1 About this guide

This guide tells you how to protect your network with Sophos security software.
The guide is for you if you are installing the software for the first time.
If you are upgrading, see the Sophos Enterprise Console upgrade guide instead.

Other documents you might need
If you have a very large network, you may want to consider the installation options in the Sophos Enterprise Console advanced startup guide.

Related information
Sophos documentation
2 What do I install?

To protect your network, you install:

- Sophos Enterprise Console. This enables you to download, install and manage Sophos security software.
- Sophos security software on your endpoint computers. This protects the computers against threats and sends alerts to Sophos Enterprise Console.
You carry out these key steps:

- Download the Sophos Enterprise Console installer.
- Check the system requirements.
- Create the accounts you need.
- Prepare for installation.
- Install Sophos Enterprise Console.
- Download security software.
- Create computer groups.
- Set up security policies.
- Search for computers.
- Prepare to protect computers.
- Protect computers.
- Check the health of your network.
4 Download the Sophos Enterprise Console installer

4.1 If you have a Sophos license

1. Log in to Sophos downloads with your Sophos ID.

   Note
   If you need help with your Sophos ID, see knowledge base 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.

   Related information
   Sophos downloads
   knowledge base article 111195

4.2 If you want to evaluate Sophos Enterprise Console

1. Go to Free trial.
2. Complete the registration form.

   After you submit the registration form, your evaluation credentials will be displayed. The credentials will also be sent to the email address you entered in the registration form. You will need them when setting up Sophos Enterprise Console.

3. Click Download and download the Sophos Enterprise Console installer.

   Related information
   Free trial
5 Check the system requirements

Check the hardware, operating system and system software requirements before you begin installation.

5.1 Hardware and operating system

For hardware and operating system requirements, see the system requirements page on the Sophos website: knowledge base article 118620.

We recommend that all Sophos Enterprise Console components are installed on a dedicated single purpose machine.

We recommend you restrict the Database access and the Management Server DCOM configuration to local only.

Related information
knowledge base article 118620

5.2 Microsoft system software

Sophos Enterprise Console requires certain Microsoft system software (for example, database software).

The Sophos Enterprise Console installer attempts to install this system software if it is not already available on your server. However, in some cases, software is incompatible with your server or needs to be installed manually.

Note
After you install the required system software, you may need to restart your computers, see knowledge base article 65190.

SQL Server installation

The installer attempts to install SQL Server 2017 Express Edition. You can choose to use an existing instance of SQL Server 2008 Express R2 or later. Note that:

- We recommend that you do not install SQL Server on a domain controller.

.NET Framework installation

The installer installs .NET Framework 4.7.2, if you don't have version 4.x already installed.
Note
As part of the .NET Framework 4.7.2 installation some system services (such as IIS Admin Service) may restart.

After .NET Framework 4.7.2 is installed, you may receive a message asking you to restart your computer. If you do, we recommend that you restart the computer immediately or shortly after the installation.

Microsoft Message Queuing installation

The installer attempts to install Microsoft Message Queuing (MSMQ), if you don't have it already installed.

Note
During MSMQ installation, the following services are stopped: MSDTC, MSSQLServer, SQLSERVERAGENT. This interrupts access to the default SQL Server database. You should ensure that the services can safely be stopped during installation. You should also check that they have restarted afterwards.

Related information
knowledge base article 65190
knowledge base article 118743

5.3 Port requirements

Sophos Enterprise Console requires certain ports to be open.

Related information
knowledgebase article 38385
6 The accounts you need

Before you install Sophos software, you should create the user accounts you need.

You need the following accounts:

- **Database account.** This is a Windows user account that enables the management service to connect to the database. It is also used by other Sophos services.
  
  We recommend that you name the database account **SophosManagement**.

- **Update Manager account.** This is a Windows user account that enables your endpoint computers to access the folders where Sophos Enterprise Console puts software updates.
  
  We recommend that you name the Update Manager account **SophosUpdateMgr**.

- **Multi-factor authentication recovery account.** This is a Windows user account that is used for multi-factor authentication recovery only. After installing Sophos Enterprise Console, grant multi-factor authentication administrator rights to this user account in role-based administration. Only use this account if a multi-factor authentication device has been lost, to recover the accounts that are usually used.

