SOPHOS

Security made simple.

Sophos Disk Encryption

License migration guide

Product version: 5.61

Document date: March 2015

Contents

1 About this guide

This guide describes migration scenarios that involve a change in your Sophos Enterprise Console or Sophos encryption software license. It covers migration of server-side software as well as endpoint software.

Important: Please note that Sophos Disk Encryption 5.61 managed by Sophos Enterprise Console will retire at the end of March 2016. This product is no longer available to purchase. For information about SafeGuard encryption product retirements, see knowledgebase article 119020 (http://www.sophos.com/en-us/support/knowledgebase/119020.aspx).

The guide assumes that you are familiar with Sophos Enterprise Console (SEC), Sophos SafeGuard Disk Encryption/Sophos SafeGuard Easy and SafeGuard Enterprise.

The following migration scenarios are described:

- Migrate from Sophos Disk Encryption 5.61 (Sophos Enterprise Console 5.1 or later with managed encryption) to SafeGuard Enterprise managed encryption.
- Add encryption to an existing Sophos security solution.
- Migrate from Sophos unmanaged encryption (SDE 4.6x / SGE 4.5x) to Sophos Disk Encryption 5.61.
- Migrate from Sophos unmanaged encryption (SDE 5.5x or 5.6x / SGE 5.5x or 5.6x) to Sophos Disk Encryption 5.61.

Migration scenarios that are not covered in this guide

The following migration scenarios are not covered:

- Migrate endpoints from SafeGuard Enterprise 6 or later /SafeGuard Easy 6 or later to Sophos Disk Encryption 5.61 to be managed by SEC. In this case you have to decrypt the endpoint and uninstall the encryption agent software. Then you have to install Sophos Disk Encryption 5.61 on the endpoint that is to be managed by SEC.
- Migrate from SafeGuard Enterprise to Sophos Disk Encryption 5.61 managed by SEC.

  Note: Provided that you do not want to use Enterprise Console to manage Sophos Disk Encryption 5.61, you can install Enterprise Console on the same server as SafeGuard Enterprise. Some specific configuration is required to set this up. For further information, see http://www.sophos.com/en-us/support/knowledgebase/117632.aspx.
- Migrate from managed encryption to unmanaged encryption. In this case you have to decrypt and then re-encrypt the endpoint computers.

Product names used in this guide

Product name	Description
Sophos Enterprise Console	Sophos console that manages and updates Sophos security software. Starting with version 5.1, it also manages encryption.
Sophos Disk Encryption 5.61	Sophos Enterprise Console managed encryption software.
Full Disk Encryption	Name of encryption feature in Sophos Enterprise Console. A feature that protects hard drives on endpoint computers from being read or changed by unauthorized persons.
Sophos SafeGuard Disk Encryption (SDE)	SafeGuard standalone encryption software available with the Endpoint Security and Data Protection (ESDP) bundle. From version 5.50, SafeGuard Policy Editor is used to configure policies for standalone computers.
Sophos SafeGuard Easy (SGE)	SafeGuard encryption software. From version 5.50, Sophos SafeGuard Easy is the product name for the SafeGuard Enterprise standalone encryption solution. From version 5.50, SafeGuard Policy Editor is used to configure policies for standalone computers.
SafeGuard Enterprise	Comprehensive, modular SafeGuard encryption suite with central, role-based management that protects data on endpoint computers from being read or changed by unauthorized persons.

Sophos documentation

Sophos documentation is published at http://www.sophos.com/en-us/support/documentation.

2 Sophos Disk Encryption 5.61 to SafeGuard Enterprise

Migration from Sophos Disk Encryption 5.61 to SafeGuard Enterprise involves the following steps:

- Export the SEC company certificate: In Enterprise Console on the **Tools** menu, click **Manage Encryption** and select **Backup Company Certificate**. Select a destination directory and file name and enter a password for the .P12 file when prompted.
- Install SafeGuard Management Center and SafeGuard Enterprise Server.

  Note: If you have the SEC management server with encryption installed on this server, install SafeGuard Enterprise on a different server.
- In the SafeGuard Management Center configuration wizard, select a new database to be created and import the company certificate exported before.
- In SafeGuard Management Center, create the endpoint configuration package: On the **Tools** menu, click **Configuration Packages Tool**. Select **Managed client packages**, make your edits and create the configuration package.
- Deploy the configuration package to the endpoints. After the endpoints have received it, they are able to connect to SafeGuard Enterprise Server. From that time on, the endpoint can be managed by SafeGuard Management Center.
- In SafeGuard Management Center, create and assign policies as desired.

