SOPHOS

Cybersecurity made simple.

Sophos Enterprise Console

upgrade guide

product version: 5.5

Contents

About this guide....1
Which versions can I upgrade from?....2
Sophos Disk Encryption....4
    Upgrade Sophos Disk Encryption 5.61 to SafeGuard Enterprise....4
    Uninstall Sophos Disk Encryption....5
Tool version compatibility for Sophos Enterprise Console....6
What are the steps in upgrading?....7
System requirements....8
    Free disk space requirements....8
The accounts you need....9
Will I get the same updates as before?....10
    About Sophos Update Manager upgrade....11
Download the installer....12
Upgrade Sophos Enterprise Console....13
    Back up Sophos Enterprise Console data and configuration....13
    Upgrade Sophos Enterprise Console....14
    Enhance database security....14
    Check existing policies....15
Enable Malicious Traffic Detection....17
Technical support....18
Legal notices....19

1 About this guide

This guide tells you how to upgrade to Sophos Enterprise Console.

2 Which versions can I upgrade from?

You can upgrade to Sophos Enterprise Console 5.5.1 directly from:

- Sophos Enterprise Console 5.5.0
- Sophos Enterprise Console 5.4.1
- Sophos Enterprise Console 5.4.0
- Sophos Enterprise Console 5.3.1
- Sophos Enterprise Console 5.3.0
- Sophos Enterprise Console 5.2.2
- Sophos Enterprise Console 5.2.1 R2
- Sophos Enterprise Console 5.2.1
- Sophos Enterprise Console 5.2.0
- Sophos Enterprise Console 5.1
- Sophos Enterprise Console 5.0

Note
If you upgrade from 5.4.0 or earlier, Sophos Enterprise Console may have problems communicating with computers running older versions of Sophos Remote Management System. See knowledgebase article 124873.

Note
Note: If you are upgrading from Sophos Enterprise Console 5.0, 5.1, 5.2.0, 5.2.1, 5.2.1 R2, 5.2.2, 5.3.0, 5.3.1, 5.4, 5.4.1 or 5.5.0, changes to the database component are required. For more information, go to knowledgebase article 128185.

Note: If you want to upgrade the Sophos databases manually by running the database install scripts, see knowledgebase article 116768.

If you are using Sophos Enterprise Console 4.x or Enterprise Manager 4.7, you will need to upgrade in two steps: first upgrade to Sophos Enterprise Console 5.1 and then upgrade to Sophos Enterprise Console 5.4.1.

If you are using Sophos Control Center 4.0.1 or 4.1, you will need to upgrade in two steps by following one of the supported upgrade paths:

- Upgrade to Sophos Enterprise Console 5.1 and then upgrade to Sophos Enterprise Console 5.5.1.
- Upgrade to Sophos Enterprise Console 5.2.2 and then upgrade to Sophos Enterprise Console 5.5.1.

Note: Alternatively, you could use Sophos Central to manage your computers. To find answers to frequently asked questions about Sophos Central, see knowledgebase article 119598. For information about migration to Sophos Central, see knowledgebase article 122264.

See also knowledgebase article 119105 for more information about different upgrade paths.

The installers for earlier versions of Sophos Enterprise Console are available from the Sophos Enterprise Console Downloads page (http://www.sophos.com/en-us/support/downloads/console/sophos-enterprise-console.aspx).

Do I need to upgrade the databases separately?

If your databases are local (on the same computer as the management server component), they will be upgraded automatically when you follow the steps in this guide.

If your databases are on a remote or clustered SQL Server, you must upgrade them first. If you're upgrading from Sophos Enterprise Console 5.2.1 or later, see knowledgebase article 33980. If you're upgrading from an earlier version and want to upgrade the Sophos databases manually by running the database install scripts, see knowledgebase article 116768.

Unix endpoints

You may need to upgrade Sophos Anti-Virus on managed UNIX endpoints after you upgrade to Sophos Enterprise Console 5.5.1.

3 Sophos Disk Encryption

There is no upgrade for Sophos Disk Encryption 5.61. The product has been retired. If you use Sophos Disk Encryption and manage it via the **Full disk encryption** policy in Sophos Enterprise Console, we recommend that you do one of the following:

- Upgrade Sophos Disk Encryption to SafeGuard Enterprise 6.10.

  Note
  A direct upgrade to SafeGuard Enterprise 7 is not supported.

- Uninstall Sophos Disk Encryption.