  **Note**

  User accounts should not be included in the Windows Protected Users security group. Microsoft's guidelines state that service accounts should not be added to this group, see [Protected Users Security Group](#). This is not supported and you must remove user accounts from this group.

**Related information**

[Protected Users Security Group](#)

6.1 Database account

You must set up a database account.

The database account should:

- Be able to log onto the computer where you are going to install the Sophos Management Server (a component of Sophos Enterprise Console).

- Be able to read and write to the system temporary directory, for example `\windows\temp\`. By default members of **Users** have this right.

- Have a UPN (User Principal Name) associated with the account if it is a domain account.

All other rights and group memberships that it needs are granted automatically during installation.

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 installation.

- Is named **SophosManagement**.

For recommendations and step-by-step instructions, see [knowledge base article 113954](#).
6.2 Update Manager account

The Update Manager account should have read access to the folder where Sophos Enterprise Console puts software updates.

By default this is: `\servername\SophosUpdate`.

Sophos recommends that the account:

- Is not set to expire and does not have any other logon restriction.
- Is not an administrative account.
- Has a UPN (User Principal Name) associated with the account if it is a domain account.
- Is named `SophosUpdateMgr`.

For recommendations and step-by-step instructions, see knowledge base article 113954.

Related information
knowledge base article 113954
7 Prepare for installation

Prepare for installation as follows:

- Ensure that you have the Windows operating system CD and Service Pack CDs. You may be prompted for them during installation.

- If User Account Control (UAC) is enabled on the server, turn off UAC and restart the server.

Note
You can turn UAC on again after you have completed the installation and downloaded your security software.
8 Install Sophos Enterprise Console

To install Sophos Enterprise Console:

1. At the computer where you want to install 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.
3. Double-click the installer.
4. When you are prompted, click Install. 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) If the System Property Checks page is displayed, review the warnings or errors and take the necessary action. For more information about the system check results, see knowledge base article 113945.
   d) On the Database Details page, enter the details of the database account you created in Database account.
   e) On the Sophos Update Manager Credentials page, enter the details of the Update Manager account you created in Update Manager account.
6. When installation is complete, you may be prompted to restart. Click Yes or Finish.

Note
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.

Related concepts
Database account (page 7)
You must set up a database account.

Update Manager account (page 8)
The Update Manager account should have read access to the folder where Sophos Enterprise Console puts software updates.

Related information
knowledge base article 113945
9 Enhance database security

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.

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 or later, you can use the SQL Server Audit feature. Versions of SQL Server earlier than SQL Server 2008 support login auditing, trigger-based auditing, and event auditing by using a built-in trace facility.

CAUTION
You can't turn off the SQL Server auditing from Sophos Enterprise Console. Having this configuration helps you investigate if a Sophos Enterprise Console user is compromised.

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:

- Security Center for SQL Server Database Engine and Azure SQL Database
- SQL Server Audit (Database Engine)

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
- 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.

Database connection check

When running the Sophos Enterprise Console 5.5.1 or later 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 knowledge base article 127521.

**Related information**
- Security Center for SQL Server Database Engine and Azure SQL Database
- SQL Server Audit (Database Engine)
- Enable Encrypted Connections to the Database Engine
- How to enable SSL encryption for an instance of SQL Server by using Microsoft Management Console
- Knowledge base article 127521
10 Install an additional remote management console

You might want to install another instance of the Sophos Enterprise Console management console on another computer, so that you can manage networked computers conveniently.

If you do not want to, skip this section.

Note
You must install the same version of Sophos Enterprise Console as is running on your management server.

Note
The new console will need to access the server on which you installed the Sophos Enterprise Console management server. If that server runs a firewall, you might need to configure the firewall to ensure that access is possible. For instructions on how to add a firewall rule to allow DCOM traffic from the remote console to the management server, see knowledge base article 49028. We recommend that you limit the port range used by DCOM and configure the firewall to allow only these ports for communication. For reference, see Enabling COM Security Using DCOMCNFG.

To install an additional management console:

If User Account Control (UAC) (on Windows Server 2008 or later and Windows Vista or later) is turned on, turn it off and restart the computer. You can turn UAC on again after you have installed the management console.