The migrated endpoints remain visible in Enterprise Console as "managed by SafeGuard Enterprise". All non-encryption related tasks can still be performed on them.

For detailed information on SafeGuard Enterprise installation, see the *SafeGuard Enterprise installation guide*.

3 Add encryption to an existing Sophos security solution

To add encryption to an existing Sophos security solution you need to upgrade Sophos Enterprise Console to include encryption and do a first-time installation of the encryption agent software on your endpoint computers.

Note: Encryption is only available if you have a valid license that includes it.

To add encryption to an existing Sophos security solution you do the following:

- If you have a previous version of Enterprise Console installed, upgrade to the latest version including encryption.

  If you already have the latest version of Enterprise Console installed without encryption, re-install it to add encryption.

- Set up the encryption agent software on endpoint computers.

3.1 Upgrade Sophos Enterprise Console

If you have Sophos Enterprise Console below 5.1 installed on your computer, upgrade to the latest version of Sophos Enterprise Console including encryption.

To do so, run the latest Enterprise Console installer and follow the instructions. For more information, see the *Sophos Enterprise Console upgrade guide*.

Note: In the installer wizard make sure that you select to manage encryption with Enterprise Console.

Sophos Enterprise Console is upgraded, the full disk encryption feature is available.

3.2 Add encryption to Sophos Enterprise Console

If you have Sophos Enterprise Console 5.1 or later without encryption installed on your computer, re-install it to add encryption.

Note: If you are not using the latest version of Enterprise Console, we recommend upgrading to the latest version first.

1. At the computer where you want to install Enterprise Console, log on as an administrator:
   - If the server is in a domain, use a domain account that has local administrator rights.
   - If the server is in a workgroup, use a local account that has local administrator rights.
2. Find the Enterprise Console installer that you downloaded earlier.
3. Double-click the installer.

4. When you are prompted, click **Modify**.

   The installation files are copied to the computer and a wizard starts.

5. The wizard guides you through installation. You should do as follows:

   a) Accept the defaults wherever possible.

   b) On the **Components Selection** page, ensure that all the components are selected.

   c) On the **Database details** page, enter details of an account that can access the computer where you are installing Enterprise Console. This should not be an administrator account.

   d) On the **Manage Encryption** page, click **Manage Encryption**.

   e) On the **Sophos Encryption** page, click **New installations**. You are prompted for the password for the certificates backup store. Make a note of the password.

6. When installation is complete, you may be prompted to restart. Click **Yes** or **Finish**.

3.3 Set up encryption software on computers

Note: Sophos Disk Encryption can be installed on Windows XP, Windows Vista and Windows 7 computers but not on Macs.

To set up Sophos Disk Encryption on computers you:

- Give administrator access to computers after installation
- Prepare to install encryption software.
- Install encryption software automatically.
- Install encryption software manually.

3.3.1 Give administrators access to computers after installation

Administrators might need to access and pre-configure computers after you have installed encryption software, for example to install other software. However, the first user who logs on after installation activates Power-on Authentication. To avoid this, add the respective administrators to a list of exceptions, as follows:

1. In Enterprise Console, in the **Policies** pane, double-click **Full disk encryption**. Double-click the **Default** policy to edit it.
2. Under **Power-on Authentication (POA)** click **Exceptions** next to **Enable Power-on Authentication**.
3. In **Exceptions**, click **Add**, enter the **User name** and the **Computer or domain name** of the relevant Windows account(s) and click **OK.**

   You can use wildcards as the first or last character. In the **User name** field, the ? character is not allowed. In the **Computer or Domain Name** field, the characters / \ [ ] : ; | = , + ? < > " are not allowed.

4. In the **Default** policy dialog, click **OK**.
5. In the **Policies** pane, select the policy and drag it onto the group to which you want to apply the policy. When prompted, confirm that you want to continue.

3.3.2 Prepare computers for installation

If your license includes full disk encryption, you must do the following before you install encryption software on computers:

- Make sure that the computer has already been protected with Sophos anti-virus software version 10 before you deploy full disk encryption.
- Make sure that third-party encryption software has been decrypted and uninstalled before you deploy full disk encryption.
- Check if a user account is set up and active. The user needs to have a password.
- Drives to be encrypted must be completely formatted and have a drive letter assigned to them.
- Uninstall third-party boot managers, such as PROnetworks Boot Pro and Boot-US.
- Create a full backup of the data.
- Check the hard disk(s) for errors with this command:

  ```
  chkdsk %drive% /F /V /X
  ```

  You might be prompted to restart the computer and run **chkdsk** again. For further information, see: www.sophos.com/en-us/support/knowledgebase/107081.aspx.