3.1 Upgrade Sophos Disk Encryption 5.61 to SafeGuard Enterprise

Migration from Sophos Disk Encryption 5.61 to SafeGuard Enterprise 6.10 involves the following steps:

1. 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.
2. 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.

   For detailed information on SafeGuard Enterprise installation, see the *SafeGuard Enterprise 6.1 installation guide*. SafeGuard Enterprise documentation is available at www.sophos.com/en-us/support/documentation/safeguard-enterprise.aspx.
3. In the SafeGuard Management Center configuration wizard, select a new database to be created and import the company certificate exported before.
4. 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.
5. 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.
6. To prevent a communication issue that causes endpoint computers to communicate with both the new SafeGuard Enterprise Server and the old Sophos Enterprise Console, see knowledgebase article 121160.
7. In SafeGuard Management Center, create and assign policies as desired.

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

3.2 Uninstall Sophos Disk Encryption

1. In Sophos Enterprise Console, check which full disk encryption policy is used by the group(s) of computers you want to migrate. In the **Groups** pane, right-click the group and click **View/Edit Group Policy Details**. In the group details dialog box, you can see the policies currently used.
2. Open the **Full disk encryption** policy you want to disable and deselect all the options under **Volumes to encrypt**.
3. Under **Power-on Authentication (POA)**, clear the **Enable Power-on Authentication** check box. Click **Yes** in the confirmation message. Click **OK**.

   Make sure the updated policy is applied to the endpoints. (In the computer list, the **Policy compliance** status changes to “Awaiting policy transfer”, and then back to “Same as policy” when the updated policy is applied to the computers.)
4. On the endpoint, if tamper protection is enabled, disable it.

   Note
   You can also disable tamper protection in Sophos Enterprise Console for a group or groups of computers. In the respective **Tamper Protection Policy**, clear the **Enable tamper protection** check box and make sure that the updated policy is applied to the computers.

5. Make sure that an update is not currently being performed.
   a) Check the updating status by right-clicking the Sophos shield in the notification area in the taskbar and ensuring that **View updating status** is grayed out and cannot be selected. If an update is currently in progress, wait for it to complete before continuing.
   b) Open Windows services. Depending on your operating system, click **Start > Run** and type “services.msc”, or click **Start**, type “services.msc” in the Start menu search box, and then press Enter.
   c) Right-click on the **Sophos AutoUpdate Service** and select **Stop**.

   Note
   Stopping the **Sophos AutoUpdate Service** prevents an update from occurring during the uninstallation. If the service is not stopped and the uninstallation of Sophos SafeGuard is delayed for a period longer than the update interval, then Sophos SafeGuard could be re-installed.

6. In Control Panel, depending on your operating system, double-click **Add/Remove Programs** or click **Programs and Features**.
7. Uninstall Sophos SafeGuard 5.61.0 Client.

   Encrypted drives on the computer are decrypted during the uninstallation.
8. Uninstall Sophos SafeGuard 5.61.0 Preinstall.
9. Restart the computer.

4 Tool version compatibility for Sophos Enterprise Console

The following table shows version compatibility between Enterprise Console tools and Enterprise Console.

Important
After an upgrade to Enterprise Console 5.5 reinstall Sophos Cloud Migration Tool and Virtualization Scan Controller, and restart the Reporting Log Writer service. This enables these tools to work.

The Enterprise Console tools are available for download from https://www.sophos.com/support/downloads.aspx.

Table 1: Tool version compatibility for Sophos Enterprise Console

Enterprise Console	Reporting Interface	Reporting Log Writer	Virtualization Scan Controller
5.5.0	*	5.1	2.0
5.4.1	*	5.1	2.0
5.4.0	*	5.1	2.0
5.3.1	*	5.1	2.0
5.3.0	*	5.1	2.0
5.2.2	*	5.1	2.0
5.2.1 R2	*	5.1	2.0
5.2.1	*	5.1	2.0
5.2	*	5.1	2.0
5.1	5.1*	5.1	1.0

* Since version 5.1, Reporting Interface database objects are installed as part of the Sophos Enterprise Console database installation, and the standalone installer on the Sophos Reporting Interface download page includes only Reporting Log Writer.

Important
If you installed Reporting Interface separately with an earlier version of Sophos Enterprise Console, uninstall it before upgrading that version.

5 What are the steps in upgrading?

Upgrading involves the following steps.

- Check the system requirements.
- Check the accounts you need.
- Check whether you need to change your software subscriptions.
- Download the installer.
- Upgrade Enterprise Console.

