APNs со стороны веб-сервиса iOS MDM предполагается осуществлять через прокси-сервер, то на устройстве с установленным веб-сервисом iOS MDM необходимо выполнить следующие действия:

1. Прописать в Реестр следующие строки:

   - Для 32-разрядной операционной системы:

```
[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>"
```

   - Для 64-разрядной операционной системы:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0\Conset]

"ApnProxyHost"="<Proxy Host Name>"

"ApnProxyPort"="<Proxy Port>"

"ApnProxyLogin"="<Proxy Login>"

"ApnProxyPwd"="<Proxy Password>"
```

2. Перезапустить службу веб-сервиса iOS MDM.

Выписка и установка общего сертификата на мобильное устройство

► *Чтобы выписать общий сертификат пользователю, выполните следующие действия:*

1. В дереве консоли в папке **Учетные записи пользователей** выберите учетную запись пользователя.

2. В контекстном меню учетной записи пользователя выберите пункт **Установить сертификат**.

Будет запущен мастер установки сертификата. Следуйте его указаниям.

В результате работы мастера сертификат будет создан и добавлен в список сертификатов пользователя.

Выписанный сертификат пользователь загружает вместе с установочным пакетом, в котором содержится iOS MDM-профиль.

После подключения мобильного устройства к Серверу iOS MDM на устройстве пользователя будут применены параметры iOS MDM-профиля. Администратор сможет управлять подключенным устройством.

Мобильное устройство пользователя, подключенное к Серверу iOS MDM, отображается в папке **Мобильные устройства**, вложенной в папку **Управление мобильными устройствами** дерева консоли.

Добавление iOS MDM-устройства в список управляемых устройств

► *Чтобы добавить iOS MDM-устройство пользователя в список управляемых устройств с помощью ссылки на App Store, выполните следующие действия:*

1. В дереве консоли выберите папку **Учетные записи пользователей**.

   По умолчанию папка **Учетные записи пользователей** вложена в папку **Дополнительно**.

2. Выберите учетную запись пользователя, мобильное устройство которого вы хотите добавить в список управляемых устройств.

3. В контекстном меню учетной записи пользователя выберите пункт **Добавить мобильное устройство**.

   Запустится мастер добавления устройства. В окне мастера **Источник сертификата** требуется указать способ создания общего сертификата, с помощью которого Сервер администрирования идентифицирует мобильное устройство. Вы можете задать общий сертификат одним из двух способов:

   - автоматически создать общий сертификат средствами Сервера администрирования и доставить сертификат на устройство;
   - указать файл общего сертификата.

4. В окне мастера **Тип устройства** выберите вариант **Ссылка на App Store**.

5. В окне мастера **Способ уведомления пользователей** настройте уведомление пользователя мобильного устройства о создании сертификата (с помощью SMS-сообщения или по электронной почте).

6. В окне мастера **Информация о сертификате** нажмите на кнопку **Готово** для завершения работы мастера установки сертификатов.

В результате работы мастера на устройство пользователя будет отправлена ссылка и QR-код для загрузки Kaspersky Safe Browser с App Store. Пользователь переходит по ссылке или сканирует QR-код. После этого операционная система устройства запрашивает у пользователя согласие на установку Kaspersky Safe Browser. Пользователь устанавливает Kaspersky Safe Browser на мобильное устройство. После установки Kaspersky Safe Browser пользователь повторно сканирует QR-код для получения параметров подключения к Серверу администрирования. В результате повторного сканирования QR-кода в Safe Browser пользователь получает параметры подключения к Серверу администрирования и общий сертификат. Мобильное устройство подключается к Серверу администрирования и загружает общий сертификат. После установки сертификата на мобильное устройство мобильное устройство будет отображаться в папке **Мобильные устройства**, вложенной в папку **Управление мобильными устройствами** дерева консоли.

Если Kaspersky Safe Browser был ранее установлен на мобильное устройство, параметры подключения к Серверу администрирования нужно вводить самостоятельно. С помощью функции сканирования приложения Kaspersky Safe Browser пользователь сканирует QR-код и получает параметры подключения устройства к Серверу администрирования. Полученные параметры пользователь сохраняет на устройстве. Далее мобильное устройство автоматически подключается к Серверу администрирования и загружает общий сертификат. После установки сертификата на мобильное устройство, мобильное устройство будет отображаться в папке **Мобильные устройства**, вложенной в папку **Управление мобильными устройствами** дерева консоли. Повторная загрузка и установка Kaspersky Safe Browser в этом случае не выполняется.

Если на iOS MDM-устройстве ранее был установлен iOS MDM-профиль, то после установки на устройстве Kaspersky Safe Browser и общего сертификата это устройство отображается в списке устройств в папке **Мобильные устройства** дважды (дублируется). Устройство дублируется в списке из-за наличия на нем двух общих (идентификационных) сертификатов.

Развертывание системы управления по KES-протоколу с помощью Self Service Portal

Kaspersky Security Center позволяет пользователям самостоятельно управлять своими мобильными устройствами, которые подключаются к Серверу администрирования по KES-протоколу, с помощью Self Service Portal.

Self Service Portal поддерживает мобильные устройства с операционными системами iOS и Android.

Развертывание системы управления по KES-протоколу с помощью Self Service Portal состоит из следующих этапов:

1. Подготовка к установке Self Service Portal:

a. Администратор устанавливает на выбранное клиентское устройство Self Service Portal.

b. Администратор сообщает адрес Self Service Portal пользователю.

2. Подключение мобильного устройства к Self Service Portal:

a. Пользователь открывает главную страницу портала.

Self Service Portal создает установочный пакет, после чего отображает на странице портала одноразовую ссылку для загрузки пакета и QR-код, в котором зашифрована ссылка. Установочный пакет необходим для установки на устройство агента управления, и применения корпоративных политик.

b. Пользователь переходит на страницу загрузки установочного пакета с мобильного устройства, которое нужно добавить на Self Service Portal, загружает установочный пакет и устанавливает агент управления на мобильное устройство.

c. После установки агента управления устройство подключается к Серверу администрирования.

В результате устройство будет добавлено в список управляемых устройств и к нему будут применены корпоративные политики. Ссылка на информацию о подключении к Серверу администрирования отправляется на электронную почту пользователя.

Добавление KES-устройства в список управляемых устройств

► *Чтобы добавить KES-устройство пользователя в список управляемых устройств с помощью ссылки на Google Play™, выполните следующие действия:*

1. В дереве консоли выберите папку **Учетные записи пользователей**.

По умолчанию папка **Учетные записи пользователей** вложена в папку **Дополнительно**.

2. Выберите учетную запись пользователя, мобильное устройство которого вы хотите добавить в список управляемых устройств.

3. В контекстном меню учетной записи пользователя выберите пункт **Добавить мобильное устройство**.

   Запустится мастер добавления устройства. В окне мастера **Источник сертификата** требуется указать способ создания общего сертификата, с помощью которого Сервер администрирования идентифицирует мобильное устройство. Вы можете задать общий сертификат одним из двух способов:

   - автоматически создать общий сертификат средствами Сервера администрирования и доставить сертификат на устройство;
   - указать файл общего сертификата.

4. В окне мастера **Тип устройства** выберите вариант **Ссылка на Google Play**.

5. В окне мастера **Способ уведомления пользователей** настройте параметры уведомления пользователя мобильного устройства о создании сертификата (с помощью SMS-сообщения, по электронной почте или информация будет отображена после окончания работы мастера).

6. В окне мастера **Информация о сертификате** нажмите на кнопку **Готово** для завершения работы мастера установки сертификатов.

В результате работы мастера на устройство пользователя будет отправлена ссылка и QR-код для загрузки Kaspersky Endpoint Security для Android с Google Play. Пользователь переходит в магазин приложений Google Play по ссылке или отсканировав QR-код. После этого операционная система устройства запрашивает у пользователя согласие на установку Kaspersky Endpoint Security для Android. После загрузки и установки Kaspersky Endpoint Security для Android мобильное устройство подключается к Серверу администрирования и загружает общий сертификат. После установки сертификата на мобильное устройство, мобильное устройство будет отображаться в папке **Мобильные устройства**, вложенной в папку **Управление мобильными устройствами** дерева консоли.

Если приложение Kaspersky Endpoint Security для Android уже установлено на устройство, пользователю нужно самостоятельно ввести параметры подключения к Серверу администрирования, получив их у администратора. После настройки параметров подключения мобильное устройство подключается к Серверу администрирования. Администратор выписывает общий сертификат для устройства и отправляет пользователю сообщение электронной почты или SMS с именем пользователя и паролем для загрузки сертификата. Пользователь загружает и устанавливает общий сертификат. После установки сертификата на мобильное устройство, мобильное устройство будет отображаться в папке **Мобильные устройства**, вложенной в папку **Управление мобильными устройствами** дерева консоли. Повторная загрузка и установка Kaspersky Endpoint Security для Android в этом случае не выполняются.

Подключение KES-устройств к Серверу администрирования

В зависимости от способа подключения устройств к Серверу администрирования существует две схемы развертывания Kaspersky Device Management для iOS для KES-устройств:

- схема развертывания с использованием прямого подключения устройств к Серверу администрирования;
- схема развертывания с использованием Forefront® Threat Management Gateway (TMG).

В этом разделе

Прямое подключение устройств к Серверу администрирования

KES-устройства могут напрямую подключаться к порту 13292 Сервера администрирования.

В зависимости от способа аутентификации существуют два варианта подключения KES-устройств к Серверу администрирования:

- подключение устройств с использованием пользовательского сертификата;
- подключение устройств без пользовательского сертификата.

Подключение устройства с использованием пользовательского сертификата

При подключении устройства с использованием пользовательского сертификата происходит привязка этого устройства к учетной записи пользователя, для которой средствами Сервера администрирования назначен соответствующий сертификат.

В этом случае будет использована двусторонняя аутентификация SSL (2-way SSL authentication, mutual authentication). Как Сервер администрирования, так и устройство будут аутентифицированы с помощью сертификатов.

Подключение устройства без пользовательского сертификата

При подключении устройства без пользовательского сертификата оно не будет привязано ни к одной учетной записи пользователя на Сервере администрирования. Но при получении устройством любого сертификата будет произведена привязка этого устройства к пользователю, которому средствами Сервера администрирования назначен соответствующий сертификат.

При подключении устройства к Серверу администрирования будет использована односторонняя SSL-аутентификация (1-way SSL authentication), при которой только Сервер администрирования аутентифицируется с помощью сертификата. После получения устройством пользовательского сертификата тип аутентификации будет изменен на двустороннюю аутентификацию SSL (2-way SSL authentication, mutual authentication (см. раздел "Предоставление доступа к Серверу администрирования из интернета" на стр. 92)).

Схема подключения KES-устройств к Серверу с использованием принудительного делегирования Kerberos (KCD)

Схема подключения KES-устройств к Серверу администрирования с использованием Kerberos Constrained Delegation (KCD) предполагает:

- интеграцию с Microsoft Forefront Threat Management Gateway (далее TMG);
- использование принудительного делегирования Kerberos Constrained Delegation (далее KCD) для аутентификации мобильных устройств;
- интеграцию с инфраструктурой открытых ключей (Public Key Infrastructure, далее PKI) для использования пользовательских сертификатов.

При использовании этой схемы подключения следует учесть следующее:

- Тип подключения KES-устройств к TMG должен быть "2-way SSL authentication", то есть устройство должно подключаться к TMG по своему пользовательскому сертификату. Для этого в инсталляционный пакет Kaspersky Endpoint Security для Android, который установлен на устройстве, необходимо интегрировать пользовательский сертификат. Этот KES-пакет должен быть создан Сервером администрирования специально для данного устройства (пользователя).
- Вместо серверного сертификата по умолчанию для мобильного протокола следует указать особый (кастомизированный) сертификат:

  1. В окне свойств Сервера администрирования в разделе **Параметры** установить флажок **Открыть порт для мобильных устройств** и в раскрывающемся списке выбрать **Добавить сертификат**.
  2. В открывшемся окне указать тот же сертификат, что задан на TMG при публикации точки доступа к мобильному протоколу на Сервере администрирования.

- Пользовательские сертификаты для KES-устройств должны выписываться доменным Certificate Authority (CA). Причем следует учесть, что если в домене несколько корневых CA, то пользовательские сертификаты должны быть выписаны тем CA, который прописан в публикации на TMG.

Обеспечить соответствие пользовательского сертификата заявленному выше требованию возможно несколькими способами:

- Указать особый пользовательский сертификат в мастере создания инсталляционных пакетов и в мастере установки сертификатов.
- Интегрировать Сервер администрирования с доменным PKI и настроить соответствующий параметр в правилах выписки сертификатов:

  1. В дереве консоли откройте папку **Управление мобильными устройствами** и выберите вложенную папку **Сертификаты**.
  2. В рабочей области папки **Сертификаты** по кнопке **Настроить правила выпуска сертификатов** откройте окно **Правила выпуска сертификатов**.
  3. В разделе **Интеграция с PKI** настройте интеграцию с инфраструктурой открытых ключей.
  4. В разделе **Выпуск сертификатов общего типа** укажите источник сертификатов.

См. разделы:

- Интеграция с Public Key Infrastructure (на стр. 357);
- Предоставление доступа к Серверу администрирования из интернета (на стр. 92).

Рассмотрим пример настройки ограниченного делегирования KCD со следующими допущениями:

- точка доступа к мобильному протоколу на Сервере администрирования поднята на 13292 порте;
- имя устройства с TMG – tmg.mydom.local;
- имя устройства с Сервером администрирования – ksc.mydom.local;
- имя внешней публикации точки доступа к мобильному протоколу – kes4mob.mydom.global.

Доменная учетная запись для Сервера администрирования

Необходимо создать доменную учетную запись (например, KSCMobileSrvcUsr), под которой будет работать служба Сервера администрирования. Указать учетную запись для службы Сервера администрирования можно при установке Сервера администрирования или с помощью утилиты klsrvswch. Утилита klsrvswch расположена в папке установки Сервера администрирования.

Указать доменную учетную запись необходимо по следующим причинам:

- Функциональность по управлению KES-устройствами является неотъемлемой частью Сервера администрирования.
- Для правильной работы принудительного делегирования (KCD) принимающая сторона, которой является Сервер администрирования, должна работать под доменной учетной записью.

Service Principal Name для http/kes4mob.mydom.local

В домене под учетной записью KSCMobileSrvcUsr требуется прописать Service Principal Name (SPN) для публикации сервиса мобильного протокола на 13292 порту устройства с Сервером администрирования. Для устройства kes4mob.mydom.local с Сервером администрирования это будет выглядеть следующим образом:

setspn -a http/kes4mob.mydom.local:13292 mydom\KSCMobileSrvcUsr

Настройка доменных свойств устройства с TMG (tmg.mydom.local)

Для делегирования трафика нужно доверить устройство с TMG (tmg.mydom.local) службе, определенной по SPN (http/kes4mob.mydom.local:13292).

Чтобы доверить устройство с TMG службе, определенной по SPN (http/kes4mob.mydom.local:13292), администратор должен выполнить следующие действия:

1. В оснастке Microsoft Management Console "Active Directory Users and Computers" необходимо выбрать устройство с установленным TMG (tmg.mydom.local).