  You can check the results (log file) in the Windows Event Viewer:

  Windows XP: Select **Application**, **Winlogon**.
  Windows 7, Windows Vista: Select **Windows Logs**, **Application**, **Wininit**.

- Use the Windows built-in **defrag** tool to locate and consolidate fragmented boot files, data files, and folders on local drives:

  ```
  defrag %drive%
  ```

  For further information, see: www.sophos.com/en-us/support/knowledgebase/109226.aspx.

- If you have used an imaging/cloning tool on the computer, clean the master boot record (MBR). Start the computer from a Windows DVD and use the command **FIXMBR** within the Windows Recovery Console. For further information, see: www.sophos.com/en-us/support/knowledgebase/108088.aspx.
- If the boot partition on the computer has been converted from FAT to NTFS, and the computer has not been restarted since then, restart the computer. If you do not do this, the installation may not complete successfully.

3.3.3 Install encryption software automatically

Make sure that the endpoints have been prepared for full disk encryption installation, in particular that the Sophos anti-virus software version 10 has been installed and that third-party encryption software has been uninstalled. For further information, see Prepare computers for installation (page 8).

To install encryption software automatically:

1. In Enterprise Console, select the computers on which you want to install full disk encryption.
2. Right-click the computers, and then click **Protect computers**. The **Protect Computers Wizard** is launched.
3. On the **Welcome** page, click **Next**.
4. On the **Installation Type** page, select **Encryption software**.
5. If there is more than one encryption subscription and installer location (bootstrap location) available, the **Encryption location** page is displayed. Select the **Encryption subscription** and **Address** to install from.
6. On the **Encryption summary** page, check for any installation problems.
7. On the **Credentials** page, enter details of an account that can be used to install software on computers.

Installation is staggered, so the process may not be complete on all the computers for some time.

The installation of encryption will cause computers to restart automatically within about 30 minutes after installation of the encryption software. If encryption is enabled by policy, it will only take place after the computer's restart.

For further information on the start behaviour of the computer and first logon after installation and activation of encryption, see the *Sophos Disk Encryption 5.61 help*.

3.3.4 Install encryption software manually

If you have computers that you cannot protect automatically, protect them by running an installer from the shared folder to which the encryption software has been downloaded. This shared folder is known as the *bootstrap location*.

Make sure that the endpoints have been prepared for full disk encryption installation, in particular that the Sophos anti-virus software version 10 has been installed and that third-party encryption software has been uninstalled.

During the installation of full disk encryption, make sure that only one user session is active on the endpoint. If you do not do this, the installation will fail.

You must log on to the computers that you want to protect as a Windows administrator.

To install encryption software on computers manually:

1. To find out which directory the installer is in, open Enterprise Console and select **Bootstrap locations** from the **View** menu.

   In the **Bootstrap Locations** dialog box, the **Location** column displays the bootstrap location for each platform. Make a note of the relevant paths.

2. At the computer that hosts the bootstrap location, create a read-only user account.
3. Go to each computer and log on with local administrator rights.
4. Locate the encryption setup program setup.exe in the bootstrap location and double-click it.

   The encryption setup program can be found in the following location: \\<ServerName>\SophosUpdate\CIDs\<Subscription>\ENCRYPTION

5. A wizard guides you through installation of the encryption software.

To complete installation, the computer is restarted automatically.

4 SDE/SGE 4.x to Sophos Disk Encryption 5.61

This section describes how to migrate from Sophos SafeGuard Disk Encryption (SDE) 4.6x / SafeGuard Easy (SGE) 4.5x to Sophos Disk Encryption 5.61. It explains which features can be migrated and details the limitations.

To migrate from SDE/SGE 4.x to Sophos Disk Encryption 5.61 you:

- Set up the latest Sophos Enterprise Console.
- Migrate computers.

  Sophos Disk Encryption 4.6x and SafeGuard Easy 4.5x endpoints can be directly migrated to Sophos Disk Encryption 5.61 by installing the Sophos encryption agent installation package on the endpoints. Hard drive encryption is being maintained, so there is no need to decrypt and re-encrypt the hard drive. It is not necessary to uninstall the Sophos encryption software before migration.

4.1 Set up Sophos Enterprise Console

If you have no Enterprise Console installed, install the latest version including encryption.

If you have a previous version of Enterprise Console installed, upgrade to the latest version including encryption.

If you already have the latest version of Enterprise Console installed without encryption, re-install it to add encryption.