6 System requirements

For system requirements, go to the system requirements page of the Sophos website (http://www.sophos.com/en-us/products/all-system-requirements.aspx).

For details of any additional requirements, for example for language support, see the "Additional information" section in the release notes.

6.1 Free disk space requirements

The amount of free disk space you need to upgrade Sophos Enterprise Console depends on the size of the Sophos Enterprise Console database files (.mdf files) and transaction log files (.ldf files) that are currently in use.

Tip
The file names begin with "SOPHOS" and usually contain Sophos Enterprise Console version number.

For information about the database file names for different console versions and how to locate the database files on disk, see Sophos knowledgebase article 17323.

To ensure that you have sufficient disk space to upgrade Sophos Enterprise Console, do the following:

- Check the disk drive on which the database files (.mdf files) are deployed and ensure that it has free capacity of at least three times the current size of the .mdf files.
- Check that the disk drive on which the transaction log files (.ldf files) are deployed and ensure that it has free capacity of at least eight times the current size of the database files (.mdf files).
- If both .mdf and .ldf files are deployed on the same disk, ensure that it has free capacity of at least 10 times the current size of the .mdf files.

If you have upgraded Sophos Enterprise Console in the past, you may still have old Sophos Enterprise Console databases that are no longer required. You may consider deleting those databases to free up disk space. For more information, see Sophos knowledgebase article 17508.

7 The accounts you need

Accounts required to perform the upgrade

Ensure that the user logged on to and running the upgrade on the management server has sufficient rights to all Sophos databases. The user running the management server upgrade should be a member of the "db_owner" role on each of the Sophos databases (members of the server role "sysadmin" would implicitly have sufficient rights to all databases). These rights are only required temporarily during the upgrade, to check that the new databases have been created and to migrate the data.

Note
For a list of database names per version of the console, see Sophos knowledgebase article 17323.

Sophos database account

When you upgrade your management console, you might be asked for details of a database account. This happens if your existing account no longer meets the requirements.

Ensure you have an account that:

- Can log onto the computer where the management console is installed. For distributed installations ofSophos Enterprise Console, the account must be able to log onto the computer where the Sophos Management Server component is installed.
- Can read and write to the system temporary directory e.g. "\windows\temp\". By default, members of "Users" have this right.
- Has a UPN (User Principal Name) associated with the account if it is a domain account.

All other rights and group memberships that the account needs are granted automatically during the upgrade.

Sophos recommends that the account:

- Is not set to expire and does not have any other logon restriction.
- Is not an administrative account.
- Is not changed after the upgrade.

For more information, see Sophos knowledgebase article 113954.

8 Will I get the same updates as before?

Since version 5.2.1, Sophos Enterprise Console supports new options for getting your automatic updates from Sophos and doesn't support some of the old ones. If you are upgrading from an earlier version, depending on the software packages you selected when you installed Sophos Enterprise Console, you may need to change your software subscription settings before you upgrade.

To open an endpoint software subscription, on the **View** menu, click **Update Managers**. In the **Software Subscriptions** pane, double-click the subscription you want to check.

To open an update manager software subscription, in the **Update managers** view, double-click the update manager you want to check. In the **Configure update manager** dialog box, go to the **Advanced** tab.

The following matrix shows whether you can or cannot upgrade with your current settings.

Table 2: Upgrading with different software subscriptions

Software package	Upgrade possible	Advice, if applicable
Endpoint		
Recommended (default)	Yes	
Previous	Yes	
Oldest	No	Resubscribe to a different package, for example, "Previous".
Extended Maintenance Recommended	Yes	
Extended Maintenance Previous	Yes	
Extended Maintenance Oldest	No	Resubscribe to a different package, for example, "Extended Maintenance Previous".
Fixed (e.g. *10.3.15 VE3.60.0*)	Yes	Sophos Enterprise Console uses fixed packages. For more information, see the Sophos Enterprise Console Help, Fixed version software packages.
Update Manager		
1 Recommended (default)	Yes	
Preview	Yes	
Extended	Yes	

Software package	Upgrade possible	Advice, if applicable
1 Previous	No	Resubscribe to "1 Recommended". For more information, read About Sophos Update Manager upgrade (page 11).
1 Oldest	No	
Fixed (e.g. *1.5.4.11*)	No	

If your software package is no longer supported and you don't change your subscription before upgrading, the installer will warn you about the unsupported subscriptions and you won't be able to proceed with the upgrade. For more information about software packages, see Sophos knowledgebase article 112580.