2. В свойствах устройства на закладке **Delegation** для переключателя **Trust this computer for delegation to specified service only** выбрать вариант **Use any authentication protocol**.

3. В список **Services to which this account can present delegated credentials** добавить SPN http/kes4mob.mydom.local:13292.

Особый (кастомизированный) сертификат для публикации (kes4mob.mydom.global)

Для публикации мобильного протокола Сервера администрирования требуется выписать особый (кастомизированный) сертификат на FQDN kes4mob.mydom.global и указать его взамен серверного сертификата по умолчанию в параметрах мобильного протокола Сервера администрирования в Консоли администрирования. Для этого в окне свойств Сервера администрирования в разделе **Параметры** необходимо установить флажок **Открыть порт для мобильных устройств** и в раскрывающемся списке выбрать **Добавить сертификат**.

Следует учесть, что в контейнере с серверным сертификатом (файл с расширением p12 или pfx) должна также присутствовать цепочка корневых сертификатов (публичные части).

Настройка публикации на TMG

На TMG для трафика, идущего со стороны мобильного устройства на 13292 порт kes4mob.mydom.global, необходимо настроить KCD на SPN http/kes4mob.mydom.local:13292 с использованием серверного сертификата, выписанного для FQND kes4mob.mydom.global. При этом следует учесть, что как на публикации, так и на публикуемой точке доступа (13292 порт Сервера администрирования) должен быть один и тот же серверный сертификат.

Использование Google Firebase Cloud Messaging

Для обеспечения своевременного реагирования KES-устройств под управлением Android на команды администратора в свойствах Сервера администрирования следует включить использование сервиса Google™ Firebase Cloud Messaging (далее GFCM).

► *Чтобы включить использование GFCM, выполните следующие действия:*

1. В Консоли администрирования выберите узел **Управление мобильными устройствами**, папку **Мобильные устройства**.

2. В контекстном меню папки **Мобильные устройства** выберите пункт **Свойства**.

3. В свойствах папки выберите раздел **Параметры Google Firebase Cloud Messaging**.

4. В полях **Идентификатор отправителя** и **Ключ сервера** укажите параметры GFCM: SENDER_ID и API Key.

Сервис GFCM работает на следующих диапазонах адресов:

- Со стороны KES-устройства необходим доступ на порты 443 (HTTPS), 5228 (HTTPS), 5229 (HTTPS), 5230 (HTTPS) следующих адресов:
  - google.com;
  - android.googleapis.com;
  - android.apis.google.com;
  - либо на все IP из списка Google's ASN of 15169.
- Со стороны Сервера администрирования необходим доступ на порт 443 (HTTPS) следующих адресов:
  - android.googleapis.com;
  - либо на все IP из списка "Google ASN 15169".

В случае если в Консоли администрирования в свойствах Сервера администрирования заданы параметры прокси-сервера (**Дополнительно / Параметры доступа к сети Интернет**), то они будут использованы для взаимодействия с GFCM.

Настройка GFCM: получение SENDER_ID, API Key

Для настройки работы с GFCM администратор должен выполнить следующие действия:

1. Зарегистрироваться на портале google https://accounts.google.com.
2. Перейти на портал для разработчиков https://console.developers.google.com/project.
3. Создать новый проект по кнопке **Create Project**, указать имя проекта, указать ID
4. Дождаться создания проекта.

   На первой странице проекта, в верхней части страницы, в поле **Project Number** указан искомый SENDER_ID.

5. Перейти в раздел **APIs & auth / APIs**, включить **Google Firebase Cloud Messaging for Android**.

6. Перейти в раздел **APIs & auth / Credentials**, нажать на кнопку **Create New Key**.

7. Нажать на кнопку **Server key**.

8. Если есть, задать ограничения, нажать на кнопку **Create**.

9. Получить API Key из свойств только что созданного ключа (поле **API key**).

Интеграция с Public Key Infrastructure

Интеграция с инфраструктурой открытых ключей (Public Key Infrastructure, далее PKI) в первую очередь предназначена для упрощения выпуска доменных пользовательских сертификатов Сервером администрирования.

Администратор может назначить для пользователя доменный сертификат в Консоли администрирования. Это можно сделать одним из следующих способов:

- назначить пользователю особый (кастомизированный) сертификат из файла в мастере подключения нового устройства либо в мастере установки сертификатов;

- выполнить интеграцию с PKI и назначить PKI источником сертификатов для конкретного типа сертификатов либо для всех типов сертификатов.

Параметры интеграции с PKI доступы в рабочей области папки **Управление мобильными устройствами / Сертификаты** по ссылке **Интегрировать с инфраструктурой открытых ключей**.

Общий принцип интеграции с PKI для выпуска доменных сертификатов пользователей

В Консоли администрирования по ссылке **Интегрировать с инфраструктурой открытых ключей** в рабочей области папки **Управление мобильными устройствами / Сертификаты** следует задать доменную учетную запись, которая будет использована Сервером администрирования для выписки доменных пользовательских сертификатов посредством доменного CA (далее – учетная запись, под которой производится интеграция с PKI).

При этом следует учесть следующее:

- В параметрах интеграции с PKI существует возможность указать шаблон по умолчанию для всех типов сертификатов. Тогда как в правилах выпуска сертификатов (правила доступны в рабочей области папки **Управление мобильными устройствами / Сертификаты** по кнопке **Настроить правила выпуска сертификатов**) присутствует возможность задать шаблон для каждого типа сертификата отдельно.

- На устройстве с установленным Сервером администрирования в хранилище сертификатов учетной записи, под которой производится интеграция с PKI, должен быть установлен специализированный сертификат Enrollment Agent (EA). Сертификат Enrollment Agent (EA) выписывает администратор доменного CA (Certificate Authority).

Учетная запись, под которой производится интеграция с PKI, должна соответствовать следующим критериям:

- Является доменным пользователем.

- Является локальным администратором устройства с установленным Сервером администрирования, с которого производится интеграция с PKI.

- Обладает правом **Вход в качестве службы**.

- Под этой учетной записью необходимо хотя бы один раз запустить устройство с установленным Сервером администрирования, чтобы создать постоянный профиль пользователя.

Веб-сервер Kaspersky Security Center

Веб-сервер Kaspersky Security Center (далее веб-сервер) – это компонент Kaspersky Security Center. Веб-сервер предназначен для публикации автономных пакетов установки, автономных инсталляционных пакетов для мобильных устройств, iOS MDM-профилей, а также файлов из папки общего доступа.

Созданные iOS MDM-профили и инсталляционные пакеты публикуются на веб-сервере автоматически и удаляются после первой загрузки. Администратор может передать

сформированную ссылку пользователю любым удобным способом, например, по электронной почте.

По полученной ссылке пользователь может загрузить на мобильное устройство предназначенную для него информацию.

Настройки веб-сервера

Для тонкой настройки веб-сервера в свойствах веб-сервера Консоли администрирования предусмотрена возможность смены портов для протоколов HTTP (8060) и HTTPS (8061). Также, помимо смены портов, возможна смена серверного сертификата для HTTPS-протокола и смена FQDN-имени веб-сервера для HTTP-протокола.

Настройка SMS-рассылки в Kaspersky Security Center

Kaspersky Security Center может использоваться для отправки пользователям мобильных устройств SMS-уведомлений.

SMS-рассылка может использоваться в следующих случаях:

- Для получения администратором SMS-уведомлений о событиях в работе Сервера администрирования и программ, установленных на клиентских устройствах.
- Для установки программ на мобильные устройства пользователей. Пользователь мобильного устройства получает SMS, в котором содержится ссылка на загрузку программы, которую необходимо установить.
- Для оповещения сотрудников организации.

Развертывание SMS-рассылки выполняется в следующей последовательности:

1. Администратор устанавливает утилиту Kaspersky SMS Broadcasting на мобильное устройство Android.

   > Утилита Kaspersky SMS Broadcasting устанавливается только на мобильные устройства на платформе Android.

2. После установки утилиты Kaspersky SMS Broadcasting на мобильное устройство администратор синхронизирует мобильное устройство с Сервером администрирования.
3. Администратор назначает мобильное устройство, на котором установлена утилита Kaspersky SMS Broadcasting, отправителем SMS в Консоли администрирования.

В этом разделе

Получение и установка утилиты Kaspersky SMS Broadcasting

Утилита Kaspersky SMS Broadcasting входит в состав пакета установки Kaspersky Endpoint Security для Android. Вы можете загрузить пакет установки Kaspersky Endpoint Security для Android с сайта "Лаборатории Касперского".

► *Чтобы установить утилиту Kaspersky SMS Broadcasting, выполните следующие действия:*

1. В дереве консоли в папке **Удаленная установка** выберите вложенную папку **Инсталляционные пакеты**.

   Папка **Удаленная установка** по умолчанию вложена в папку **Дополнительно**.

2. Нажмите на кнопку **Дополнительные действия** и из раскрывающегося списка выберите пункт **Управлять пакетами мобильных приложений**.

3. В окне **Управление пакетами мобильных приложений** выберите пакет мобильного приложения, содержащего утилиту Kaspersky SMS Broadcasting.

   Если пакет не создавался, нажмите на кнопку **Новый** и создайте пакет мобильного приложения для утилиты Kaspersky SMS Broadcasting.

4. В окне **Управление пакетами мобильных приложений** нажмите на кнопку **Опубликовать на веб-сервере**.

   Ссылка на скачивание пакета мобильного приложения с утилитой Kaspersky SMS Broadcasting будет опубликована на веб-сервере.

5. В окне **Управление пакетами мобильных приложений** нажмите на кнопку **Отправить по почте**, чтобы отправить пользователю мобильного устройства ссылку на скачивание пакета мобильных приложений, содержащего утилиту Kaspersky SMS Broadcasting.

6. Скачайте с веб-сервера на мобильное устройство пакет мобильных приложений, содержащий утилиту Kaspersky SMS Broadcasting.

7. Выполните установку утилиты Kaspersky SMS Broadcasting штатными средствами мобильного устройства.

Вы также можете скачать утилиту Kaspersky SMS Broadcasting на мобильное устройство с сайта "Лаборатории Касперского" или подключить мобильное устройство к клиентскому устройству и скопировать уже скачанную утилиту Kaspersky SMS Broadcasting на мобильное устройство.

Синхронизация мобильного устройства с Сервером администрирования

► *Чтобы синхронизировать мобильное устройство с Сервером администрирования, выполните следующие действия:*

1. В дереве консоли Kaspersky Security Center в контекстном меню папки **Сервер администрирования** выберите пункт **Свойства**.

   Откроется окно свойств Сервера администрирования.

2. В окне свойств Сервера администрирования в разделе **Параметры** установите флажок **Открыть порт для мобильных устройств**.

3. В разделе **Параметры** в поле **Порт для мобильных устройств** укажите порт синхронизации мобильного устройства с Сервером администрирования. По умолчанию используется порт 13292.

4. Запустите утилиту Kaspersky SMS Broadcasting на мобильном устройстве.

5. В главном окне утилиты Kaspersky SMS Broadcasting нажмите на кнопку **Параметры синхронизации**.

6. В окне **Параметры синхронизации** в поле **Адрес сервера** укажите IP-адрес Сервера администрирования.

7. В поле **Порт** укажите порт подключения к Серверу администрирования. По умолчанию используется порт 13292.

8. Нажмите на кнопку **ОК**.

Когда мобильное устройство синхронизируется с Сервером администрирования, вы можете назначить это мобильное устройство отправителем SMS-сообщений.

Назначение мобильного устройства отправителем SMS-сообщений

► *Чтобы назначить мобильное устройство отправителем SMS-сообщений, выполните следующие действия:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.

2. В рабочей области узла выберите закладку **События**.

3. По ссылке **Настроить параметры уведомлений и экспорта событий** в раскрывающемся списке выберите значение **Настроить список отправителей SMS**.

   Откроется окно свойств событий на разделе **Отправители SMS**.

4. В разделе **Отправители SMS** нажмите на кнопку **Добавить**.

   Откроется окно **Выбор устройства**.

5. В окне **Выбор устройства** укажите мобильное устройство, которое будет использоваться в качестве отправителя SMS-сообщений.

6. Нажмите на кнопку **ОК**.

На устройстве, которое назначено отправителем SMS-сообщений, должна быть установлена утилита Kaspersky SMS Broadcasting.

Уведомления о событиях

В этом разделе описано, как выбрать способ уведомления администратора о событиях на клиентских устройствах, а также как настроить параметры уведомления о событиях.

Кроме того, описано, как проверить распространение уведомлений о событиях с помощью тестового «вируса» Eicar.

В этом разделе

Настройка параметров уведомлений о событиях

Kaspersky Security Center позволяет выбирать способ уведомления для администратора о событиях на клиентских устройствах и настраивать параметры уведомлений:

- Электронная почта. При возникновении события программа посылает уведомление на указанные адреса электронной почты. Вы можете настроить текст уведомления.
- SMS. При возникновении события программа посылает уведомления на указанные номера телефонов. Вы можете настроить отправку SMS через почтовый шлюз или с помощью утилиты Kaspersky SMS Broadcasting.
- Исполняемый файл. При возникновении события на устройстве, исполняемый файл запускается на рабочем месте администратора. С помощью исполняемого файла администратор может получать параметры произошедшего события (см. раздел "Уведомление о событиях с помощью исполняемого файла" на стр. 366).

► *Чтобы настроить параметры уведомлений о событиях на клиентских устройствах, выполните следующие действия:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите закладку **События**.
3. По ссылке **Настроить параметры уведомлений и экспорта событий** в раскрывающемся списке выберите значение **Настроить параметры уведомлений**.

   В результате откроется окно **Свойства: События**.
4. В разделе **Уведомление** выберите способ уведомления (электронная почта, SMS, исполняемый файл для запуска) и настройте параметры уведомлений.
5. В поле **Текст уведомления** введите текст, который программа будет отправлять при возникновении события.

   Из раскрывающего списка, расположенного справа от текстового поля, можно добавлять в сообщение подстановочные параметры с деталями события (например, описание события, время возникновения и прочее).

   > Если текст уведомления содержит символ %, нужно указать его два раза подряд, чтобы сообщение было отправлено. Например, "Загрузка процессора составляет 100%%".
6. По кнопке **Отправить пробное сообщение** проверьте, правильно ли настроены уведомления.

   Программа отправляет тестовое уведомление указанному получателю.
7. Нажмите на кнопку **ОК**, чтобы сохранить изменения.

В результате настроенные параметры уведомления распространяются на все события, происходящие на клиентских устройствах.

Вы также можете быстро настроить уведомления о событии в окне свойств события по ссылкам **Настроить параметры событий Kaspersky Endpoint Security** и **Настроить параметры событий Сервера администрирования**.

Проверка распространения уведомлений

Для проверки распространения уведомлений о событиях используется уведомление об обнаружении тестового "вируса" Eicar на клиентских устройствах.

► *Чтобы проверить распространение уведомлений о событиях, выполните следующие действия:*

1. Остановите задачу постоянной защиты файловой системы на клиентском устройстве и скопируйте тестовый "вирус" Eicar на клиентское устройство. Снова включите задачу постоянной защиты файловой системы.

2. Запустите задачу проверки клиентских устройств для группы администрирования или набора устройств, в который входит клиентское устройство с "вирусом" Eicar.

   Если задача проверки настроена верно, в процессе ее выполнения тестовый "вирус" будет обнаружен. Если параметры уведомлений настроены верно, вы получите уведомление о найденном вирусе.

   В рабочей области узла **Сервер администрирования** на закладке **События** в выборке **Последние события** отобразится запись об обнаружении "вируса".

Тестовый "вирус" Eicar не содержит программного кода, который может навредить вашему устройству. При этом большинство программ защиты компаний-производителей идентифицируют его как вирус. Загрузить тестовый "вирус" можно с официального веб-сайта организации EICAR (http://www.eicar.org/86-0-Intended-use.html).

Уведомление о событиях с помощью исполняемого файла

Kaspersky Security Center позволяет с помощью запуска исполняемого файла уведомлять администратора о событиях на клиентских устройствах. Исполняемый файл должен