When the latest version is installed, configure the full disk encryption policy.

Note: Using the SafeGuard Policy Editor to manage the Enterprise Console database is not supported.

4.1.1 Install Enterprise Console

To install Enterprise Console:

1. Go to the download web page that is specified in your download email. Type your username and password. Download the installers that you need.
2. At the computer where you want to install Enterprise Console, log on as an administrator:
   - If the server is in a domain, use a domain account that has local administrator rights.
   - If the server is in a workgroup, use a local account that has local administrator rights.
3. Find the Enterprise Console installer that you downloaded earlier.
4. Double-click the installer.

5. When you are prompted, click **Install**.

   The installation files are copied to the computer and a wizard starts.

6. The wizard guides you through installation. You should do as follows:
   a) Accept the defaults wherever possible.
   b) On the **Components Selection** page, ensure that all the components are selected.
   c) On the **Database details** page, enter details of an account that can access the computer where you are installing Enterprise Console. This should not be an administrator account.
   d) On the **Manage Encryption** page, click **Manage Encryption**.
   e) On the **Sophos Encryption** page, click **New installations**. You are prompted for the password for the certificates backup store. Make a note of the password.

7. When installation is complete, you may be prompted to restart. Click **Yes** or **Finish**.

4.1.2 Upgrade Sophos Enterprise Console

If you have Sophos Enterprise Console below 5.1 installed on your computer, upgrade to the latest version of Sophos Enterprise Console including encryption.

To do so, run the latest Enterprise Console installer and follow the instructions. For more information, see the *Sophos Enterprise Console upgrade guide*.

Note: In the installer wizard make sure that you select to manage encryption with Enterprise Console.

Sophos Enterprise Console is upgraded, the full disk encryption feature is available.

4.1.3 Add encryption to Sophos Enterprise Console

If you have Sophos Enterprise Console 5.1 or later without encryption installed on your computer, re-install it to add encryption.

Note: If you are not using the latest version of Enterprise Console, we recommend upgrading to the latest version first.

1. At the computer where you want to install Enterprise Console, log on as an administrator:
   - If the server is in a domain, use a domain account that has local administrator rights.
   - If the server is in a workgroup, use a local account that has local administrator rights.
2. Find the Enterprise Console installer that you downloaded earlier.
3. Double-click the installer.
4. When you are prompted, click **Modify**.

   The installation files are copied to the computer and a wizard starts.

5. The wizard guides you through installation. You should do as follows:
   a) Accept the defaults wherever possible.
   b) On the **Components Selection** page, ensure that all the components are selected.
   c) On the **Database details** page, enter details of an account that can access the computer where you are installing Enterprise Console. This should not be an administrator account.
   d) On the **Manage Encryption** page, click **Manage Encryption**.
   e) On the **Sophos Encryption** page, click **New installations**. You are prompted for the password for the certificates backup store. Make a note of the password.
6. When installation is complete, you may be prompted to restart. Click **Yes** or **Finish**.

4.1.4 Configure the full disk encryption policy

On endpoint computers that have been encrypted before migration, hard drives remain encrypted. Data on encrypted hard drives can be accessed as before.

Configure the full disk encryption policy in Sophos Enterprise Console. A default full disk encryption policy is available with pre-defined encryption and authentication settings for quick and easy policy deployment. Select the volumes to encrypt in the default policy and configure it to your needs.

After migrating the computers, assign the full disk encryption policy to them to make sure that all encryption settings are consistent.

For further information, see the *Sophos Enterprise Console Help*.

4.2 Migrate computers

To migrate computers with Sophos Disk Encryption (SDE) 4.6x / SafeGuard Easy 4.5x installed to Sophos Disk Encryption you:

- Prepare computers.
- Start migration.
- Log on to the computer after migration.
- Convert keys for encrypted removable media.

4.2.1 Prerequisites

- Direct migration is supported for Sophos SafeGuard Disk Encryption 4.6x and SafeGuard Easy 4.5x. A direct upgrade should also work for SafeGuard Easy versions 4.3x and 4.4x. SafeGuard Easy versions older than 4.3x must be upgraded to SafeGuard Easy 4.50 first.

- SafeGuard Easy/Sophos SafeGuard Disk Encryption must be running on the following operating system:

  Windows XP Professional Workstation Service Pack 2, 3

- Windows Installer Version 3.01 or higher has to be installed.

