



**Kaspersky Security Center 10 SP1
Full Disk Encryption Quick Start Installation Guide**

1 Prerequisites



Heads up! The prerequisites listed here, as well as the rest of the information in this documentation are **specifically** for Kaspersky Lab Endpoint Security SP1.

While this information may be relevant for future versions of this software, please ensure you are actively reviewing the correct documentation and prerequisites as they are subject to change.

- A fully installed Kaspersky Security Center server
- The proper licensing key for Encryption
- A Windows workstation that meets the systems requirements found on this support page:
support.kaspersky.com/kes10wks#requirements

2 Required Downloads

All necessary files are built into the (Full) Kaspersky Security Center 10 SP1 installation package, which is a requirement of this process.

The download page for this software can be found here: support.kaspersky.com/ksc10#downloads

3 Understanding the Technology

There are five main components in play when the Full Disk Encryption feature set of the Kaspersky Endpoint Security software is fully implemented.

The **Kaspersky Security Center 10 SP1 (KSC)** software is first, and it is entirely responsible for the policies that dictate how the workstation's endpoint security software will behave. It is also where a second copy of the symmetric encryption key is held for administrative purposes. Should an end user forget their credentials, the administrator of the Kaspersky Security Center has the ability to issue new credentials, add new users to the PreBoot agent and perform any other administrative duties.

The second component is the **Kaspersky Endpoint Security SP1 (KES)** software which resides on the workstations themselves.

The third component is the **Network Agent** which provides communication between the endpoint workstation and the Kaspersky Security Center.

The fourth component is the **AES Encryption Module**, which is installed in tandem with the Kaspersky Endpoint Security software and handles the encryption aspect behind the scenes. This encryption is further enhanced by the AES-NI processor instruction set standardized on all modern (post 2008) processor chipsets.

Lastly, the fifth component is the **Kaspersky PreBoot Agent** which is the gateway application that lies between the initial startup of the machine and the Windows environment. Without the proper credentials to get past this startup screen, the end user will not be able to gain access to any encrypted files on the workstation.

The Kaspersky Security Center must first be installed.

From here, the Kaspersky Endpoint Security (with the AES Module in place) and Network Agent software are both deployed and the Kaspersky Security Center policy for the workstation in question will be modified to enable Full Disk Encryption (FDE).

Behind the scenes, once the workstation receives the policy it will generate a 256 bit symmetric encryption key using the AES module and send that data to the Kaspersky Security Center for safe keeping. The workstation will then request a restart to test the workstation to ensure the PreBoot software will work properly given the hardware of the machine.



Once restarted, the machine will return to the Windows environment.

If the Kaspersky Security Center has properly received the encryption key from the workstation, it will relay this message to the workstation and the end user will be prompted to enter their current user credentials they are using to gain access to the desktop.

This is designed so that the passwords for both Windows authentication and the PreBoot software both match, preventing the end user from having to memorize a separate password for both components.

At this point, the encryption process will begin running in the background and upon the next reboot, the end user will be automatically pushed into the PreBoot authentication screen and prompted for authentication credentials.

4 Preparing the software for deployment



Please ensure that the Advanced licensing key has been added to the Kaspersky Security Center. Encryption is **not** supported in the base level “Select” licensing tier.

Open the Kaspersky Security Center Console and navigate to the **Installation packages** node located under **Remote installation**.

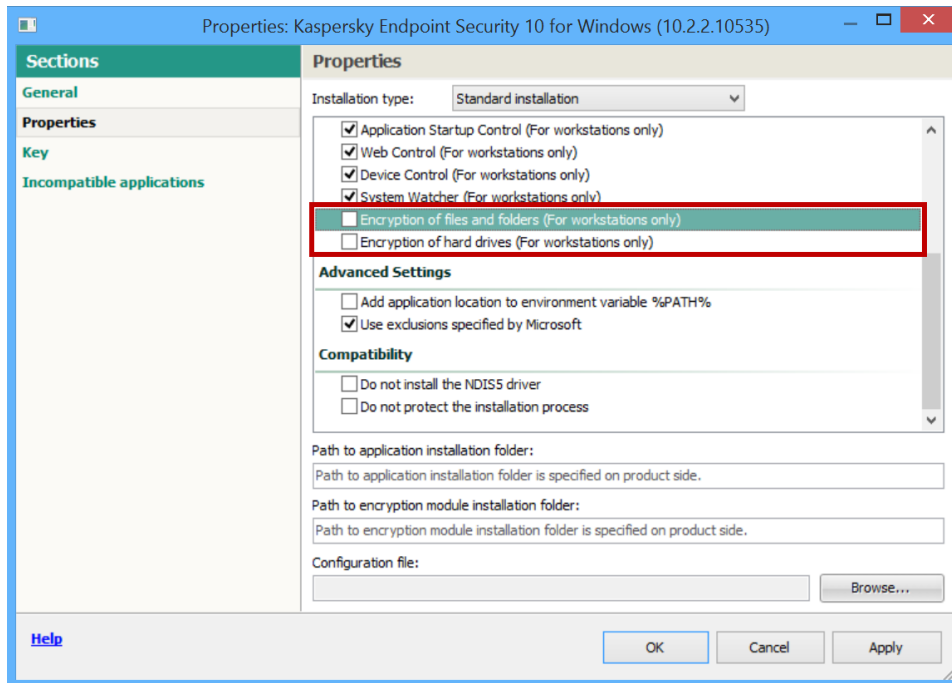
Right click on **Kaspersky Endpoint Security 10 for Windows** and click on **Properties**

Installation packages
Installation packages are used for remote deployment.