содержать другой исполняемый файл с подстановочными параметрами события, которые нужно передать администратору.

Таблица 31. Подстановочные параметры для описания события

Подстановочный параметр	Описание подстановочного параметра
%SEVERITY%	Уровень важности события
%COMPUTER%	Имя устройства, на котором произошло событие
%DOMAIN%	Домен
%EVENT%	Событие
%DESCR%	Описание события
%RISE_TIME%	Время возникновения
%KLCSAK_EVENT_TASK_DISPLAY_NAME%	Название задачи
%KL_PRODUCT%	Агент администрирования Kaspersky Security Center
%KL_VERSION%	Номер версии Агента администрирования
%HOST_IP%	IP-адрес
%HOST_CONN_IP%	IP-адрес соединения

Пример

Для уведомления о событии используется исполняемый файл (например, *script1.bat)*, внутри которого запускается другой исполняемый файл (например, *script2.bat*) с подстановочным параметром %COMPUTER%. При возникновении события на устройстве администратора будет запущен файл *script1.bat*, который, в свою очередь, запустит файл *script2.bat* с параметром %COMPUTER%. В результате администратор получит имя устройства, на котором произошло событие.

Нагрузка на сеть

В этом разделе приводится информация об объеме сетевого трафика, которым обмениваются между собой клиентские устройства и Сервер администрирования в ходе выполнения ключевых административных сценариев.

Основная нагрузка на сеть связана с выполнением следующих административных сценариев:

- первоначальное развертывание антивирусной защиты;
- первоначальное обновление антивирусных баз;
- синхронизация клиентского устройства с Сервером администрирования;
- регулярное обновление антивирусных баз;
- обработка событий на клиентских устройствах Сервером администрирования.

В этом разделе

Первоначальное развертывание антивирусной защиты

В этом разделе приведен расход трафика при установке на клиентском устройстве Агента администрирования версии 10 и Kaspersky Endpoint Security 11 для Windows (см. таблицу ниже).

Агент администрирования устанавливается путем форсированной установки, когда требуемые для установки файлы копируются Сервером администрирования в папку общего доступа на клиентском устройстве. После установки Агент администрирования получает дистрибутив Kaspersky Endpoint Security 11 для Windows, используя соединение с Сервером администрирования.

Таблица 32. Расход трафика

Сценарий	Установка Агента администрирования для одного клиентского устройства	Установка Kaspersky Endpoint Security 11 для Windows для одного клиентского устройства (с обновленными базами)	Совместная установка Агента администрирования и Kaspersky Endpoint Security 11 для Windows
Трафик от клиентского устройства к Серверу администрирования, КБ	1087,83	5564,49	6179,68
Трафик от Сервера администрирования к клиентскому устройству, КБ	38 835,86	203 366,39	242 536,62
Общий трафик (для одного клиентского устройства), КБ	39 923,70	208 930,88	248 716,31

После установки Агентов администрирования на клиентские устройства можно назначить одно из устройств в группе администрирования на роль агента обновлений. Он будет использоваться для распространения инсталляционных пакетов. В этом случае объем трафика, передаваемого при первоначальном развертывании антивирусной защиты, существенно отличается в зависимости от того, используется ли многоадресная IP-рассылка.

В случае использования многоадресной IP-рассылки инсталляционные пакеты будут разосланы всем включенным устройствам в группе администрирования один раз. Таким

образом, общий трафик уменьшится примерно в N раз, где N – общее число включенных устройств в группе администрирования. Если многоадресная IP-рассылка не используется, общий трафик совпадает с трафиком в случае получения инсталляционных пакетов с Сервера администрирования, но источником инсталляционных пакетов является не Сервер администрирования, а агент обновлений.

Первоначальное обновление антивирусных баз

В этом разделе приведена информация о расходе трафика при первом запуске задачи обновления баз на клиентском устройстве (см. таблицу ниже). Данные, приведенные в таблице, могут несколько отличаться в зависимости от текущей версии баз.

Таблица 33. Расход трафика

Сценарий	Первоначальное обновление антивирусных баз
Трафик от клиентского устройства к Серверу администрирования, КБ	80,0
Трафик от Сервера администрирования к клиентскому устройству, КБ	61,2
Общий трафик (для одного клиентского устройства), КБ	141,2

Синхронизация клиента с Сервером администрирования

Этот сценарий характеризует состояние системы администрирования в случае, когда происходит активная синхронизация данных между клиентским устройством и Сервером администрирования. Клиентские устройства подключаются к Серверу администрирования с периодом, заданным администратором. Сервер администрирования сравнивает состояние данных на клиентском устройстве с состоянием данных на Сервере, регистрирует данные о

последнем подключении клиентского устройства в базе данных и проводит синхронизацию данных.

В разделе приведена информация о расходе трафика для основных административных сценариев при подключении клиента к Серверу администрирования с синхронизацией (см. таблицу ниже). Данные, приведенные в таблице, могут несколько отличаться в зависимости от текущей версии баз.

Таблица 34. Расход трафика

Сценарий	Трафик от клиентских устройств к Серверу администрирования, КБ	Трафик от Сервера администрирования к клиентским устройствам, КБ	Общий трафик (для одного клиентского устройства), КБ
Первоначальная синхронизация до обновления баз на клиентском устройстве	368,6	463,7	832,3
Первоначальная синхронизация после обновления баз на клиентском устройстве	1 748,3	34 388,3	36 136,6
Синхронизация при отсутствии изменений на клиентском устройстве и на Сервере администрирования	8,7	6,6	15,3
Синхронизация при изменении одного параметра в политике группы	11,1	13,3	24,4
Синхронизация при изменении одного параметра в групповой задаче	10,0	12,5	22,5
Принудительная синхронизация при отсутствии изменений на клиентском устройстве	47,3	15,5	62,8

Объем общего трафика существенно изменяется в зависимости от того, используется ли многоадресная IP-рассылка внутри групп администрирования. В случае использования многоадресной IP-рассылки общий трафик для группы уменьшается примерно в N раз, где N – число включенных устройств в группе администрирования.

Объем трафика при первоначальной синхронизации до и после обновления баз указан для следующих случаев:

- установка на клиентское устройство Агента администрирования и программы защиты;
- перенос клиентского устройства в группу администрирования;
- применение к клиентскому устройству политики и задач, созданных для группы по умолчанию.

В таблице указан объем трафика при изменении одного из параметров защиты, входящих в параметры политики Kaspersky Endpoint Security. Данные для других параметров политики могут отличаться от данных, представленных в таблице.

Добавочное обновление антивирусных баз

В этом разделе приведена информация о расходе трафика при инкрементальном обновлении антивирусных баз через 20 часов после предыдущего обновления (см. таблицу ниже). Данные, приведенные в таблице, могут несколько отличаться в зависимости от текущей версии баз.

Таблица 35. Расход трафика

Сценарий	Инкрементальное обновление антивирусных баз
Трафик от клиентского устройства к Серверу администрирования, КБ	436,9
Трафик от Сервера администрирования к клиентскому устройству, КБ	9 979,2
Общий трафик (для одного клиентского устройства), КБ	10 416,1

Объем трафика существенно изменяется в зависимости от того, используется ли многоадресная IP-рассылка внутри групп администрирования. В случае использования многоадресной IP-рассылки общий трафик для группы уменьшается примерно в N раз, где N – число включенных устройств в группе администрирования.

Обработка событий клиентов Сервером администрирования

В этом разделе приведен расход трафика при возникновении на клиентском устройстве события "Найден вирус", информация о котором передается на Сервер администрирования и регистрируется в базе данных (см. таблицу ниже).

Таблица 36. Расход трафика

Сценарий	Передача на Сервер администрирования данных при наступлении события "Найден вирус"	Передача на Сервер администрирования данных при наступлении девяти событий "Найден вирус"
Трафик от клиентского устройства к Серверу администрирования, КБ	27,2	100,4
Трафик от Сервера администрирования к клиентскому устройству, КБ	25,8	52,5
Общий трафик (для одного клиентского устройства), КБ	53,0	152,9

Данные, приведенные в таблице, могут несколько отличаться в зависимости от текущей версии антивирусной программы и в зависимости от того, какие именно события определены в политике как требующие регистрации в базе данных Сервера администрирования.

Расход трафика за сутки

В этом разделе приведена информация о расходе трафика за сутки работы системы администрирования в состоянии "покоя", когда не происходит изменений данных ни со стороны клиентских устройств, ни со стороны Сервера администрирования (см. таблицу ниже).

Данные, приведенные в таблице, характеризуют состояние сети после стандартной установки Kaspersky Security Center и завершения работы мастера первоначальной настройки. Период синхронизации клиентского устройства с Сервером администрирования составлял 20 минут, загрузка обновлений в хранилище Сервера администрирования происходила каждый час.

Таблица 37. Расход трафика

Сценарий	Состояние "покоя" системы администрирования
Трафик от клиентского устройства к Серверу администрирования, КБ	2 162,2
Трафик от Сервера администрирования к клиентскому устройству, КБ	51 000,2
Общий трафик (для одного клиентского устройства), КБ	53 162,4

Скорость заполнения базы данных событиями Kaspersky Endpoint Security

В этом разделе приведены примеры скорости заполнения базы данных Сервера администрирования событиями, возникающими в работе управляемых программ.

Информация о событиях в работе управляемых программ передается с клиентского устройства и регистрируется в базе данных Сервера администрирования.

В базу данных поступает (Ne*Nh) событий в день (см. таблицу ниже). Здесь Nh – количество клиентских устройств, на которых установлены управляемые программы, Ne – количество событий в день, информацию о которых передает с клиентского устройства установленная на нем управляемая программа Kaspersky Endpoint Security для Windows. По умолчанию Kaspersky Endpoint Security для Windows (версии 10 и 11) при штатной работе передает в базу данных около 20 событий в день. Максимальное количество событий, которое может обработать Kaspersky Security Center, составляет 2 000 000 событий в день.

Таблица 38. Скорость заполнения событиями базы данных (при штатной работе)

Количество устройств, на которых установлена программа Kaspersky Endpoint Security	Количество событий, передаваемое в базу данных в день
100	до 2 000
1000	до 20 000
10 000	до 200 000
100 000	до 2 000 000

Максимальное количество событий, хранящихся в базе данных, определяется в разделе **Хранение событий** окна свойств Сервера администрирования. По умолчанию в базе данных хранится не более 400 000 событий.

Устранение неисправностей

В этом разделе содержится информация о наиболее распространенных ошибках и проблемах при развертывании и использовании Kaspersky Security Center, а также рекомендации по решению проблем.

В этом разделе

Проблемы при удаленной установке программ

В таблице ниже перечислены проблемы, возникающие при удаленной установке программ, и типовые причины возникновения этих проблем.

Таблица 39. Проблемы при удаленной установке программ

Проблема	Типовая причина проблемы и вариант решения
Недостаточно прав для установки	Учетная запись, под которой запущена установка, не имеет достаточно прав для выполнения операций, необходимых для установки программы.
Недостаточно места на диске	Недостаточно свободного места на диске для завершения установки. Освободите место на диске и повторите операцию.
Произошла незапланированная перезагрузка ОС	Во время установки произошла незапланированная перезагрузка ОС, точный результат установки может быть неизвестен. Проверьте правильность параметров запуска инсталляционного приложения или обратитесь в Службу технической поддержки.
Не найден необходимый файл	В инсталляционном пакете не найден необходимый файл. Проверьте целостность используемого инсталляционного пакета.
Несовместимая платформа	Инсталляционный пакет не предназначен для данной платформы. Используйте соответствующий инсталляционный пакет.
Несовместимая программа	На устройстве установлена программа, несовместимая с устанавливаемой программой. Перед установкой удалите все программы, входящие в список несовместимых.
Недостаточные системные требования	Инсталляционный пакет требует наличия в системе дополнительного программного обеспечения. Проверьте соответствие конфигурации системы системным требованиям устанавливаемой программы.

Проблема	Типовая причина проблемы и вариант решения
Незавершенная установка	Предыдущая установка или удаление программы не было штатно завершено. Для завершения предыдущей установки или удаления программы, выполненного на данном устройстве, необходимо перезагрузить ОС и повторить процесс установки.
Не та версия инсталляционного приложения	Установка данного инсталляционного пакета не поддерживается версией инсталляционного приложения, установленного на устройстве.
Инсталляция уже запущена	На устройстве уже запущена установка другого приложения.
Не удалось открыть инсталляционный пакет	Не удалось открыть инсталляционный пакет. Возможные причины: пакет отсутствует, пакет поврежден, недостаточно прав для доступа к пакету.
Несовместимая локализация	Инсталляционный пакет не предназначен для установки на данную локализацию ОС.
Установка запрещена политикой	Установка программ на данном устройстве запрещена политикой.
Ошибка записи файла	Во время установки программы произошла ошибка записи. Проверьте наличие прав у учетной записи, под которой выполняется установка, и наличие свободного места на диске.
Неверный пароль деинсталляции	Пароль для удаления программы задан неверно.
Недостаточные аппаратные требования	Аппаратные требования системы не удовлетворяют требованиям программы (объем оперативной памяти, свободное место на диске и так далее).

Проблема	Типовая причина проблемы и вариант решения
Недопустимый каталог установки	Установка программы в указанный каталог запрещена политикой инсталляционного приложения.
Требуется повторная попытка установки после перезагрузки устройства	Требуется повторный запуск инсталлятора программы после перезагрузки устройства.
Для продолжения установки требуется перезагрузка устройства	Для продолжения работы инсталлятора программы требуется перезагрузка устройства.

Неверно выполнено копирование образа жесткого диска

Если копирование образа жесткого диска с установленным Агентом администрирования было выполнено без учета правил развертывания (см. раздел "Развертывание захватом и копированием образа жесткого диска устройства" на стр. 229), часть устройств в Консоли администрирования может отображаться как один значок устройства, постоянно меняющий имя.

Можно использовать следующие способы решения этой проблемы:

- Удаление Агента администрирования.

  Этот способ является самым надежным. На устройствах, которые были скопированы из образа неправильно, нужно при помощи сторонних средств удалить Агент администрирования, а затем установить его заново. Удаление Агента администрирования не может быть выполнено средствами Kaspersky Security Center, поскольку для Сервера администрирования все проблемные устройства неразличимы (им всем соответствует один и тот же значок в Консоли администрирования).

- Запуск утилиты klmover с ключом "-dupfix".

На проблемных устройствах (на всех, которые были скопированы из образа неправильно) необходимо при помощи сторонних средств однократно запустить утилиту klmover с ключом "-dupfix" (klmover -dupfix), расположенную в папке установки Агента администрирования. Запуск утилиты не может быть выполнен средствами Kaspersky Security Center, поскольку для Сервера администрирования все проблемные устройства неразличимы (им всем соответствует один и тот же значок в Консоли администрирования).

Затем следует удалить значок, на который отображались проблемные устройства до запуска утилиты.

- Ужесточение правила обнаружения неправильно скопированных устройств.

  > Этот способ можно использовать только в случае, если установлены Сервер администрирования и Агенты администрирования версии 10 Service Pack 1 или новее.

  Следует ужесточить правило обнаружения неправильно скопированных Агентов администрирования таким образом, чтобы изменение NetBIOS-имени устройства приводило к автоматической "починке" таких Агентов администрирования (предполагается, что скопированные устройства имеют различные NetBIOS-имена).

  На устройстве с Сервером администрирования нужно импортировать в Реестр представленный ниже reg-файл и перезапустить службу Сервера администрирования.

  - Если на устройстве с Сервером администрирования установлена 32-разрядная операционная система:

```
REGEDIT4

[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags]

"KLSRV_CheckClones"=dword:00000003
```

- Если на устройстве с Сервером администрирования установлена 64-разрядная операционная система:

```
REGEDIT4

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\Products\1093\1.0.0.0\ServerFlags]

"KLSRV_CheckClones"=dword:00000003
```

Проблемы с Сервером мобильных устройств Exchange ActiveSync

Этот раздел содержит информацию об ошибках и проблемах, связанных с использованием Сервера мобильных устройств Exchange ActiveSync.

Ошибка во время установки Сервера мобильных устройств Exchange ActiveSync

Если во время локальной или удаленной установки возникла ошибка, то причину ошибки можно узнать, открыв файл error.log, который расположен на устройстве, где производилась установка программы, по пути C:\Windows\Temp\klmdm4exch-2014-11-28-15-56-37\ (где цифры – это дата и время установки программы). Как правило, информации из файла error.log достаточно для решения возникшей проблемы.

В таблице ниже приведены примеры типичных ошибок, регистрируемых в файле error.log.

Таблица 40. Типичные ошибки

Ошибка	Описание	Причина
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.	Аккаунт, под которым производилась установка программы, не обладает ролью Organization Management.
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.	Механизм аутентификации Windows в настройках веб-сервера IIS для виртуальной директории PowerShell не включен.

Список устройств и почтовых аккаунтов пуст

Причину, из-за которой не удается получить список устройств и почтовых аккаунтов, можно узнать из событий, сохраненных в Консоли администрирования в узле Сервер администрирования на закладке **События** в выборке событий **Отказы функционирования**. Если в событиях нет информации, необходимо проверить подключение между Агентом администрирования устройства, на котором развернут Сервер мобильных устройств Exchange ActiveSync и Сервером администрирования.

Проблемы с Сервером iOS MDM

Этот раздел содержит информацию об ошибках и проблемах, связанных с использованием Сервера iOS MDM, а также о способах их решения.

В этом разделе

Портал support.kaspersky.ru

Информация о некоторых проблемах, возникающих при использовании Сервера iOS MDM, приведена в Базе знаний на веб-сайте Службы технической поддержки http://support.kaspersky.ru/ks10mob.

Проверка доступности сервиса APN

Для проверки доступности сервиса APN вы можете использовать следующие команды утилиты Telnet:

- Со стороны веб-сервиса iOS MDM:

```
$ telnet gateway.push.apple.com 2195
```

- Со стороны iOS MDM-устройства (проверку необходимо провести из сети, в которой находится устройство):

```
$ telnet 1-courier.push.apple.com 5223
```

Рекомендуемая последовательность действий для решения проблем с веб-сервисом iOS MDM

► *Если при использовании веб-сервиса iOS MDM возникают проблемы, выполните следующие действия:*

1. Проверьте, что сертификаты корректны.
2. Проверьте события Консоли администрирования на наличие ошибок и невыполненных команд со стороны Сервера iOS MDM.
3. Проверьте мобильное устройство с помощью консоли приложения iPhone Configuration Utility.
4. Проверьте файлы трассировки веб-сервиса iOS MDM: внутренние сервисы, такие как RPC-сервис и веб-сервис (100 потоков), должны быть успешно запущены.

Проверка корректности сертификата веб-сервиса iOS MDM с помощью мультиплатформенной утилиты OpenSSL

Пример команды:

```
$ openssl s_client -connect mymdm.mycompany.com:443
```

Результат выполнения:

```
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

...

.
```

Проверка трассировок веб-сервиса iOS MDM

О том, как получить трассировки веб-сервиса iOS MDM, см. статью в Базе знаний на веб-сайте Службы технической поддержки http://support.kaspersky.ru/9792.

Пример успешных трассировок:

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]

Пример трассировок с занятым портом:

[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

Проверка трассировок с помощью консоли приложения iPhone Configuration Utility

Пример успешных трассировок:

Службы, отвечающие за 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...

Проблемы с KES-устройствами

Этот раздел содержит информацию об ошибках и проблемах, связанных с использованием KES-устройств, а также о способах их решения.

В этом разделе

Портал support.kaspersky.ru

Информация о проблемах, возникающих при работе с KES-устройствами, приведена в Базе знаний на веб-сайте Службы технической поддержки http://support.kaspersky.ru/ks10mob.

Проверка настроек сервиса Google Firebase Cloud Messaging

Проверка настроек сервиса Google Firebase Cloud Messaging может быть выполнена на портале Google https://code.google.com/apis/console/#project:[YOUR.

Проверка доступности сервиса Google Firebase Cloud Messaging

Для проверки доступности сервиса Google Firebase Cloud Messaging со стороны Kaspersky Security Center (см. раздел "Использование Google Firebase Cloud Messaging" на стр. 355) вы можете использовать команду утилиты Telnet:

```
telnet android.googleapis.com 443
```

Масштабирование Kaspersky Security Center

В этом разделе представлена информация по масштабированию Kaspersky Security Center. В разделе приведена следующая информация:

- об ограничениях Kaspersky Security Center;
- о расчетах для ключевых узлов Kaspersky Security Center – Серверов администрирования и агентов обновлений;
    - об аппаратных требованиях к Серверам администрирования и к агентам обновлений;
    - о расчете количества и иерархии Серверов администрирования;
    - о расчете количества и конфигурации агентов обновлений;
- о настройке параметров сохранения событий в базе данных в зависимости от числа устройств в сети;
- о настройке параметров некоторых задач для обеспечения оптимальной производительности Kaspersky Security Center;
- о потреблении трафика (нагрузке на сеть) между Сервером администрирования Kaspersky Security Center и каждым защищаемым устройством.

Рекомендуется обращаться к этому руководству в следующих ситуациях:

- при планировании ресурсов перед установкой Kaspersky Security Center;
- при планировании существенных изменений размеров сети, в которой развернут Kaspersky Security Center;
- при переходе от тестового режима использования Kaspersky Security Center на маленьком участке сети к полноценному использованию Kaspersky Security Center в сети организации;

- при изменениях в наборе используемых функциональностей Kaspersky Security Center.

Для достижения и сохранения оптимальной производительности при различных условиях работы учитывайте количество устройств в сети, топологию сети и необходимый вам набор функций Kaspersky Security Center.

Все рекомендации и расчеты приведены для сетей, в которых Kaspersky Security Center управляет защитой устройств с установленным программным обеспечением "Лаборатории Касперского", в том числе мобильных. Если мобильные устройства необходимо учитывать отдельно, это специально оговаривается.

В этом разделе

Информация об ограничениях Kaspersky Security Center

В таблице ниже приведены ограничения текущей версии Kaspersky Security Center 10 Service Pack 3.

Таблица 41. Ограничения Kaspersky Security Center 10 Service Pack 3

Тип ограничения	Значение
Максимальное количество управляемых устройств на один Сервер администрирования	100 000
Максимальное количество устройств с установленным флажком **Не разрывать соединение с Сервером администрирования**	300
Максимальное количество групп администрирования	10 000
Максимальное количество хранимых событий	45 000 000
Максимальное количество политик	2000
Максимальное количество задач	2000
Максимальное суммарное количество объектов Active Directory (подразделений и учетных записей пользователей, устройств и групп безопасности)	1 000 000
Максимальное количество профилей в политике	100
Максимальное количество подчиненных Серверов у одного главного Сервера администрирования	500
Максимальное количество виртуальных Серверов администрирования	500
Максимальное количество устройств, которые может обслуживать один агент обновлений	500, не считая мобильных устройств
Максимальное количество мобильных устройств на один Сервер администрирования	100 000 минус количество стационарных управляемых устройств

Расчеты для Серверов администрирования

В этом разделе приведены программно-аппаратные требования к устройствам, которые используются в качестве Серверов администрирования, и рекомендации по расчету количества и иерархии Серверов администрирования в зависимости от устройства сети организации.

В этом разделе

Расчет аппаратных ресурсов для Сервера администрирования

В этом разделе приведены расчеты, которыми можно руководствоваться при планировании аппаратных ресурсов для Сервера администрирования. Отдельно приводится рекомендация по расчету места на диске при использовании функциональности Системное администрирование.

В этом разделе

Аппаратные требования для СУБД и Сервера администрирования

В таблицах ниже приведены минимальные аппаратные требования СУБД и Сервера администрирования, полученные в ходе тестирования. Полный список поддерживаемых операционных систем и СУБД см. в перечне аппаратных и программных требований (см. раздел «Аппаратные и программные требования» на стр. 18).

Сервер администрирования и SQL-сервер на разных устройствах, в сети 50 000 устройств

Таблица 42. Конфигурация устройства с Сервером администрирования

Оборудование	Значение
Процессор	4 ядра, 2500 МГц
Память	8 ГБ
Жесткий диск	300 ГБ, желателен RAID
Сетевой адаптер	1 Гбит

Таблица 43. Конфигурация устройства с SQL-сервером

Оборудование	Значение
Процессор	4 ядра, 2500 МГц
Память	16 ГБ
Жесткий диск	200 ГБ SATA RAID
Сетевой адаптер	1 Гбит

Сервер администрирования и SQL-сервер на одном устройстве, в сети 50 000 устройств

Таблица 44. Конфигурация устройства с Сервером администрирования и SQL-сервером

Оборудование	Значение

Оборудование	Значение
Процессор	8 ядер, 2500 МГц
Память	16 ГБ
Жесткий диск	500 ГБ SATA RAID
Сетевой адаптер	1 Гбит

Сервер администрирования и SQL-сервер на разных устройствах, в сети 100 000 устройств

Таблица 45. Конфигурация устройства с Сервером администрирования

Оборудование	Значение
Процессор	8 ядер, 2,13 ГГц
Память	8 ГБ
Жесткий диск	1 ТБ, RAID
Сетевой адаптер	1 Гбит

Таблица 46. Конфигурация устройства с SQL Server

Оборудование	Значение
Процессор	8 ядер, 2,53 ГГц
Память	26 ГБ
Жесткий диск	500 ГБ SATA RAID
Сетевой адаптер	1 Гбит

Тестирование проводилось со следующими настройками:

- на Сервере администрирования включено автоматическое назначение агентов обновлений, либо агенты обновлений назначены вручную по рекомендуемой таблице (см. раздел "Расчет количества и конфигурации агентов обновлений" на стр. 98);
- задача резервного копирования сохраняет резервные копии на файловый ресурс, расположенный на отдельном сервере (см. раздел "Резервное копирование и восстановление параметров Сервера администрирования" на стр. 217);
- период синхронизации Агентов администрирования настроен в соответствии с таблицей ниже.

Таблица 47. Период синхронизации Агентов администрирования

Период синхронизации, минуты	Количество управляемых устройств
15	10 000
30	20 000
45	30 000
60	40 000
75	50 000
150	100 000

Расчет места в базе данных

Место, которое будет занято в базе данных, можно приблизительно оценить по следующей формуле:

(200 * C + 2.3 * E + 2.5 * A), КБ

где:

- "C" – количество устройств.
- "E" – количество сохраняемых событий (см. раздел "Скорость заполнения событиями базы данных" на стр. 407).

- "A" – суммарное количество объектов Active Directory:
  - учетных записей устройств;
  - учетных записей пользователей;
  - учетных записей групп безопасности;
  - подразделений Active Directory.

  Если сканирование Active Directory выключено, то "A" следует считать равным нулю.

Если вы планируете включить в параметрах политики Kaspersky Endpoint Security информирование Сервера администрирования о запускаемых программах, то для хранения информации о запускаемых программах в базе данных дополнительно потребуется (0,03 * C) ГБ.

Если Сервер администрирования распространяет обновления Windows (играет роль WSUS-сервера), то в базе данных дополнительно потребуется 2,5 ГБ.

В ходе работы в базе данных всегда образуется так называемое *незанятое пространство* (unallocated space). Поэтому реальный размер файла базы данных (по умолчанию файл KAV.MDF в случае использования СУБД "SQL Server") часто оказывается примерно в два раза больше, чем занятое в базе данных место.

Размер журнала транзакций (по умолчанию файл KAV_log.LDF в случае использования СУБД "SQL Server") может достигать 2 ГБ.

Расчет места на диске (с учетом и без учета использования Системного администрирования)

Расчет места на диске без учета использования функциональности Системное администрирование

Место на диске Сервера администрирования, требуемое для папки %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit, можно приблизительно оценить по формуле:

(220.0 * C + 0.15 * E + 0.17 * A), КБ

где:

- "C" – количество устройств.
- "E" – количество сохраняемых событий.
- "A" – суммарное количество объектов Active Directory:
  - учетных записей устройств;
  - учетных записей пользователей;
  - учетных записей групп безопасности;
  - подразделений Active Directory.

Если сканирование Active Directory выключено, то "A" следует считать равным нулю.

Расчет дополнительного места на диске с учетом использования функциональности Системное администрирование

- Обновления. В папке общего доступа требуется дополнительно не менее 4 ГБ для хранения обновлений.
- Инсталляционные пакеты. При наличии на Сервере администрирования инсталляционных пакетов в папке общего доступа дополнительно потребуется количество места, равное суммарному размеру устанавливаемых имеющихся инсталляционных пакетов.
- Задачи удаленной установки. При наличии на Сервере администрирования задач удаленной установки на диске дополнительно потребуется количество места на диске (в папке %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit), равное суммарному размеру устанавливаемых инсталляционных пакетов.
- Патчи. Если Сервер администрирования используется для установки патчей, то потребуется дополнительное место на диске:
  - В папке для хранения патчей – количество места, равное суммарному размеру всех загруженных патчей. По умолчанию патчи хранятся в папке %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\wusfiles (вы можете назначить для хранения патчей другую папку при помощи утилиты

klsrvswch). Если Сервер администрирования используется в качестве WSUS, то рекомендуется зарезервировать под эту папку не менее 100 ГБ.

- В папке %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit – количество места, равное суммарному размеру тех патчей, на которые ссылаются имеющиеся экземпляры задачи установки обновлений (патчей) и закрытия уязвимостей.

Расчет количества и конфигурации Серверов администрирования

Чтобы снизить нагрузку на главный Сервер администрирования, вы можете назначить в каждую группу администрирования отдельный Сервер администрирования. Количество Серверов администрирования, подчиненных главному Серверу, не может превышать 500.

Рекомендуется выстраивать конфигурацию Серверов администрирования в зависимости от того, как устроена сеть в вашей организации. Типовые конфигурации описаны в соответствующем разделе справки (см. раздел "Типовые конфигурации Kaspersky Security Center" на стр. 89).

Расчеты для агентов обновлений и шлюзов соединений

В этом разделе приведены аппаратные требования к устройствам, которые используются в качестве агентов обновлений, и рекомендации по расчету количества агентов обновлений и шлюзов соединений в зависимости от устройства сети организации.

В этом разделе

Оценка места на диске для агента обновлений

Для работы агента обновлений необходимо не менее 4 ГБ свободного места на диске.

При наличии на Сервере администрирования задач удаленной инсталляции, на устройстве с агентом обновлений дополнительно потребуется количество места на диске, равное суммарному размеру устанавливаемых инсталляционных пакетов.

При наличии на Сервере администрирования одного или нескольких экземпляров задачи установки обновлений (патчей) и закрытия уязвимостей, на устройстве с агентом обновлений дополнительно потребуется количество места на диске, равное удвоенному суммарному размеру всех устанавливаемых патчей.

Расчет количества и конфигурации агентов обновлений

Чем больше клиентских устройств в сети, тем больше необходимость в агентах обновлений. Рекомендуется не отключать автоматическое назначение агентов обновлений. При включенном автоматическом назначении агентов обновлений Сервер администрирования назначает агенты обновлений, если число клиентских устройств достаточно велико, и определяет их конфигурацию.

Использование постоянно включенных и доступных устройств

Если вы планируете использовать в качестве агентов обновлений какие-то определенные устройства (например, выделенные для этого серверы), то вы можете не использовать автоматическое назначение агентов обновлений. В этом случае убедитесь, что устройства, которые вы хотите назначить агентом обновлений, имеют достаточно свободного места на диске (см. раздел "Оценка места на диске для агента обновлений" на стр. 404), их не отключают регулярно и на них выключен "спящий режим".

Если вы планируете использовать в качестве агента обновлений специально выделенное для этого устройство, то рекомендуется назначать один агент обновлений не более чем на 1000 клиентских устройств. Если вы планируете использовать в качестве агентов обновлений обычное клиентское устройство, то рекомендуется назначать один агент обновлений не более чем на 100 устройств. При превышении рекомендуемого числа клиентских устройств на один агент обновлений возрастает нагрузка на процессор, что может помешать повседневной работе пользователей.

Использование устройств, которые регулярно бывают отключены или недоступны

Если устройство, назначенное агентом обновлений, отключено или по другим причинам недоступно, то управляемые устройства, которые подключаются к этому агенту обновлений, могут обращаться за обновлениями к Серверу администрирования.

Если вы планируете использовать в качестве агентов обновлений устройства, которые регулярно бывают отключены или уходят в "спящий режим", то во избежание избыточной нагрузки на Сервер администрирования рекомендуется назначать агенты обновлений следующим образом (см. таблицу ниже):

Таблица 48. Количество агентов обновлений в зависимости от количества устройств в сети

Количество устройств в сети	Количество агентов обновлений
Менее 10	0 (не назначать агенты обновлений)
10–30	1
30–300	2
Более 300	(N/1000 +1), где N – число устройств в сети, но не менее 3 агентов обновлений

Расчет количества шлюзов соединений

Рекомендуется использовать в качестве шлюза соединений выделенное устройство и назначать на один шлюз соединений не более 500 управляемых устройств, в т.ч. мобильных.

Расчеты, связанные с хранением событий в базе данных

В этом разделе приведены расчеты, связанные с хранением событий в базе данных Сервера администрирования, и даны рекомендации, как минимизировать количество событий и таким образом снизить нагрузку на Сервер администрирования.

В этом разделе

Скорость заполнения событиями базы данных

В этом разделе приведены примеры скорости заполнения базы данных Сервера администрирования событиями, возникающими в работе управляемых программ.

Информация о событиях в работе управляемых программ передается с клиентского устройства и регистрируется в базе данных Сервера администрирования.

В базу данных поступает (Ne*Nh) событий в день (см. таблицу ниже). Здесь Nh – количество клиентских устройств, на которых установлены управляемые программы, Ne – количество событий в день, информацию о которых передает с клиентского устройства установленная на нем управляемая программа Kaspersky Endpoint Security для Windows. По умолчанию Kaspersky Endpoint Security для Windows (версии 10 и 11) при штатной работе передает в базу данных около 20 событий в день. Максимальное количество событий, которое может обработать Kaspersky Security Center, составляет 2 000 000 событий в день.

Таблица 49. Скорость заполнения событиями базы данных (при штатной работе)

Количество устройств, на которых установлена программа Kaspersky Endpoint Security	**Количество событий, передаваемое в базу данных в день**
100	до 2 000
1000	до 20 000
10 000	до 200 000
100 000	до 2 000 000

Максимальное количество событий, хранящихся в базе данных, определяется в разделе **Хранение событий** окна свойств Сервера администрирования. По умолчанию в базе данных хранится не более 400 000 событий.

Хранение информации о событиях для задач и политик

По умолчанию в свойствах каждой задачи и каждой политики указано сохранение в журнале всех событий, связанных с выполнением задачи и применением политики.

Однако если задача запускается достаточно часто (например, более одного раза в неделю) и на достаточно большом количестве устройств (например, более 10 000), количество событий может оказаться слишком большим, и события могут заполнить базу данных. В таком случае рекомендуется указать в свойствах задачи один из двух других вариантов:

- **Сохранять события о ходе выполнения задачи**. В этом случае с каждого устройства, на котором выполнена задача, в базу данных поступает только информация о запуске задачи, о ее ходе и о ее выполнении (успешном, с предупреждением либо с ошибкой).
- **Сохранять только результат выполнения**. В этом случае с каждого устройства, на котором выполнена задача, в базу данных поступает только информация о выполнении задачи (успешном, с предупреждением либо с ошибкой).

Если политика определена для достаточно большого количества устройств (например, более 10 000), количество событий также может оказаться слишком большим, и события могут заполнить базу данных. В таком случае рекомендуется выбрать в свойствах политики только наиболее важные события и включить их сохранение. Сохранение всех других событий рекомендуется отключить.

Таким образом вы уменьшаете количество событий в базе данных, увеличиваете скорость работы сценариев, связанных с анализом таблицы событий в базе данных, и снижаете риск вытеснения важных событий большим количеством событий об изменении состояния групповых задач.

Вы также можете уменьшить срок хранения событий, связанных с задачей (политикой). По умолчанию этот срок составляет семь дней для событий, связанных с задачей, и 30 дней для событий, связанных с политикой. При изменении срока хранения событий принимайте в расчет порядок работы, принятый в вашей организации, и количество времени, которое системный администратор может уделять анализу каждого события.

Вносить изменения в параметры хранения событий целесообразно в любом из следующих случаев:

- события об изменении промежуточных состояний групповых задач и о применении политик занимают значительный процент всех событий в базе данных Kaspersky Security Center;