- The hardware must meet the system requirements of the Sophos Disk Encryption 5.61 encryption agent.
- When using special software (for example Lenovo middleware), it must meet the system requirements of the Sophos Disk Encryption 5.61 encryption agent.
- Upgrade is supported if the hard disks are encrypted with the following algorithms: AES128, AES256, 3DES, IDEA.
- Users need a valid Windows account and password. If they do not know their Windows password because they have previously been logged on to Windows using Secure Automatic Logon, the Windows user password has to be reset before migration and the new password has to be forwarded to the users.

4.2.2 Limitations

- The following installations cannot be migrated and a migration should not be attempted.

  Note:

  If you start migrating in the following cases, an error message is displayed (error number 5006).

  Twin Boot installations

  Installations with active Compaq Switch

  Lenovo Computrace installations

  Hard drives that are partially encrypted, for example with boot sector encryption only.

  Hard drives with hidden partitions

  Hard drives that have been encrypted with one of the following algorithms: XOR, STEALTH, DES, RIJNDAEL, Blowfish-8, Blowfish-16

  Multi-boot scenarios with a second Windows or Linux partition

- Removable media that have been encrypted with one of the following algorithms cannot be migrated: XOR, STEALTH, DES, RIJNDAEL, Blowfish-8, Blowfish-16.

  Note:

  There is a risk of data being lost in these cases. After migration, data on the removable medium cannot be accessed with Sophos Disk Encryption any more.

- Removable media with Super Floppy volumes cannot be transformed after migration.

4.2.3 Which functionality is migrated

The table below shows which functionality is migrated and how it is handled in Sophos Disk Encryption.

Sophos SafeGuard Disk Encryption/SafeGuard Easy	Migration	Sophos Disk Encryption
Encrypted hard drives	Yes	The hard drive keys are protected by Power-on Authentication. So the hard drive key is at no time exposed. If Boot Protection mode has been selected in SafeGuard Easy, the current version has to be uninstalled. The hard drive encryption algorithm is not changed by migration. Therefore the actual algorithm for this type of migrated hard drive may differ from the general policy.
Encrypted removable media (only applicable when migrating from SafeGuard Easy)	Yes	Encrypted removable media remain encrypted and data copied to it will be encrypted. You can access the encrypted data. Removable media that was unencrypted before migration will stay unencrypted after migration.
Sophos SafeGuard Disk Encryption/SafeGuard Easy user names and passwords	No	Windows user names and passwords are used instead.
Policies	No	To make sure that all settings are consistent, no automatic upgrade is executed. The policies have to be reset in Enterprise Console.
Pre-Boot Authentication	No	Pre-Boot Authentication (PBA) is replaced by Power-on Authentication (POA).
Tokens/smartcards (only applicable when migrating from SafeGuard Easy)	No	Sophos Disk Encryption 5.61 on endpoints does not support tokens/smartcards. Logging on is only possible with user name and password or Fingerprint. It is absolutely necessary to make sure that users know their Windows credentials. Otherwise they cannot log on.
Logon with Lenovo Fingerprint Reader	To some degree	Fingerprint logon can continue to be used. The fingerprint reader hardware and software has to be supported by Sophos Disk Encryption 5.61 and the fingerprint user data have to be rolled out again. For further information on fingerprint logon, see the *Sophos Disk Encryption Help*.

4.2.4 Prepare computers

- Prepare the endpoints for installation of the encryption software, see Prepare computers for installation (page 8).
- We recommend that you create a valid kernel backup and save this backup in a location that can always be accessed, for example a network path. For further information, see *Saving the*

system kernel and creating emergency media in the *SafeGuard Easy 4.5x/Sophos SafeGuard Disk Encryption 4.6x Help*.

- To reduce the risk of data loss, we recommend that you create a test environment for the first upgrade.
- When migrating from older versions of SafeGuard Easy, first upgrade to version 4.50.
- Leave the computers switched on throughout the upgrade process.
- **Note:** Users need a valid Windows account and password. If they do not know their Windows password because they have previously been logged on to Windows using Secure Automatic Logon, the Windows user password has to be reset before migration and the new password has to be forwarded to the users.

  The administrator should keep the users' Windows credentials at hand in case users have forgotten their Windows passwords after upgrading.

4.2.5 Start migration

Note:

The installation can be carried out on a running Sophos SafeGuard Disk Encryption / SafeGuard Easy system. Decryption of encrypted hard drives is not necessary.

To start the migration:

1. Double-click WIZLDR.exe from the Sophos SafeGuard Disk Encryption / SafeGuard Easy program folder of the endpoint that is to be upgraded. This starts the Migration Wizard.
2. In the Migration Wizard, enter the **SYSTEM** password and click **Next**. In **Destination folder**, click **Next**, and then click **Finish**. A migration configuration file **`SGEMIG.cfg`** is created.
3. In Windows Explorer, rename this file from **`SGEMIG.cfg`** to **`SGE2SGN.cfg`**.