Log on as an administrator.

• If the computer is in a domain, use a domain account that has local administrator rights.
• If the computer is in a workgroup, use a local account that has local administrator rights.

1. Find the Sophos Enterprise Console installer that you downloaded earlier and double-click it.

2. Extract the installation files to the suggested destination folder or another one of your choice. The folder must be on this computer.

An installation wizard guides you through installation. Accept the default options, except as shown below:

a) On the Components Selection page, make sure that Management Console is selected and Management Server and Database are not selected.

b) On the Management Server page, enter the name of the server on which you installed the Sophos Enterprise Console management server.

Note
If you changed the port during the management server installation, make sure that you specify the same port on this page.

c) If you are in a domain environment, enter the user account that is used to access the Sophos Enterprise Console databases.
The account is the one that you entered when you installed the Sophos Enterprise Console databases. It is the same as that used by the Sophos Management Host service on the server on which you installed the Sophos Enterprise Console management server.

When the wizard has finished, log off or restart the computer (the final page in the wizard shows which). When you log on again, Sophos Enterprise Console opens automatically. If the **Download Security Software Wizard** runs, cancel it.

If you turned off User Account Control before installation, you can now turn it on again.

To enable other users to use the additional management console:

- Add them to the **Sophos Console Administrators** group and the **Distributed COM Users** group on the server on which you have installed the management server.

- Assign them to at least one Sophos Enterprise Console role and sub-estate.

**Related information**
knowledge base article 49028
Enabling COM Security Using DCOMCNFG
11 Download protection software

When you log back on (or restart) for the first time after installation, Sophos Enterprise Console opens automatically and a wizard runs.

Note
If you used Remote Desktop for installation, the console does not open automatically. Open it from the Start menu.

The wizard guides you through selecting and downloading protection software. You should do as follows:

1. On the Sophos download account details page, enter the username and password printed on your license schedule. If you access the network via a proxy server, select the Access Sophos via a proxy server check box and enter the proxy details.
2. On the Platform selection page, select only the platforms you need to protect now. When you click Next, Sophos Enterprise Console begins downloading your software.
3. On the Downloading software page, downloading progress is displayed. Click Next at any time.
4. On the Import computers from Active Directory page, select Set up groups for your computers if you want Sophos Enterprise Console to use your existing Active Directory computer groups.

Note
For information about protecting Windows 8 computers, see knowledge base article 118261.

If you turned off User Account Control before installation, you can now turn it on again.

Related information
knowledge base article 118261
12 Create computer groups

Before you can protect and manage computers, you need to create groups for them.

To create groups:

1. If Sophos Enterprise Console is not already open, open it.
2. In the Groups pane (on the left-hand side of the console), ensure that the server name shown at the top is selected.
3. On the toolbar, click the Create group icon.
   A new group is added to the list, with its name highlighted.
4. Type a name for the group.

To create further groups, go to the left-hand pane. Select the server shown at the top if you want another top-level group. Select a group if you want a sub-group within it. Then create and name the group as before.
13 Set up security policies

Sophos Enterprise Console applies default security policies to your computer groups. You do not have to change these policies unless you want to, with these exceptions:

• If you want to use Sophos Client Firewall, we recommend that you set up the firewall policy before deploying the firewall to computers.

• You must edit the application control, device control, patch or web control policies if you want to use these features. You can do this any time.

13.1 Set up a firewall policy

Follow these instructions to set up a firewall policy.

Note
During the installation of firewall, there will be a temporary disconnection of network adapters. The interruption may cause the disconnection of networked applications, such as Remote Desktop.

By default, the firewall blocks all non-essential connections. Therefore you must configure the firewall before you protect your computers.

1. In the Policies pane, right-click Firewall, and click Create Policy.
   A New Policy is added to the list, with its name highlighted. Type the name that you want to use for the policy.

2. Double-click the policy to edit it.
   A wizard is launched.

3. In the Firewall Policy Wizard we recommend that you make the following selections.
   a) On the Configure firewall page, select Single location unless you want the firewall to use different settings according to the location where you use it.

   b) On the Operational Mode page, select Block inbound and allow outbound traffic.

   c) On the File and print sharing page, select Allow file and print sharing.
14 Search for computers

Follow these instructions to search for computers.