- в журнале событий Kaspersky Event Log появляются записи об автоматическом удалении событий при превышения заданного лимита на общее число событий, хранимых в базе данных.

Выбирайте варианты сохранения событий исходя из того, что оптимальное количество событий, поступающих с одного устройства в сутки, должно быть не более 20 (см. раздел "Скорость заполнения событиями базы данных" на стр. 407); при необходимости вы можете немного увеличить этот лимит, но только если количество устройств в вашей сети невелико (менее 10 000).

Особенности и оптимальные параметры некоторых задач

Некоторые задачи имеют особенности, связанные с количеством устройств в сети. В этом разделе даны рекомендации по оптимальной настройке параметров для таких задач.

Опрос сети, задача резервного копирования данных, задача обслуживания базы данных и групповые задачи обновления Kaspersky Endpoint Security входят в базовую функциональность Kaspersky Security Center.

Задача инвентаризации входит в функциональность Системное администрирование и недоступна, если эта функциональность не активирована.

В этом разделе

Опрос сети

Не рекомендуется увеличивать частоту опроса сети, установленную по умолчанию, так как это может создать чрезмерную нагрузку на контроллеры домена. Рекомендуется, наоборот, устанавливать расписание опроса сети с минимально возможной частотой, насколько позволяют потребности вашей организации. В таблице ниже приведены рекомендации по расчету оптимального расписания опроса сети.

Таблица 50. Расписание опроса сети

Количество устройств в сети	Рекомендуемая частота опроса сети
Менее 10 000	Установленная по умолчанию или реже
10 000 и более	Один раз в сутки или реже

Задачи резервного копирования данных Сервера администрирования и обслуживания базы данных

Сервер администрирования перестает функционировать во время выполнения следующих задач:

- Резервное копирование данных Сервера администрирования.

- Обслуживание базы данных.

Пока выполняются эти задачи, данные не могут поступать в базу данных.

Вам может потребоваться изменить расписание этих задач так, чтобы их выполнение не пересекалось по времени с выполнением других задач Сервера администрирования.

Групповые задачи обновления Kaspersky Endpoint Security

Если источником обновлений является Сервер администрирования, то для групповых задач обновления Kaspersky Endpoint Security версии 10 и выше рекомендуется расписание **При загрузке обновлений в хранилище** с установленным флажком **Автоматически определять интервал для распределения запуска задачи**.

Если вы создали на каждом агенте обновлений локальную задачу загрузки обновлений в хранилище с серверов "Лаборатории Касперского", то для групповой задачи обновления Kaspersky Endpoint Security рекомендуется периодическое расписание. Значение периода рандомизации в этом случае должно составлять один час.

Задача инвентаризации программного обеспечения

Количество исполняемых файлов, получаемых Сервером администрирования от одного устройства, не может превышать 150 000. При достижении этого ограничения Kaspersky Security Center не получит новые файлы.

Количество файлов на обыкновенном управляемом устройстве, как правило, составляет не более 60 000. Количество исполняемых файлов на файловом сервере может быть больше и может даже превышать порог в 150 000.

Тестовые замеры показали, что на устройстве под управлением системы Windows 7, на котором установлена программа Kaspersky Endpoint Security 11 и не установлены никакие сторонние программы, результаты выполнения задачи инвентаризации следующие:

- Со снятыми флажками **Инвентаризация DLL-модулей** и **Инвентаризация файлов скриптов**: около 3000 файлов.
- С установленными флажками **Инвентаризация DLL-модулей** и **Инвентаризация файлов скриптов**: от 10 000 до 20 000 файлов, в зависимости от количества установленных обновлений операционной системы.
- С установленным одним флажком **Инвентаризация файлов скриптов**: около 10 000 файлов.

Информация о нагрузке на сеть между Сервером администрирования и защищаемыми устройствами

В этом разделе приводятся результаты тестовых замеров трафика в сети с указанием условий, при которых проводились замеры. Вы можете использовать эту информацию как справочную при планировании сетевой инфраструктуры и пропускной способности каналов внутри организации (либо между Сервером администрирования и организацией, в которой расположены защищаемые устройства). Зная пропускную способность сети, вы также можете приблизительно оценивать, сколько времени должно занять та или иная операция, связанная с передачей данных.

В этом разделе

Расход трафика при выполнении различных сценариев

В таблице ниже приводятся результаты тестовых замеров трафика между Сервером администрирования и управляемым устройством при выполнении различных сценариев.

Синхронизация устройства с Сервером администрирования происходит по умолчанию раз в 15 минут либо реже (см. раздел "Опрос сети" на стр. 410). Однако если вы меняете на Сервере администрирования параметры политики или задачи, то происходит досрочная синхронизация устройств, для которых применима эта политика (задача), и новые параметры передаются на устройства.

Таблица 51. Трафик между Сервером администрирования и управляемым устройством

Сценарий	Трафик от Сервера к управляемому устройству	Трафик от управляемого устройства к Серверу
Установка Kaspersky Endpoint Security 11 для Windows с обновленными базами	208 МБ	5,7 МБ
Установка Агента администрирования	40 МБ	1 МБ
Совместная установка Агента администрирования и Kaspersky Endpoint Security 11 для Windows	248 МБ	6,3 МБ
Первоначальное обновление антивирусных баз без обновления баз в пакете (при отказе от участия в KSN)	160 МБ	5,5 МБ
Ежесуточное обновление антивирусных баз; первоначальное обновление антивирусных баз (при участии в KSN)	32 МБ	5,3 МБ
Первоначальная синхронизация до обновления баз на устройстве (передача политик и задач)	254 КБ	221 КБ

Сценарий	Трафик от Сервера к управляемому устройству	Трафик от управляемого устройства к Серверу
Первоначальная синхронизация после обновления баз на устройстве	160 КБ	54 КБ
Синхронизация при отсутствии изменений на Сервере администрирования (по расписанию)	20 КБ	32 КБ
Синхронизация при изменении одного параметра в политике группы (досрочная, сразу после внесения изменения)	11 КБ	12 КБ
Синхронизация при изменении одного параметра в групповой задаче (досрочная, сразу после внесения изменения)	12 КБ	11 КБ
Принудительная синхронизация	7 КБ	11 КБ
Событие **Найден вирус** (1 вирус)	28 КБ	42 КБ
Событие **Найден вирус** (10 вирусов)	46 КБ	73 КБ

В таблице ниже представлен средний расход трафика за сутки между Сервером администрирования и управляемым устройством с установленным Агентом администрирования и Kaspersky Endpoint Security 11 для Windows при следующих условиях:

- Устройство не назначено агентом обновлений.
- Функциональность Системное администрирование не включена.
- Период синхронизации с Сервером администрирования составляет 15 минут.

Таблица 52. Средний расход трафика за сутки

Трафик от Сервера к управляемому устройству	Трафик от управляемого устройства к Серверу
52 МБ	4 МБ

Процедура приемки

Перед вводом программы в эксплуатацию проводится процедура приемки, включающая проверку правильной установки, работоспособности и соответствия безопасной (сертифицированной) конфигурации.

В этом разделе

Безопасное состояние

Программа находится в безопасном состоянии (сертифицированной конфигурации), если выполняются следующие условия:

Параметры программы находятся в рамках допустимых значений, приведенных в приложении к этому документу (см. раздел "Приложение. Сертифицированное состояние программы: параметры и их значения" на стр. 430).

Проверка работоспособности Kaspersky Security Center

После установки Kaspersky Security Center вы можете проверить его работоспособность с помощью выполнения алгоритма проверки. В таблице ниже приведен порядок действий для проверки работоспособности программы и ожидаемые результаты выполнения этих действий.

Таблица 53. Шаги алгоритма проверки работоспособности Kaspersky Security Center

Номер шага	Действие	Результат
1	Подключитесь к Серверу администрирования с помощью Консоли Администрирования (см. раздел "Настройка подключения Консоли администрирования к Серверу администрирования" на стр. 174).	Консоль администрирования подключена к Серверу администрирования. В списке управляемых устройств появилось как минимум одно устройство Сервера администрирования.
2	Выполните первоначальную настройку Сервера администрирования с помощью мастера первоначальной настройки (см. раздел "Мастер первоначальной настройки Сервера администрирования" на стр. 176).	Мастер первоначальной настройки создал необходимые для развертывания защиты политики и задачи с параметрами по умолчанию.
3	Установите Агент администрирования и Kaspersky Endpoint Security для Windows на устройство (см. раздел "Удаленная установка программ" на стр. 265).	Управляемое устройство, на которое была произведена установка программ, присутствует в списке нераспределенных устройств. В свойствах устройства в разделе **Программы** присутствуют программы Агент администрирования и Kaspersky Endpoint Security для Windows.

Номер шага	Действие	Результат
4	Загрузите обновления в хранилище Сервера администрирования, запустив задачу загрузки обновлений в хранилище. Подробнее см. в Руководстве по эксплуатации, в разделе "Создание задачи загрузки обновлений в хранилище".	Задача завершена успешно и обновления загружены в хранилище.
5	Обновите программу защиты Kaspersky Endpoint Security для Windows. Для этого выполните задачу обновления. Подробнее см. в Руководстве по эксплуатации, в разделе "Автоматическая установка обновлений для Kaspersky Endpoint Security на устройства".	В свойствах управляемого устройства в разделе **Программы** в свойствах программы Kaspersky Endpoint Security для Windows дата последнего обновления баз соответствует дате последнего запуска задачи обновления.
6	Внесите произвольные тестовые изменения в политику Kaspersky Endpoint Security для Windows.	Политика применена на управляемом устройстве, обнаруженном в сети: • В свойствах политики присутствует информация о том, что она применена на устройства. • Параметры программы защиты соответствуют параметрам политики.

Номер шага	Действие	Результат
7	Скопируйте на одно из управляемых устройств тестовый файл EICAR (см. раздел "Проверка распространения уведомлений" на стр. 366).	В журнале событий есть записи об обнаружении и ликвидации зараженного файла. В свойствах устройства в разделе **Защита** в поле **Обнаружено вирусов** значение увеличилось на один.

Приложения

В этом разделе содержится справочная и дополнительная информация, касающаяся использования Kaspersky Security Center:

- сведения об ограничениях текущей версии программы (максимальные количества управляемых устройств, политик, задач и прочее);
- аппаратные требования для установки Сервера администрирования и СУБД;
- справочная информация о количестве места на диске, необходимого для работы компонентов программы;
- справочная информация о среднесуточном объеме трафика между Агентом администрирования и Сервером администрирования;
- информация о решении типовых проблем, возникающих при использовании Kaspersky Security Center, в том числе о решении проблем с управлением мобильными устройствами пользователей.

В этом разделе

Ограничения Kaspersky Security Center

В таблице ниже приведены ограничения текущей версии Kaspersky Security Center 10 Service Pack 3.

Таблица 54. Ограничения Kaspersky Security Center 10 Service Pack 3

Тип ограничения	Значение
Максимальное количество управляемых устройств	100 000
Максимальное количество устройств с установленным флажком **Не разрывать соединение с Сервером администрирования**	300
Максимальное количество групп администрирования	10 000
Максимальное количество хранимых событий	15 000 000
Максимальное количество политик	2000
Максимальное количество задач	2000
Максимальное суммарное количество объектов Active Directory (подразделений и учетных записей пользователей, устройств и групп безопасности)	1 000 000
Максимальное количество профилей в политике	100
Максимальное количество подчиненных Серверов у одного главного Сервера администрирования	500
Максимальное количество виртуальных Серверов администрирования	500
Максимальное количество устройств, которые может обслуживать один агент обновлений	500

Аппаратные требования для СУБД и Сервера администрирования

В таблицах ниже приведены минимальные аппаратные требования СУБД и Сервера администрирования, полученные в ходе тестирования. Полный список поддерживаемых операционных систем и СУБД см. в перечне аппаратных и программных требований (см. раздел «Аппаратные и программные требования» на стр. 18).

Сервер администрирования и SQL-сервер на разных устройствах, в сети 50 000 устройств

Таблица 55. Конфигурация устройства с Сервером администрирования

Оборудование	Значение
Процессор	4 ядра, 2500 МГц
Память	8 ГБ
Жесткий диск	300 ГБ, желателен RAID
Сетевой адаптер	1 Гбит

Таблица 56. Конфигурация устройства с SQL-сервером

Оборудование	Значение
Процессор	4 ядра, 2500 МГц
Память	16 ГБ
Жесткий диск	200 ГБ SATA RAID
Сетевой адаптер	1 Гбит

Сервер администрирования и SQL-сервер на одном устройстве, в сети 50 000 устройств

Таблица 57. Конфигурация устройства с Сервером администрирования и SQL-сервером

Оборудование	Значение

Оборудование	Значение
Процессор	8 ядер, 2500 МГц
Память	16 ГБ
Жесткий диск	500 ГБ SATA RAID
Сетевой адаптер	1 Гбит

Сервер администрирования и SQL-сервер на разных устройствах, в сети 100 000 устройств

Таблица 58. Конфигурация устройства с Сервером администрирования

Оборудование	Значение
Процессор	8 ядер, 2,13 ГГц
Память	8 ГБ
Жесткий диск	1 ТБ, RAID
Сетевой адаптер	1 Гбит

Таблица 59. Конфигурация устройства с SQL Server

Оборудование	Значение
Процессор	8 ядер, 2,53 ГГц
Память	26 ГБ
Жесткий диск	500 ГБ SATA RAID
Сетевой адаптер	1 Гбит

Тестирование проводилось со следующими настройками:

- на Сервере администрирования включено автоматическое назначение агентов обновлений, либо агенты обновлений назначены вручную по рекомендуемой таблице (см. раздел "Расчет количества и конфигурации агентов обновлений" на стр. 98);
- задача резервного копирования сохраняет резервные копии на файловый ресурс, расположенный на отдельном сервере (см. раздел "Резервное копирование и восстановление параметров Сервера администрирования" на стр. 217);
- период синхронизации Агентов администрирования настроен в соответствии с таблицей ниже.

Таблица 60. Период синхронизации Агентов администрирования

Период синхронизации, минуты	Количество управляемых устройств
15	10 000
30	20 000
45	30 000
60	40 000
75	50 000
150	100 000

Оценка места на диске для агента обновлений

Для работы агента обновлений необходимо не менее 4 ГБ свободного места на диске.

При наличии на Сервере администрирования задач удаленной инсталляции, на устройстве с агентом обновлений дополнительно потребуется количество места на диске, равное суммарному размеру устанавливаемых инсталляционных пакетов.

При наличии на Сервере администрирования одного или нескольких экземпляров задачи установки обновлений (патчей) и закрытия уязвимостей, на устройстве с агентом

обновлений дополнительно потребуется количество места на диске, равное удвоенному суммарному размеру всех устанавливаемых патчей.

Предварительный расчет места в базе данных и на диске для Сервера администрирования

Оценка места в базе данных Сервера администрирования

Место, которое будет занято в базе данных, можно приблизительно оценить по следующей формуле:

(200 * C + 2,3 * E + 2,5 * A), КБ

где:

"C" – Количество устройств.

"E" – Количество сохраняемых событий.

"A" – Суммарное количество объектов Active Directory:

- учетных записей устройств;
- учетных записей пользователей;
- учетных записей групп безопасности;
- подразделений Active Directory.

Если сканирование Active Directory выключено, то "A" следует считать равным нулю.

Если Сервер администрирования распространяет обновления Windows (играет роль WSUS-сервера), то в базе данных дополнительно потребуется 2,5 ГБ.

Следует учитывать, что в ходе работы в базе данных всегда образуется так называемое "незанятое пространство" (unallocated space). Поэтому реальный размер файла базы данных (по умолчанию файл KAV.MDF в случае использования СУБД "SQL Server") часто оказывается примерно в два раза больше, чем занятое в базе данных место.

Размер журнала транзакций (по умолчанию файл KAV_log.LDF в случае использования СУБД "SQL Server") может достигать 2 ГБ.

Оценка места на диске для устройства с Сервером администрирования

Место на диске в директории %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit на устройстве с Сервером администрирования можно приблизительно оценить по формуле:

(220 * C + 0,15 * E + 0,17 * A), КБ

Значения переменных "C", "E" и "A" см. выше.

Обновления

В папке общего доступа требуется не менее 4 ГБ для хранения обновлений.

Инсталляционные пакеты

При наличии на Сервере администрирования инсталляционных пакетов в папке общего доступа дополнительно потребуется место, равное суммарному размеру имеющихся инсталляционных пакетов.

Задачи удаленной установки

При наличии на Сервере администрирования задач удаленной установки на устройстве с Сервером администрирования дополнительно потребуется количество места на диске (в папке %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit), равное суммарному размеру устанавливаемых инсталляционных пакетов.

Патчи

Если Сервер администрирования используется для установки патчей, то потребуется дополнительное место на диске:

- В папке для хранения патчей – количество места, равное суммарному размеру всех скачанных патчей. Папкой для хранения патчей по умолчанию является %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\wusfiles. Папка может быть изменена при помощи утилиты klsrvswch. Если Сервер администрирования используется в качестве WSUS, то рекомендуется зарезервировать под эту папку не менее 100 ГБ.