   Note: Owner/creator rights have to be set for this file and the file path where it is stored during the upgrade. Otherwise, the upgrade may fail and a message stating that **`SGE2SGN.cfg`** cannot be found, is displayed.

4. Install the Sophos Disk Encryption agent by running the setup.exe from the central installation directory and adding the parameter MIGFILE with the file path and name of the migration configuration file.

   Example:

   ```
   \\<ServerName>\SophosUpdate\CIDs\<Subscription>\ENCRYPTION\Setup.exe
   /migfile \\Server\Share\SGE2SGN.cfg
   ```

5. In Enterprise Console, assign the full disk encryption policy created before to the migrated computers.

- If the migration is successful, the Sophos Disk Encryption agent is ready on the computer.
- If the migration fails, Sophos SafeGuard Disk Encryption / SafeGuard Easy can still be used on the computer. In such cases the new encryption agent is automatically removed.

4.2.6 Log on to computers after migration

To log on to computers that have been migrated:

1. Restart the endpoint computer. The first logon is still achieved with Autologon. New keys and certificates are assigned to the user.
2. Restart the endpoint computer for a second time. Log on at the Power-on Authentication. The computers are protected again only after the second restart.
3. Log on to Windows to receive new keys and certificates.
4. To be able to access the hard drive, restart the computer again.

4.2.7 Convert keys for encrypted removable media

The appropriate encryption policy has to be present on the computer before conversion. Otherwise the keys are not converted.

Encrypted removable media remain encrypted, but the keys have to be converted to a compatible format.

Note:

After conversion, an encrypted data medium can only be read with Sophos Disk Encryption and only at the one endpoint computer where it was converted during migration.

1. Detach the media from the computer and reinsert it. This ensures that you can decrypt removable media or add and remove keys for removable media encryption.
2. In Windows Explorer, double-click the media you want to access.
3. You are prompted to confirm the transformation of the encryption keys into a compatible format.
   - If you confirm the conversion, full access to the migrated data is provided.
   - If you reject the conversion, the migrated data can still be opened for reading and writing.

5 SDE/SGE 5.5x or 5.6x to Sophos Disk Encryption 5.61

You can migrate Sophos SafeGuard Disk Encryption (SDE) / SafeGuard Easy (SGE) 5.5x or 5.6x to Sophos Disk Encryption 5.61 with central management through Enterprise Console to make use of comprehensive management features.

To migrate from SDE/SGE 5.5x or 5.6x to Sophos Disk Encryption 5.61 you:

- Set up Enterprise Console.
- Upgrade computers.

5.1 Set up Sophos Enterprise Console

If you have no Enterprise Console installed, install the latest version including encryption.

If you have a previous version of Enterprise Console installed, upgrade to the latest version including encryption.

If you already have the latest version of Enterprise Console installed without encryption, re-install it to add encryption.

When the latest version is installed, configure the full disk encryption policy.

Note: Using the SafeGuard Policy Editor to manage the Enterprise Console database is not supported.

5.1.1 Install Enterprise Console

To migrate from SafeGuard Disk Encryption 5.5x or 5.6x/SafeGuard Easy 5.5x or 5.6x with SafeGuard Policy Editor to Sophos Enterprise Console, the following prerequisites must be met:

- Access to the MSO certificate and private key (.p12) of your SafeGuard Disk Encryption 5.x/SafeGuard Easy 5.x environment and the corresponding password must be available.
- Access to the company certificate backup (.p12) of your SafeGuard Disk Encryption 5.5x or 5.6x/SafeGuard Easy 5.5x or 5.6x environment must be available.
- The server component of the Sophos Enterprise Console cannot be installed on a computer with SafeGuard Policy Editor or with Sophos SafeGuard Client.

1. Go to the download web page that is specified in your download email. Type your username and password. Download the installers that you need.
2. At the computer where you want to install Enterprise Console, log on as an administrator:
   - If the server is in a domain, use a domain account that has local administrator rights.
   - If the server is in a workgroup, use a local account that has local administrator rights.
3. Find the Enterprise Console installer that you downloaded earlier.

4. Double-click the installer.
5. When you are prompted, click **Install**.

   The installation files are copied to the computer and a wizard starts.