8.1 About Sophos Update Manager upgrade

Since version 5.2.1, Sophos Enterprise Console supports only one, recommended Sophos Update Manager software package. If you are upgrading from a version earlier that 5.2.1, Update Manager (and any additional Update Managers, if you use them) must be subscribed to the "1 Recommended" package. Otherwise, you won't be able to upgrade.

If you are not subscribed to the "1 Recommended" package, you will need to subscribe to it and ensure that Update Manager has been updated to the latest recommended version before upgrading Sophos Enterprise Console.

If the Update Manager installer in the share `\\Servername\SUMInstallSet` on the computer where Sophos Enterprise Console management server is installed is earlier than the latest recommended version, the installer will be updated during the upgrade.

9 Download the installer

Note
You can download the installers at any computer and then copy them to the computer where you will use them.

1. Log in to https://www.sophos.com/en-us/support/downloads.aspx with your Sophos ID.

   Note
   If you need help with your Sophos ID, see Sophos knowledgebase article 111195.

2. If you have logged in for downloads before, you see the **Product Downloads and Updates** page.

   Note
   If this is your first time, you see your profile. Click **Endpoint and Server Protection** and then **Downloads and Updates**.

3. Under **Console**, click the link for **Sophos Enterprise Console** and download the installer.

10 Upgrade Sophos Enterprise Console

10.1 Back up Sophos Enterprise Console data and configuration

Before you upgrade Sophos Enterprise Console, use the DataBackupRestore.exe tool to back up:

- Databases: Enterprise Console (core) - SOPHOS5x, Patch - SOPHOSPATCH or SOPHOSPATCH5x, and Auditing - SophosSecurity.
- Registry settings
- Account information
- Configuration files

Important
The DataBackupRestore.exe tool will back up the Sophos management server's configuration only from a default installation location. Backing up or restoring the configuration files will fail if you have installed Sophos Enterprise Console to a non-default location. The default location is:

- Windows 64-bit: %programfiles(x86)%\Sophos\Enterprise Console\
- Windows 32 **and** 64-bit: %programfiles%\Sophos\Enterprise Console\

If you use a non-default installation location, see Sophos knowledgebase article 114299 for advice.

If Sophos Enterprise Console databases are on a remote server, you can use Sophos tools BackupDB.bat and RestoreDB.bat to back up and restore the databases. For more information, see Sophos knowledgebase article 110380.

To back up the Sophos Enterprise Console data and configuration:

1. Log on as the Administrator to the computer where the Sophos Enterprise Console management server is installed.
2. Open Command Prompt (click **Start**, **Run**, type **cmd**, and then press Enter).
3. Browse to the folder containing the tool.
   - In Windows 64-bit, type:

     ```
     cd "C:\Program Files (x86)\Sophos\Enterprise Console\"
     ```
   - In Windows 32-bit, type:

     ```
     cd "C:\Program Files\Sophos\Enterprise Console\"
     ```
4. To back up everything, type:

   ```
   DataBackupRestore.exe -action=backup
   ```

   To display the usage options, type:

   ```
   DataBackupRestore.exe -?
   ```

   For more information about using the tool, see also Sophos knowledgebase article 114299.

You are now ready to upgrade Sophos Enterprise Console.

10.2 Upgrade Sophos Enterprise Console

Important
If you have the Sophos Management Database component installed on a separate server, you must upgrade the database component first before upgrading the management server.

You must not make any changes in Sophos Enterprise Console (for example, change policy settings) between upgrading the database and upgrading the management server.

For more information about upgrading the database on a remote server, including upgrading on a secure server using a script and upgrading in a clustered SQL Server environment, see Sophos knowledgebase article 33980.

To upgrade Sophos Enterprise Console:

1. At the computer where you want to upgrade Sophos 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 Sophos Enterprise Console installer that you downloaded earlier.

   Tip
   The installer file name includes "sec".

3. Double-click the installer.
4. A wizard guides you through the upgrade.
5. Complete the wizard.

Important
The Sophos Auditing database, **SophosSecurity**, must be present and running side by side with the other Sophos Enterprise Console databases, even if you don't intend to use the Sophos Auditing feature. This is because the database is used for enhanced access control as well as for logging audit events.

10.3 Enhance database security

Audit the database

In addition to the protection built into the Sophos Enterprise Console databases, we recommend setting additional protection at the SQL Server instance level (if not already in place) to audit user activities and changes on your SQL Server.