- В директории %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit – количество места, равное суммарному размеру патчей, на которые ссылаются имеющиеся экземпляры задачи установки обновлений (патчей) и закрытия уязвимостей.

Оценка трафика между Агентом администрирования и Сервером администрирования

В таблице ниже приведен среднесуточный трафик между Сервером администрирования Kaspersky Security Center 10 Service Pack 3 и управляемым устройством, на котором установлены Агент администрирования и Kaspersky Endpoint Security 11 для Windows.

Таблица 61. Среднесуточный трафик: Kaspersky Security Center 10 Service Pack 3

	От Сервера к управляемому устройству (download)	**От управляемого устройства к Серверу (upload)**
Средний ежесуточный трафик с параметрами задачи обновления по умолчанию	52 МБ	4 МБ
Средний ежесуточный трафик с выключенной задачей обновления	836 КБ	726 КБ

Приложение. Сертифицированное состояние программы: параметры и их значения

Этот раздел содержит перечень параметров программы, влияющих на безопасное состояние программы, и безопасные значения (диапазоны значений) параметров в сертифицированной конфигурации.

Изменение каких-либо из перечисленных параметров с их значений (диапазона значений) в сертифицированном конфигурации на другие значения выводит программу из безопасного состояния.

Таблица 62. Параметры и их значения для программы в сертифицированном состоянии

Параметр	Краткое описание и диапазон значений	Значение параметра для программы в сертифицированном состоянии
Месторасположение папки общего доступа	При установке Kaspersky Security Center папка общего доступа, которая по умолчанию называется KLSHARE, находится не в папке установки Сервера администрирования. По умолчанию указана папка <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.	Не в папке, где установлен Сервер администрирования Kaspersky Security Center.
Политики	Для каждой управляемой программы создана политика.	
Пароль на деинсталляцию Агента администрирования	В политике Агента администрирования установлен пароль на удаление Агента администрирования. Возможные значения: • установлен; • снят.	Установлен.

Параметр	Краткое описание и диапазон значений	Значение параметра для программы в сертифицированном состоянии
Защита паролем политики Kaspersky Endpoint Security для Windows. Параметр программы Kaspersky Endpoint Security для Windows, если эта программа установлена.	Защита паролем позволяет установить ограничение на управление всеми или отдельными функциями и параметрами Kaspersky Endpoint Security для Windows, снижая вероятность несанкционированного или непреднамеренного внесения изменений в работу программы. Возможные значения: • установлена; • снята.	Установлена.
Автоматическое обновление модулей Агентов администрирования	Обновления модулей Агента администрирования устанавливаются автоматически, после того как Сервер администрирования завершает задачу получения обновлений. Возможные значения: • включен; • выключен.	Выключен.

Параметр	Краткое описание и диапазон значений	Значение параметра для программы в сертифицированном состоянии
Установка применимых обновлений со статусом одобрения *Не определено*	Патчи "Лаборатории Касперского" со статусом одобрения *Не определено* устанавливаются автоматически на управляемые устройства сразу после загрузки с серверов обновлений. Возможные значения: • включен; • выключен.	Выключен.
Запуск задачи **Загрузка обновлений в хранилище**	Задача **Загрузка обновлений в хранилище** выполняет загрузку обновлений баз и программных модулей, которые копируются с источника обновлений и размещаются в папке общего доступа. Возможные значения: • вручную; • автоматически по расписанию.	Автоматически по расписанию. Рекомендуемый интервал запуска задачи – один раз в час.

Параметр	Краткое описание и диапазон значений	Значение параметра для программы в сертифицированном состоянии
Запуск задачи **Установка обновлений**	Задача **Установка обновлений** выполняет установку ранее загруженных в хранилище обновлений на клиентские устройства. Возможные значения: • вручную; • автоматически по расписанию.	Автоматически, по завершении задачи **Загрузка обновлений в хранилище**.

Параметр	Краткое описание и диапазон значений	Значение параметра для программы в сертифицированном состоянии
Передача данных сервису KSN	Kaspersky Security Network (KSN) – это инфраструктура онлайн-служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции программ "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний. Возможные значения передачи данных программы сервису KSN: • отключена; • включена.	Отключена.

Параметр	Краткое описание и диапазон значений	Значение параметра для программы в сертифицированном состоянии
Источник обновлений задачи **Загрузка обновлений в хранилище**	Источник обновлений баз и модулей управляемых программ "Лаборатории Касперского". Возможные значения: • Серверы обновлений "Лаборатории Касперского"; • Главный Сервер администрирования; • Локальная или сетевая папка.	• Главный Сервер администрирования; • Локальная или сетевая папка. Источник обновлений *Серверы обновлений "Лаборатории Касперского"* удален, чтобы программа не передавала информацию на серверы обновлений "Лаборатории Касперского".
Способ активации Сервера администрирования	Возможные значения: • с помощью файла ключа; • с помощью кода активации.	С помощью файла ключа.
Служба прокси-сервера активации "Лаборатории Касперского"	Служба прокси-сервера активации "Лаборатории Касперского" используется для обеспечения передачи запросов на активацию от управляемых программ к серверам активации "Лаборатории Касперского". Возможные значения: • отключена; • включена.	Отключена

Параметр	Краткое описание и диапазон значений	Значение параметра для программы в сертифицированном состоянии
Доверенные каналы с использованием SSL-протокола	Протокол SSL позволяет идентифицировать стороны, взаимодействующие при подключении (взаимодействие между Севером администрирования и устройствами), осуществлять шифрование передаваемых данных и обеспечивать их защиту от изменения при передаче. Возможные значения: • используется; • не используется.	Используется.
Права пользователей	Права обеспечивают доступ администраторов, пользователей и групп пользователей к разным функциям программы.	Минимально необходимые права настроены: только уполномоченные роли имеют права изменять параметры защиты.
Условия для статуса *Критический*	Набор условий при котором устройство принимает статус *Критический*.	Выбрано условие **Найдено много вирусов**. Параметр **Более чем** равен значению 0.

Параметр	Краткое описание и диапазон значений	Значение параметра для программы в сертифицированном состоянии
Максимальное количество событий, хранящихся в базе данных Сервера администрирования	Максимальное количество событий, которое хранится в базе данных Сервера администрирования, необходимое для проведения аудита программы.	Рекомендуется установить значение не меньше 400 000 событий.
Срок хранения событий	Срок, в течение которого события хранятся в базе данных Сервера администрирования, необходимый для проведения аудита программы.	Рекомендуется установить значения: • Для событий с уровнем важности *Критические* – не меньше 180 дней. • Для событий с уровнем важности *Предупреждение* – не меньше 90 дней. • Для событий с уровнем важности *Информационное сообщение* – не меньше 30 дней.
Срок хранения ревизий изменений объектов	Срок, в течение которого хранятся ревизии изменений объектов, необходимый для проведения регулярного аудита программы.	Рекомендуется установить значение не меньше 90 дней.

См. также

Настройка эталонных значений параметров программы

Этот раздел содержит инструкции по установке эталонных значений параметров программы. Настройка программы по эталонным параметрам необходима для работы сертифицированной конфигурации программы.

Месторасположение папки общего доступа Сервера администрирования

Измените месторасположение папки общего доступа Сервера администрирования. Папка должна находиться не в папке установки Сервера администрирования.

► *Чтобы изменить папку общего доступа при установке Сервера администрирования, выполните следующие действия:*

1. Запустите установку Сервера администрирования (см. раздел "Установка и удаление Kaspersky Security Center" на стр. 129).
2. В окне **Папка общего доступа** мастера установки измените путь к папке общего доступа (см. раздел "Шаг 10. Определение папки общего доступа" на стр. 154).

► *Чтобы изменить папку общего доступа установленного Сервера администрирования, выполните следующие действия:*

1. В дереве консоли выберите узел Сервер администрирования.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования в разделе **Папка общего доступа** измените расположение папки общего доступа.

Политики

Настройте активные политики для каждой управляемой программы "Лаборатории Касперского" для всех групп администрирования, в том числе политику Агента администрирования и политику Kaspersky Endpoint Security для Windows. Для политики Агента администрирования необходимо установить пароль на удаление программы Агента администрирования. Для политики Kaspersky Endpoint Security для Windows необходимо настроить защиту паролем на удаление, изменение или восстановление программы Kaspersky Endpoint Security для Windows.

Пароль на деинсталляцию Агента администрирования

► *Чтобы установить пароль на удаление программы Агента администрирования, выполните следующие действия:*

1. В дереве консоли перейдите в папку **Политики**.
2. В контекстном меню политики Агент администрирования выберите пункт **Свойства**.
3. В окне свойств политики в разделе **Параметры** выберите установите флажок **Использовать пароль деинсталляции**.
4. Нажмите на кнопку **Изменить**.
5. В окне **Изменения пароля** введите пароль.
6. В окне **Защита паролем** в блоке **Область действия пароля** установите флажок **Удаление / Изменение / Восстановление программы**.
7. Нажмите на кнопку **ОК**.

Защита паролем политики Kaspersky Endpoint Security для Windows

► *Чтобы установить защиту паролем на удаление, изменение или восстановление программы Kaspersky Endpoint Security для Windows, выполните следующие действия:*

1. В дереве консоли перейдите в папку **Политики**.
2. В контекстном меню политики Kaspersky Endpoint Security для Windows выберите пункт **Свойства**.

3. В окне свойств политики в разделе **Дополнительные параметры** выберите подраздел **Параметры программы**.

4. В разделе **Параметры программы** в блоке **Защита паролем** нажмите на кнопку **Настроить**.

5. В окне **Защита паролем** установите флажок **Включить защиту паролем**.

6. В окне **Защита паролем** в блоке **Область действия пароля** установите флажок **Удаление / Изменение / Восстановление программы**.

7. Нажмите на кнопку **ОК**.

Автоматическое обновление модулей Агентов администрирования

По умолчанию обновления модулей Агента администрирования устанавливаются автоматически, после того как Сервер администрирования завершает задачу получения обновлений. Отключите автоматическое обновление модулей Агента администрирования. Сертификации подлежат только определенные версии исполняемых модулей программы.

► *Чтобы отключить автоматическое обновление исполняемых модулей программы, выполните следующие действия:*

1. В дереве консоли выберите папку **Задачи**.

2. В папке **Задачи** выберите задачу **Загрузка обновлений в хранилище**.

3. В контекстном меню задачи выберите пункт **Свойства**.

4. В окне свойств задачи выберите раздел **Параметры**.

5. В подразделе **Прочие параметры** перейдите по ссылке **Настроить**.

   Откроется окно **Прочие параметры**.

6. Снимите флажок **Обновлять модули Агентов администрирования**.

   Если флажок снят, автоматическая установка обновлений не выполняется. Полученные обновления модулей Агента администрирования можно установить вручную.

7. Нажмите на кнопку **ОК**.

Установка применимых обновлений со статусом одобрения "Не определено"

1. По умолчанию патчи "Лаборатории Касперского" со статусом одобрения *Не определено* устанавливаются автоматически на управляемые устройства сразу после загрузки с серверов обновлений. Отключите автоматическую установку патчей "Лаборатории Касперского" со статусом одобрения *Не определено*.

► *Чтобы отключить автоматическую установку патчей "Лаборатории Касперского" со статусом одобрения* Не определено, выполните следующие действия:

1. В дереве консоли перейдите в папку **Политики**.
2. В папке **Политики** выберите политику Агент администрирования.
3. В контекстном меню политики выберите пункт **Свойства**.
4. В разделе свойств политики **Управление патчами и обновлениями** снимите флажок **Устанавливать применимые обновления со статусом одобрения "Не определено"**.

   Если флажок **Устанавливать применимые обновления со статусом одобрения "Не определено"** снят, загруженные патчи "Лаборатории Касперского" со статусом *Не определено* устанавливаются после того, как администратор изменит их статус на *Одобрен*.
5. Нажмите на кнопку **ОК**.

Запуск задачи Загрузка обновлений в хранилище

Настройте автоматический запуск задач **Загрузка обновлений в хранилище** и **Установка обновлений**.

Рекомендуемый интервал автоматического запуска задачи Сервера администрирования **Загрузка обновлений в хранилище** составляет один раз в час.

► *Чтобы настроить автоматический запуск задачи Сервера администрирования **Загрузка обновлений в хранилище** один раз в час, выполните следующие действия:*

1. В дереве консоли перейдите в папку **Задачи**.

2. В контекстном меню задачи **Загрузка обновлений в хранилище** выберите пункт **Свойства**.

3. В окне свойств перейдите в раздел **Расписание**.

4. В поле **Запуск по расписанию** выберите значение **Каждый N час**.

5. В поле **Интервал запуска (ч)** установите значение 1.

6. Нажмите на кнопку **ОК**.

Запуск задачи Установка обновлений

Настройте запуск задачи **Установка обновлений** после выполнения задачи **Загрузка обновлений в хранилище**.

► *Чтобы настроить автоматический запуск задачи **Установка обновлений** после выполнения задачи **Загрузка обновлений в хранилище**, выполните следующие действия:*

1. В дереве консоли перейдите в папку **Задачи**.

2. В контекстном меню задачи **Установка обновлений** выберите пункт **Свойства**.

3. В окне свойств перейдите в раздел **Расписание**.

4. В поле **Запуск по расписанию** выберите значение **По завершении другой задачи**.

5. В поле **Название задачи** выберите значение **Загрузка обновлений в хранилище**.

6. В поле **Результат выполнения** выберите значение **Завершена успешно**.

7. Нажмите на кнопку **ОК**.

Передача данных сервису KSN

Kaspersky Security Network (KSN) – это инфраструктура онлайн-служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции программ "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

Для работы программы в сертифицированной конфигурации службы, которые связаны с отправкой данных на внешние сервера и получением команд от внешних серверов (за периметром сети организации), должны быть отключены. Отключите передачу данных программой сервису KSN.

► *Чтобы отключить передачу данных сервису KSN, выполните следующие действия:*

1. В дереве консоли выберите Сервер администрирования, для которого нужно отключить передачу данных к сервису KSN.

2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.

3. В окне свойств Сервера администрирования в разделе **Прокси-сервер KSN** выберите раздел **Параметры прокси-сервера KSN**.

4. Снимите флажок **Я принимаю условия использования Kaspersky Security Network**, чтобы выключить автоматическую передачу данных "Лаборатории Касперского" о работе установленных на устройствах программ "Лаборатории Касперского".

5. При необходимости снимите флажок **Использовать Сервер администрирования как прокси-сервер**, чтобы выключить службу прокси-сервера KSN.

6. Нажмите на кнопку **ОК**.

Если флажок снят, передача данных в KSN от Сервера администрирования и от клиентских устройств через Kaspersky Security Center не осуществляется. При этом клиентские устройства в соответствии со своими параметрами могут передавать данные в KSN напрямую (не через Kaspersky Security Center). Действующая на клиентских устройствах политика Kaspersky Endpoint Security для Windows определяет, какие данные эти устройства напрямую (не через Kaspersky Security Center) передают в KSN.

Передача данных сервису KSN должна быть отключена во всех управляемых программах.

Альтернативой отказу от использования KSN может стать использование Локального KSN. В этом случае вы получите доступ к оперативной базе знаний "Лаборатории Касперского", но информация о работе программ "Лаборатории Касперского" не будет передаваться на

сервера "Лаборатории Касперского". Подробнее см. в Руководстве по эксплуатации, в разделе " Настройка доступа к KSN".

Источник обновлений задачи Загрузка обновлений в хранилище

Отключите передачу данных программой сервису обновлений "Лаборатории Касперского". Для этого необходимо удалить серверы обновлений "Лаборатории Касперского" в задачи Загрузка обновлений в хранилище из источников обновлений.

► *Чтобы удалить серверы обновлений "Лаборатории Касперского" в задаче Загрузка обновлений в хранилище из источников обновлений, выполните следующие действия:*

1. В дереве консоли перейдите в папку **Задачи**.
2. В контекстном меню задачи **Загрузка обновлений в хранилище** выберите пункт **Свойства**.
3. В окне свойств задачи перейдите в раздел **Параметры**.
4. В подразделе **Источники обновлений** перейдите по ссылке **Настроить**.
5. В окне **Источники обновлений** удалите значение *Серверы обновлений "Лаборатории Касперского"*.

Настройку необходимо выполнить для задачи **Загрузка обновлений в хранилище** Сервера администрирования и для всех агентов обновлений.

Сервер администрирования необходимо активировать при помощи файлов ключа, так как при активации программы с помощью кода активации программа регулярно отправляет запросы на серверы активации «Лаборатории Касперского» для проверки текущего статуса ключа.