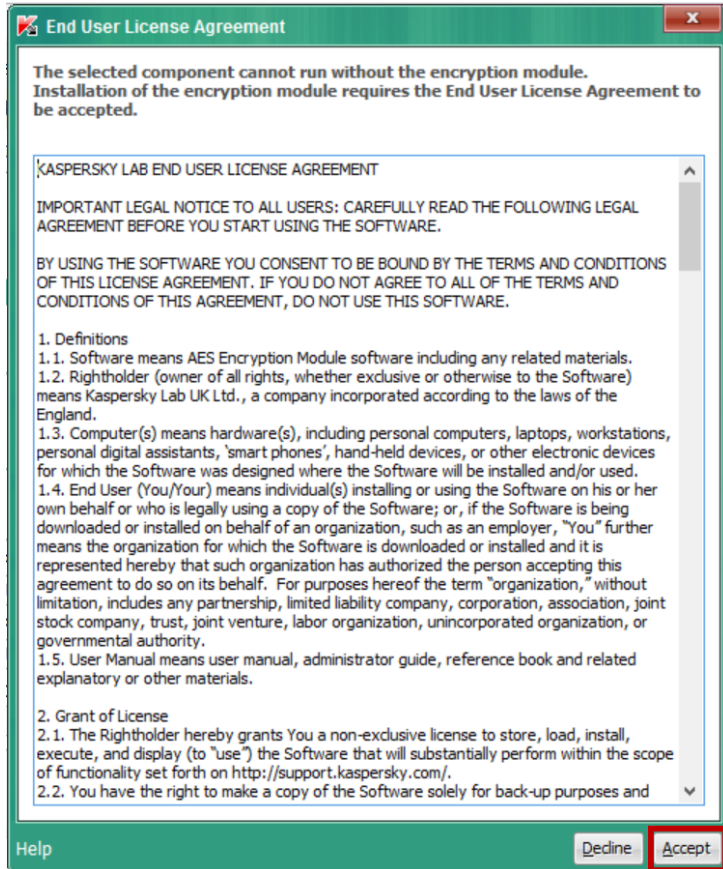
- Create installation package**
You have the option of creating installation packages for remote installation of Kaspersky Lab products, third-party systems from images. You can create packages for deploying operating systems from images by making OS images.
- Manage packages of mobile applications**
Mobile applications packages are intended for installation on mobile devices not using Kaspersky Security Center. Mobile applications packages can be uploaded to the Web server for further downloading and installation.
- View the list of stand-alone packages**
Stand-alone installation packages are intended for installation not using Kaspersky Security Center. For example, the Web server for further downloading and installation. Stand-alone packages are created based on an existing application.
- View current version of Kaspersky Lab applications**
 - View report on versions of installed applications
 - Add/Remove columns
 - Refresh

Name	Application
Exchange ActiveSync Mobile Device Server (10.2.434)	Managing mobile devices via Exchange ser...
iOS MDM Mobile Device Server (10.2.434)	Management of iOS-based mobile devices
Kaspersky Endpoint Security 10 for Windows (10.2.2.10...)	Kaspersky Endpoint Security 10 Service Pac...
Kaspersky Security 10 for Mobile (10.0)	Kaspersky Endpoint Security 10 Service Pac...
Kaspersky Security Center Network Agent (10.2.434)	Kaspersky Security Center Network Agent

In the window that appears, click on the **Properties** link on the left hand side.
Scroll to the bottom and check on **Encryption of hard drives (For workstations online)**



A window warning you of an agreement will pop up. Accept to close the window.
Click **OK** to exit the window.



5 Deploying the KES software to the workstation

Create tasks to install the Network Agent and Kaspersky Endpoint Security software