6. The wizard guides you through installation. You should do as follows:
   a) Accept the defaults wherever possible.
   b) On the **Components Selection** page, ensure that all the components are selected.
   c) On the **Database details** page, enter details of an account that can access the computer where you are installing Enterprise Console. This should not be an administrator account.
   d) On the **Manage Encryption** page, click **Manage encryption**.
   e) On the **Sophos Encryption** page, click **Existing installations**.
   f) On the **Import Certificates** page, click **Import** to browse for the respective certificate backups of your previous Sophos encryption installation. Enter the password for each backup.
7. When installation is complete, you may be prompted to restart. Click **Yes** or **Finish**.

5.1.2 Upgrade Sophos Enterprise Console

If you have Sophos Enterprise Console below 5.1 installed on your computer, upgrade to the latest version of Sophos Enterprise Console including encryption.

To do so, run the latest Enterprise Console installer and follow the instructions. For more information, see the *Sophos Enterprise Console upgrade guide*.

Note: In the installer wizard make sure that you select to manage encryption with Enterprise Console.

Sophos Enterprise Console is upgraded, the full disk encryption feature is available.

5.1.3 Add encryption to Sophos Enterprise Console

If you have Sophos Enterprise Console 5.1 or later without encryption installed on your computer, re-install it to add encryption.

Note: If you are not using the latest version of Enterprise Console, we recommend upgrading to the latest version first.

1. At the computer where you want to install Enterprise Console, log on as an administrator:
   - If the server is in a domain, use a domain account that has local administrator rights.
   - If the server is in a workgroup, use a local account that has local administrator rights.
2. Find the Enterprise Console installer that you downloaded earlier.
3. Double-click the installer.
4. When you are prompted, click **Modify**.

   The installation files are copied to the computer and a wizard starts.

5. The wizard guides you through installation. You should do as follows:
   a) Accept the defaults wherever possible.
   b) On the **Components Selection** page, ensure that all the components are selected.
   c) On the **Database details** page, enter details of an account that can access the computer where you are installing Enterprise Console. This should not be an administrator account.
   d) On the **Manage Encryption** page, click **Manage Encryption**.
   e) On the **Sophos Encryption** page, click **Existing installations**.
   f) On the **Import Certificates** page, click **Import** to browse for the respective certificate backups of your previous Sophos encryption installation. Enter the password for each backup.
6. When installation is complete, you may be prompted to restart. Click **Yes** or **Finish**.

5.1.4 Configure the full disk encryption policy

On endpoint computers that have been encrypted before migration, hard drives remain encrypted. Data on encrypted hard drives can be accessed as before.

Configure the full disk encryption policy in Sophos Enterprise Console. A default full disk encryption policy is available with pre-defined encryption and authentication settings for quick and easy policy deployment. Select the volumes to encrypt in the default policy and configure it to your needs.

After migrating the computers, assign the full disk encryption policy to them to make sure that all encryption settings are consistent.

For further information, see the *Sophos Enterprise Console Help*.

5.2 Upgrade computers

You upgrade computers with Sophos SafeGuard Disk Encryption (SDE) / SafeGuard Easy (SGE) 5.5x or 5.6x installed to Sophos Disk Encryption 5.61 by simply installing the Sophos Disk Encryption 5.61 agent software. There is no need to uninstall the previous Sophos encryption software.

You can do this either automatically or manually.

Note: Migration of endpoints with SafeGuard Data Exchange installed is not supported. You have to uninstall SafeGuard Data Exchange first before migration.

5.2.1 Install encryption software automatically

Make sure that the endpoints have been prepared for full disk encryption installation, in particular that the Sophos anti-virus software version 10 has been installed and that third-party encryption software has been uninstalled. For further information, see Prepare computers for installation (page 8).

To install encryption software automatically:

1. In Enterprise Console, select the computers on which you want to install full disk encryption.

2. Right-click the computers, and then click **Protect computers**. The **Protect Computers Wizard** is launched.
3. On the **Welcome** page, click **Next**.
4. On the **Installation Type** page, select **Encryption software**.
5. If there is more than one encryption subscription and installer location (bootstrap location) available, the **Encryption location** page is displayed. Select the **Encryption subscription** and **Address** to install from.
6. On the **Encryption summary** page, check for any installation problems.
7. On the **Credentials** page, enter details of an account that can be used to install software on computers.

Installation is staggered, so the process may not be complete on all the computers for some time.

The installation of encryption will cause computers to restart automatically within about 30 minutes after installation of the encryption software. If encryption is enabled by policy, it will only take place after the computer's restart.

For further information on the start behaviour of the computer and first logon after installation and activation of encryption, see the *Sophos Disk Encryption 5.61 help*.