Способ активации Сервера администрирования

Сервер администрирования необходимо активировать с помощью файла ключа.

► *Чтобы активировать Сервер администрирования с помощью файла ключа, выполните следующие действия:*

1. В дереве консоли выберите Сервер администрирования, который вы хотите активировать.
2. В контекстном меню Сервера администрирования выберите пункт **Все задачи** → **Мастер первоначальной настройки**.
3. В окне мастера **Выбор способа активации программы** нажмите на кнопку **Активировать программу с помощью файла ключа**.
4. В окне мастера **Активация программы** укажите файл ключа, на основании которого ключ будет добавлен в программу.

Служба прокси-сервера активации "Лаборатории Касперского"

Рекомендуется отключить службу прокси-сервера активации "Лаборатории Касперского".

► *Чтобы отключить службу прокси-сервера активации "Лаборатории Касперского", выполните следующие действия:*

1. Откройте список служб вашего устройства.
2. Выберите в списке службу прокси-сервера активации "Лаборатории Касперского".
3. В контекстном меню службы выберите раздел **Свойства**.
4. В окне свойства службы на закладке **Общие** в поле Т**ип запуска** выберите значение **Отключена**.
5. Нажмите на кнопку **Остановить**.
6. Нажмите на кнопку **ОК**.

Доверенные каналы с использованием SSL-протокола

Настройте использование SSL-соединений для гарантированной доставки информации по доверенному каналу. В сертифицированной конфигурации программа должна использовать только доверенные каналы. Для этого на устройстве с установленным Сервером администрирования необходимо закрыть не использующие SSL-протоколы порты, по которым происходит соединение с Сервером администрирования извне. По умолчанию

используется порт 14000. В политике Агента администрирования необходимо настроить использование SSL-соединения.

► *Чтобы настроить использование SSL-соединения в политике Агента администрирования, выполните следующие действия:*

1. В дереве консоли перейдите в папку **Политики**.
2. В папке **Политики** выберите политику Агента администрирования.
3. В контекстном меню политики Агента администрирования выберите пункт **Свойства**.
4. В окне свойств Агента администрирования свойств в разделе **Сеть** выберите вложенный раздел **Сеть**.
5. Установите флажок **Использовать SSL-соединение**.
6. Нажмите на кнопку **ОК**.

   Если флажок установлен, подключение Агента администрирования к Серверу администрирования будет выполняться через защищенный порт с использованием SSL-протокола.
7. В разделе **Подключения** выберите профиль подключения и нажмите на кнопку Свойства.
8. В окне свойств профиля подключения установите флажок **Использовать SSL-соединение**.

   Флажок **Использовать SSL-соединение** необходимо установить для всех профилей подключений.
9. Нажмите на кнопку **ОК**.

Права пользователей

Внутренним пользователям Kaspersky Security Center должны быть назначены минимально необходимые права для выполнения их функций в программе. Для этого вы можете назначить пользователю или группе пользователей роль с набором прав на работу с Сервером администрирования.

► *Чтобы назначить роль пользователю или группе пользователей, выполните следующие действия:*

1. В дереве консоли выберите узел с именем необходимого Сервера администрирования.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования выберите раздел **Безопасность**.
4. В поле **Имена групп или пользователей** выберите пользователя или группу пользователей, которым нужно присвоить роль.

   Если пользователь или группа отсутствуют в поле, добавьте их по кнопке **Добавить**.

   При добавлении пользователя по кнопке **Добавить** можно выбрать тип аутентификации пользователя (Microsoft Windows или Kaspersky Security Center). Аутентификация Kaspersky Security Center используется для выбора учетных записей внутренних пользователей, которые используются для работы с виртуальными Серверами администрирования.
5. Перейдите на закладку **Роли** и нажмите на кнопку **Добавить**.

   Откроется окно **Роли пользователей**. В окне отображаются созданные роли пользователей.
6. В окне **Роли пользователей** выберите роль для группы пользователей.
7. Нажмите на кнопку **ОК**.

В результате роль с набором прав на работу с Сервером администрирования будет назначена пользователю или группе пользователей. Назначенные роли отображаются на закладке **Роли** в разделе **Безопасность** окна свойств Сервера администрирования

Условия для статуса "Критический"

Настройте изменение статуса устройства на *Критический* при обнаружении на нем хотя бы одного вируса.

► *Чтобы настроить изменение статуса устройства на* Критический, *выполните следующие действия:*

1. Откройте окно свойств одним из следующих способов:

   - В папке **Политики** в контекстном меню политики Сервера администрирования выберите пункт **Свойства**.

   - В контекстном меню группы администрирования выберите пункт **Свойства**.

2. В окне свойств перейдите в раздел **Статус устройства**.

3. В блоке **Условия для статуса Критический** установите флажок для условия **Найдено много вирусов**.

4. Для условия **Найдено много вирусов** установите значение *Более чем 0*.

5. Нажмите на кнопку **ОК**.

Максимальное количество событий, хранящихся в базе данных Сервера администрирования

Установите максимальное количество событий, хранящихся в базе данных Сервера администрирования, необходимое для проведения аудита программы. Рекомендуется хранить не менее 400 000 событий в базе данных Сервера администрирования.

► *Чтобы изменить максимальное количество событий, хранящихся в базе данных Сервера администрирования, выполните следующие действия:*

1. В дереве консоли выберите Сервер администрирования, для которого нужно настроить максимальное количество событий, хранящихся на Сервере.

2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.

3. В окне свойств Сервера администрирования перейдите в раздел **Хранение событий**.

4. В поле **Максимальное количество событий, хранящихся в базе данных** установите рекомендуемое значение, не меньше 400 000 событий.

По умолчанию емкость базы данных Сервера администрирования составляет 400.000 событий. Максимальная рекомендованная емкость базы данных – 15 000 000 событий. Если

количество событий в базе данных достигает указанного администратором максимального значения, программа удаляет самые старые события и записывает новые.

Срок хранения событий

Настройте срок хранения событий в базе данных Сервера администрирования, необходимый для проведения аудита программы.

► *Чтобы изменить срок хранения событий, выполните следующие действия:*

1. В дереве консоли выберите Сервер администрирования, для которого нужно настроить срок хранения изменений объектов.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования перейдите в раздел **Настройка событий**.
4. Установите время хранения событий по уровню их важности:
   - На закладке **Критическое событие** установите необходимое значение (не меньше 180 дней).
   - На закладке **Предупреждение** установите необходимое значение (не меньше 90 дней).
   - На закладке **Информационное сообщение** установите необходимое значение (не меньше 30 дней).
5. Нажмите на кнопку **ОК**.

Срок хранения событий можно настроить также в свойствах политики Сервера администрирования.

► *Чтобы настроить срок хранения событий в свойствах политики Сервера администрирования, выполните следующие действия:*

1. В дереве консоли выберите папку **Политики**.
2. В контекстном меню политики Сервера администрирования выберите пункт **Свойства**.

3. В окне свойств политики Сервера администрирования перейдите в раздел **Настройка событий**.

4. Установите время хранения событий, в зависимости от уровня важности событий:

   - На закладке **Критическое событие** установите значение не меньше 180 дней.
   - На закладке **Предупреждение** установите значение не меньше 90 дней.
   - На закладке **Информационное сообщение** установите значение не меньше 30 дней.

5. Нажмите на кнопку **ОК**.

Срок хранения ревизии изменений объектов

Настройте срок хранения ревизии объектов, необходимый для проведения аудита программы. Рекомендуемый срок хранения ревизии изменения объектов 90 дней. Такой срок достаточен для проведения регулярного аудита программы.

► *Чтобы изменить срок хранения ревизии изменения объектов, выполните следующие действия:*

1. В дереве консоли выберите Сервер администрирования, для которого необходимо настроить срок хранения изменений объектов.

2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.

3. В окне свойств Сервера администрирования перейдите в раздел **Хранение истории изменений**.

4. В поле **Срок хранения ревизии изменения объекта** установите значение не меньше 90.

5. Нажмите на кнопку **ОК**.

Способы получения технической поддержки

Если вы не нашли решения вашей проблемы в документации или других источниках информации о программе, рекомендуется обратиться в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании программы.

Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки (https://support.kaspersky.ru/support/rules#ru_ru).

Вы можете связаться со специалистами Службы технической поддержки одним из следующих способов:

- позвонить в Службу технической поддержки по телефону (https://support.kaspersky.ru/b2b) ;
- отправить запрос в Службу технической поддержки "Лаборатории Касперского" с портала Kaspersky CompanyAccount (https://companyaccount.kaspersky.com).

Техническая поддержка по телефону

В большинстве регионов по всему миру вы можете позвонить специалистам Службы технической поддержки. Вы можете найти информацию о способах получения технической поддержки в вашем регионе и контакты Службы технической поддержки на веб-сайте Службы технической поддержки "Лаборатории Касперского" (https://support.kaspersky.ru/b2b).

> Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки (https://support.kaspersky.ru/support/rules#ru_ru).

Техническая поддержка через Kaspersky CompanyAccount

Kaspersky CompanyAccount (https://companyaccount.kaspersky.com) – это портал для организаций, использующих программы "Лаборатории Касперского". Портал Kaspersky CompanyAccount предназначен для взаимодействия пользователей со специалистами "Лаборатории Касперского" с помощью электронных запросов. На портале Kaspersky CompanyAccount можно отслеживать статус обработки электронных запросов специалистами "Лаборатории Касперского" и хранить историю электронных запросов.

Вы можете зарегистрировать всех сотрудников вашей организации в рамках одной учетной записи Kaspersky CompanyAccount. Одна учетная запись позволяет вам централизованно управлять электронными запросами от зарегистрированных сотрудников в "Лабораторию Касперского", а также управлять правами этих сотрудников в Kaspersky CompanyAccount.

Портал Kaspersky CompanyAccount доступен на следующих языках:

- английском;
- испанском;
- итальянском;
- немецком;
- польском;
- португальском;
- русском;
- французском;
- японском.

Вы можете узнать больше о Kaspersky CompanyAccount на веб-сайте Службы технической поддержки (https://support.kaspersky.ru/faq/companyaccount_help).

АО "Лаборатория Касперского"

"Лаборатория Касперского" – известный в мире производитель систем компьютерной защиты от различных видов угроз, включая защиту от вирусов и других вредоносных программ, нежелательной почты (спама), сетевых и хакерских атак.

В 2008 году "Лаборатория Касперского" вошла в четверку мировых лидеров рынка программных решений для обеспечения информационной безопасности конечных пользователей (рейтинг "IDC Worldwide Endpoint Security Revenue by Vendor"). В России, по данным IDC, "Лаборатория Касперского" – самый предпочитаемый производитель систем компьютерной защиты для домашних пользователей ("IDC Endpoint Tracker 2014").

"Лаборатория Касперского" основана в России в 1997 году. Сегодня "Лаборатория Касперского" – это международная группа компаний с 38 офисами в 33 странах мира. В компании работает более 3000 квалифицированных специалистов.

Продукты. Продукты "Лаборатории Касперского" защищают как домашние компьютеры, так и компьютерные сети организаций.

Линейка персональных продуктов включает программы, обеспечивающие информационную безопасность настольных компьютеров и ноутбуков, планшетных компьютеров, смартфонов и других мобильных устройств.

Компания предлагает решения и технологии для защиты и контроля рабочих станций и мобильных устройств, виртуальных машин, файловых и веб-серверов, почтовых шлюзов, сетевых экранов. Также в портфеле компании есть специализированные продукты для защиты от DDoS-атак, защиты сред под управлением АСУТП и предотвращения финансового мошенничества. Использование этих решений в сочетании с централизованными средствами управления позволяет построить и эксплуатировать эффективную автоматизированную защиту организации любого размера от компьютерных угроз. Продукты "Лаборатории Касперского" сертифицированы крупными тестовыми лабораториями, совместимы с программным обеспечением многих поставщиков программного обеспечения и оптимизированы для работы на многих аппаратных платформах.

Вирусные аналитики "Лаборатории Касперского" работают круглосуточно. Каждый день они находят сотни тысяч новых компьютерных угроз, создают средства их обнаружения и лечения и включают сигнатуры этих угроз в базы, используемые программами "Лаборатории Касперского".

Технологии. Многие технологии, без которых трудно представить себе современный антивирус, впервые разработаны именно "Лабораторией Касперского". Не случайно программное ядро Антивируса Касперского используют в своих продуктах многие другие разработчики программного обеспечения, среди них: Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, Facebook, General Dynamics, H3C, Juniper Networks, Lenovo, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu, ZyXEL. Многие из инновационных технологий компании подтверждены патентами.

Достижения. За годы борьбы с компьютерными угрозами "Лаборатория Касперского" завоевала сотни наград. Например, в 2014 году по итогам испытаний и исследований, проведенных авторитетной австрийской антивирусной лабораторией AV-Comparatives, "Лаборатория Касперского" стала одним из двух лидеров по количеству полученных сертификатов Advanced+, в результате компания была удостоена сертификата Top Rated. Но главная награда "Лаборатории Касперского" – это приверженность пользователей по всему миру. Продукты и технологии компании защищают более 400 миллионов пользователей. Количество организаций, являющихся ее клиентами, превышает 270 тысяч.

Сайт "Лаборатории Касперского":	https://www.kaspersky.ru
Вирусная энциклопедия:	https://securelist.ru/
Вирусная лаборатория:	https://virusdesk.kaspersky.ru/ (для проверки подозрительных файлов и сайтов)
Веб-форум "Лаборатории Касперского":	https://forum.kaspersky.com

Информация о стороннем коде

Информация о стороннем коде содержится в файле legal_notices.txt, расположенном в папке установки программы.

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Active Directory, ActiveSync, Edge, Internet Explorer, Hyper-V, Microsoft, MultiPoint, SharePoint, SQL Server, Windows, Windows Server, Windows Phone, Windows Vista – товарные знаки Microsoft Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

Android, Chrome, Google Play – товарные знаки Google, Inc.

Apache и Apache feather logo – товарные знаки Apache Software Foundation.

Apple, App Store, Leopard, Mac, Mac OS, macOS, Safari, Snow Leopard, OS X, Tiger – товарные знаки Apple Inc., зарегистрированные в США и других странах.

Cisco – зарегистрированный в Соединенных Штатах Америки и в других странах товарный знак Cisco Systems, Inc. и / или ее аффилированных компаний.

Citrix, XenServer – товарные знаки Citrix Systems, Inc. и / или дочерних компаний, зарегистрированные в патентном офисе США и других стран.

Debian – зарегистрированный товарный знак Software in the Public Interest, Inc.

Intel, Core, Xeon – товарные знаки Intel Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

CentOS, Fedora, Red Hat Enterprise Linux – товарные знаки Red Hat Inc., зарегистрированные в Соединенных Штатах Америки и в других странах.

Firefox – товарный знак Mozilla Foundation.

Знак FreeBSD является зарегистрированным товарным знаком фонда FreeBSD.

Oracle и Java – зарегистрированные товарные знаки Oracle Corporation и / или ее аффилированных компаний.

Linux – товарный знак Linus Torvalds, зарегистрированный в США и в других странах.

Novell, Netware – товарные знаки Novell Inc., зарегистрированные в Соединенных Штатах Америки и в других странах.

SUSE – зарегистрированный в США и других странах товарный знак SUSE LLC.

Ubuntu – зарегистрированный товарный знак Canonical Ltd.

UNIX – товарный знак, зарегистрированный в США и других странах, использование лицензировано X/Open Company Limited.

VMware – товарный знак VMware, Inc. или зарегистрированный в США или других юрисдикциях товарный знак VMware, Inc.

Владельцем товарного знака Symbian является Symbian Foundation Ltd.

Товарный знак BlackBerry принадлежит Research In Motion Limited, зарегистрирован в США и может быть подан на регистрацию или зарегистрирован в других странах.

Соответствие терминов

В этом разделе приведено соответствие терминов, используемых в документации, и терминов, используемых в требованиях ФСТЭК.

Таблица 63. Соответствие терминов

Термин в документации	Термин в требованиях ФСТЭК
программа	продукт, объект оценки, программное изделие
виртуальная инфраструктура VMware	среда функционирования
файл виртуальной машины	объект воздействия
вирус, программа, представляющая угрозу, вредоносная программа	КВ, компьютерный вирус
антивирусные базы, базы программы	базы данных признаков компьютерных вирусов (БД ПКВ)
антивирусная проверка	поиск вирусов
события	данные аудита
администратор	администратор безопасности, уполномоченный субъект информационной системы, уполномоченный пользователь