For example, if you are using an Enterprise edition of SQL Server 2008, you can use the SQL Server Audit feature. Earlier versions of SQL Server support login auditing, trigger-based auditing, and event auditing by using a built-in trace facility.

For more information about features that you can use for auditing activities and changes on your SQL Server system, see the documentation for your version of SQL Server. For example:

- SQL Server Audit (Database Engine)
- Auditing (Database Engine), SQL Server 2008 R2
- Auditing in SQL Server 2008
- Auditing (Database Engine), SQL Server 2008

Encrypt connections to the database

We strongly recommend that you encrypt connections between any clients and the Sophos Enterprise Console databases. For more information, see the SQL Server documentation:

- Enable Encrypted Connections to the Database Engine (SQL Server Configuration Manager)
- Encrypting Connections to SQL Server 2008 R2
- How to enable SSL encryption for an instance of SQL Server by using Microsoft Management Console

Control access to the database backups

Ensure proper, restrictive access control to any database backups or copies. This will ensure that unauthorized users cannot access the files, tamper with them, or accidentally delete them.

Note
The links in this section lead to information maintained by third parties and are provided for your convenience. Although we try to review the accuracy of the links periodically, the links may change without our knowledge.

Database connection check

When running the Sophos Enterprise Console 5.5.1 installer, database connection checks are made (prior to installation or upgrade) to establish whether a connection can be made to the database using TLS 1.2.

To ensure that TLS 1.2 is used when connecting to the database, use the **CheckDBConnection.exe** tool to provide output on the connection checks and make manual changes.

For more information, see knowledgebase article 127521.

10.4 Check existing policies

10.4.1 Check policy settings

Note
If you use role-based administration, you must have the **Computer search, protection and groups** right to perform these tasks. For more information, see the Sophos Enterprise Console Help.

To check that your policy settings have been preserved after upgrading Sophos Enterprise Console:

1. Start Sophos Enterprise Console.
2. In the **Policies** pane, double-click a policy type (for example, **Anti-virus and HIPS**).
3. Double-click the policy you want to check.
4. In the dialog box that is displayed, review the policy settings.

10.4.2 Check policies applied to computer groups

Note
If you use role-based administration, you must have the **Computer search, protection and groups** right to perform these tasks. For more information, see the Sophos Enterprise Console Help.

To check that your groups have the correct policies applied to them after upgrading Sophos Enterprise Console, do the following.

Note
Features not included in your license, which were displayed in previous versions of Sophos Enterprise Console, may no longer be displayed.

1. Start Sophos Enterprise Console.
2. In the **Groups** pane, right-click a group, and then click **View/Edit Group Policy Details**.
3. In the **Group Details** dialog box, verify that the group is assigned the right policies. If not, for a policy type, select a different policy from the drop-down list.

You have finished upgrading Sophos Enterprise Console.

11 Enable Malicious Traffic Detection

Sophos Enterprise Console 5.3.0 introduced support for Malicious Traffic Detection, which detects communications between endpoint computers and command and control servers involved in botnet or other malware attacks. If you upgraded from a version earlier than 5.3.0, or haven't enabled this feature before, you need to enable it after the upgrade to benefit from it.

Note
Malicious traffic detection is currently supported only on Windows 7 and later non-server operating systems and is first available in Sophos Endpoint Security and Control 10.6.0.

1. Check which anti-virus and HIPS policy is used by the group or groups of computers for which you want to enable the new feature.

   In the **Groups** pane, right-click the group. Select **View/Edit Group Policy Details**. In the group details dialog box, you can see the policies currently used.
2. In the **Policies** pane, double-click **Anti-virus and HIPS**.
3. Double-click the policy you want to change.
   The **Anti-Virus and HIPS policy** dialog box is displayed.
4. In the **On-access scanning** panel, make sure the **Enable behavior monitoring** check box is selected.
5. Beside **Enable behavior monitoring**, click **Configure**.
6. In the **Configure Behavior Monitoring** dialog box, make sure the **Detect malicious behavior** check box is selected.
7. To enable malicious traffic detection, select the **Detect malicious traffic** check box.

   Note
   Malicious traffic detection uses the same set of exclusions as the Sophos Anti-Virus on-access scanner (InterCheck™).

12 Technical support

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

- Visit the Sophos Community at community.sophos.com/ and search for other users who are experiencing the same problem.
- Visit the Sophos support knowledge base 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.

13 Legal notices