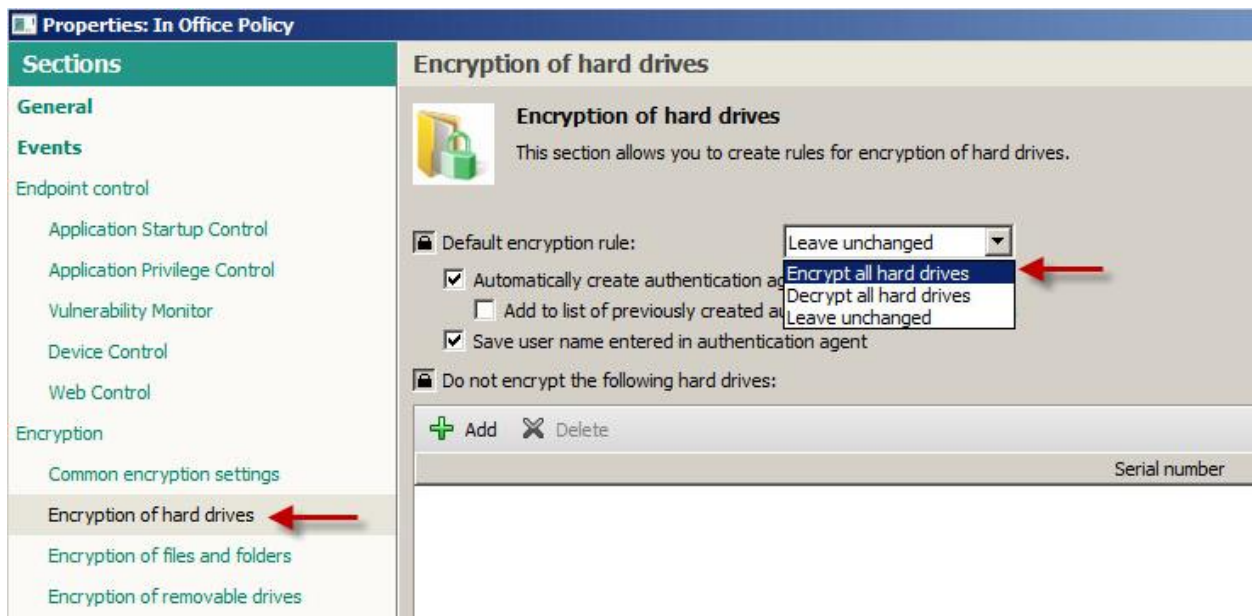
6 Enforcing the Encryption policy

Navigate to the policy that governs the computer in question.

Navigate to the **Encryption of hard drives** node in the left hand navigation pane.

In the dropdown box for the Default encryption rule, modify this from **Leave unchanged** to **Encrypt all hard drives**.

Click **OK** to set the policy.

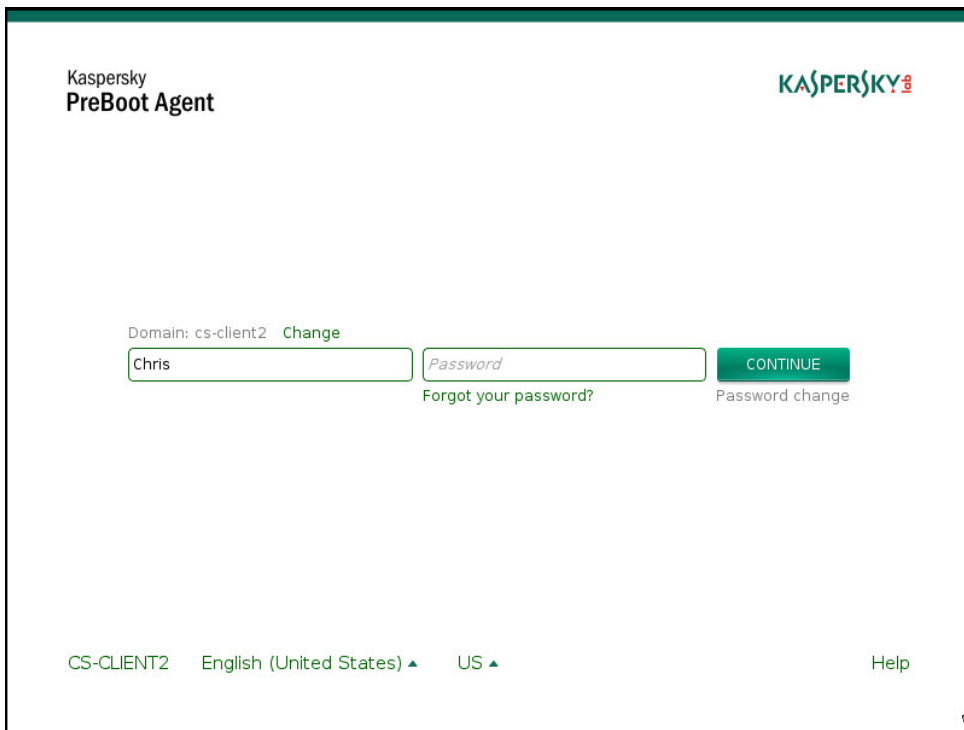


7 Working on the Endpoint

Restart the endpoint machine. The first restart should prompt the preboot agent to check the hardware of the device to ensure compatibility.

Once you return back to the desktop, you should be prompted to enter a username and password for passing through the Kaspersky PreBoot authentication area.

Restart once more to ensure that the PreBoot Agent begins as it should.



The screenshot shows the Kaspersky PreBoot Agent authentication interface. At the top left, it says "Kaspersky PreBoot Agent" and at the top right is the "KASPERSKY Lab" logo. Below the logo, the domain is set to "cs-client2" with a "Change" link. There are two input fields: one for the username containing "Chris" and one for the password containing "Password". To the right of the password field is a green "CONTINUE" button. Below the password field, there is a link for "Forgot your password?" and a link for "Password change". At the bottom left, the system information shows "CS-CLIENT2", "English (United States)", and "US". At the bottom right, there is a "Help" link. A small cursor icon is visible in the bottom right corner of the window.