5.2.2 Install encryption software manually

If you have computers that you cannot protect automatically, protect them by running an installer from the shared folder to which the encryption software has been downloaded. This shared folder is known as the *bootstrap location*.

Make sure that the endpoints have been prepared for full disk encryption installation, in particular that the Sophos anti-virus software version 10 has been installed and that third-party encryption software has been uninstalled.

During the installation of full disk encryption, make sure that only one user session is active on the endpoint. If you do not do this, the installation will fail.

You must log on to the computers that you want to protect as a Windows administrator.

To install encryption software on computers manually:

1. To find out which directory the installer is in, open Enterprise Console and select **Bootstrap locations** from the **View** menu.

   In the **Bootstrap Locations** dialog box, the **Location** column displays the bootstrap location for each platform. Make a note of the relevant paths.

2. At the computer that hosts the bootstrap location, create a read-only user account.
3. Go to each computer and log on with local administrator rights.
4. Locate the encryption setup program setup.exe in the bootstrap location and double-click it.

   The encryption setup program can be found in the following location:
   \\<ServerName>\SophosUpdate\CIDs\<Subscription>\ENCRYPTION

5. A wizard guides you through installation of the encryption software.

To complete installation, the computer is restarted automatically.

5.3 Merge two SDE/SGE 5.5x or 5.6x environments into Sophos Disk Encryption 5.61

You only need to carry out this step, if you have two Sophos SafeGuard Disk Encryption (SDE) 5.5x or 5.6x/ SafeGuard Easy (SGE) 5.5x or 5.6x environments using different company certificates and want to merge them into one Sophos Disk Encryption environment.

Note: You must have carried out the steps for migrating SDE/SGE 5.5x or 5.6x to Sophos Disk Encryption 5.61, see SDE/SGE 5.5x or 5.6x to Sophos Disk Encryption 5.61 (page 17).

The SDE/SGE protected computers need to be moved to one SDE/SGE environment managed by one SafeGuard Policy Editor. You therefore need to decide which is your source environment (the computers that need to be moved) and which is your target environment (the SDE/SGE environment where they should be moved to).

5.3.1 Replace the company certificate

The following prerequisites must be met:

Decide which is your source and which is your target Policy Editor environment. The source Policy Editor is the one you used for creating the configuration packages for the endpoints that are to be moved. The target Policy Editor is the one the endpoints will be moved to.

To replace the company certificate:

1. Upgrade each SafeGuard Policy Editor instance of the two environments you want to merge into Sophos Disk Encryption with SafeGuard Policy Editor version 5.61. If necessary, import a valid license file or use the license file that can be downloaded together with new SafeGuard Policy Editor version. For further information, see the *SDE/SGE Administrator help*.
2. On the target Policy Editor, export the company certificate: On the **Tools** menu, click **Options**. Select the **Certificates** tab and click the **Export** button under **Company Certificate**. Enter and confirm a password for the certificate backup when prompted and select a destination directory and filename when prompted. The company certificate is exported (.p12 file).
3. On the source Policy Editor, on the **Tools** menu, click **Options** and select **Create...** next to **Create signed Company Certificate Change order (CCO)**. In the **Create CCO** dialog, browse for the target company certificate you exported on the target Policy Editor (step 2). Make sure that it is the desired certificate. Click **Create** and select a destination directory and file name for the .cco file. Confirm that you want to place a **Company Certificate Change Order**.
4. On the target Policy Editor, create a configuration package: On the **Tools** menu, click **Configuration Package Tool** and add a new configuration package. Leave the policy group and POA group settings to **not configured**. Do not specify a key backup location. Select **Include Company Certificate Change order (CCO)** and specify an output path. Click **Create Configuration Package**. Select the .cco file created in the source Policy Editor when prompted. Click **Open**. The configuration package is created in the specified location.

   Note: Do not remove or change existing configuration packages as they are needed by Enterprise Console.

5. Install this configuration package on all endpoints you want to move from the source environment to the target environment.

6 Technical support

You can find technical support for Sophos products in any of these ways:

- Visit the SophosTalk community at community.sophos.com/ and search for other users who are experiencing the same problem.
- Visit the Sophos support knowledgebase at www.sophos.com/en-us/support.aspx.
- Download the product documentation at www.sophos.com/en-us/support/documentation.aspx.
- Open a ticket with our support team at https://secure2.sophos.com/support/contact-support/support-query.aspx.

7 Legal notices

You find copyright information on third party suppliers in the *Disclaimer and Copyright for 3rd Party Software* document in your SafeGuard product directory.