If you used the **Download Security Software Wizard** to set up your computer groups (based on your Active Directory groups), skip this section. Go to **Prepare to protect computers**.

You must search for computers on the network before Sophos Enterprise Console can protect and manage them.

1. Click the **Discover computers** icon in the toolbar.
2. Select the method you want to use to search for computers.
3. Enter account details if necessary and specify where you want to search.

If you use one of the **Discover** options, the computers are placed in the **Unassigned** group.

**Related concepts**

*Prepare to protect computers* (page 19)
15 Prepare to protect computers

Before you protect computers, you must prepare them as follows:

• Prepare for removal of third-party security software.
• Check that you have an account that can be used to install software.
• Prepare for installation of anti-virus software.

15.1 Prepare for removal of third-party security software

If you want the Sophos installer to remove any previously installed security software, do the following:

• If computers are running another vendor’s anti-virus software, ensure that its user interface is closed.
• If computers are running another vendor’s firewall or HIPS product, ensure that it is turned off or configured to allow the Sophos installer to run.

If computers are running another vendor’s update tool, you may want to remove it. See Remove third-party security software in Sophos Enterprise Console help.

15.2 Check that you have an account that can be used to install software

You must have a Windows user account that can be used to install software.

You will be prompted to enter details of a Windows user account that can be used to install security software. It must:

• Have local administrator rights on computers you want to protect.
• Be able to log on to the computer where you installed Sophos Enterprise Console.
• Have Read permission to the location that computers will update from. To check this location, in the Policies pane, double-click Updating, and then double-click Default.

Note

If the Policies pane (bottom left-hand side of the window) is not displayed, on the View menu, click Endpoints.

We recommend that the account:

• Is not a domain administrator account and is configured for constrained delegation.
• Has no administrative rights or any elevated privileges on the computer where Sophos Enterprise Console is installed.
• Has no Write or Modify permission to the location that computers will update from.
• Is used only for protecting computers and not used for general administrative tasks.
• Has its password changed frequently.

15.3 Prepare for installation of anti-virus software

You may need to prepare computers prior to installation of anti-virus software. We recommend that the computers being protected have a firewall enabled.

Note
After the computers have been successfully protected and appear as managed in Sophos Enterprise Console, consider disabling any firewall exceptions created specifically to allow remote deployment on the computers.
16 Protect computers

This section tells you how to:

• Protect Windows computers automatically.
• Protect Windows computers or Macs manually.
• Protect Linux computers (if your license includes this).

You can also use your own tools or scripts for installing protection on Windows computers, see knowledge base article 114191.

Related information
knowledge base article 114191

16.1 Protect Windows computers automatically

Follow these instruction to protect Windows computers.

To protect computers:

1. Select the computers you want to protect.
2. Right-click and select Protect computers.

Note
If computers are in the Unassigned group, simply drag them to your chosen groups.

3. A wizard guides you through the installation of Sophos security software. You should do as follows:
   a) On the Welcome page, click Next.
   b) On the Installation Type page, leave the option Protection software selected.
   c) On the Select features page, you can choose to install optional features.
      The current version of the firewall (included with Sophos Endpoint Security and Control 10.2 or earlier) cannot be installed on Windows 8 computers.
   d) On the Protection summary page, check for any installation problems.
   e) On the Credentials page, enter details of a Windows user account that can be used to install software on computers.

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

When installation is complete, look at the list of computers again. In the On-access column, the word Active indicates that the computer is running on-access virus scanning.

Related concepts
Troubleshooting (page 25)
When you run the Protect computers wizard, installation of security software can fail for a number of reasons.

16.2 Protect Windows computers or Macs manually

16.2.1 Locate the installers

If you have computers that you cannot protect from Sophos Enterprise Console, you can protect them by running an installer from the shared folder to which the security software has been downloaded. This folder is known as the bootstrap location.

To locate the installers:

1. In Sophos Enterprise Console, on the View menu, click Bootstrap Locations. A list of locations is displayed.
2. Make a note of the location for each operating system you want to protect.

16.2.2 Protect Windows computers manually

You can protect computers manually.

You must use an administrator account on the computers that you want to protect.

To protect computers:

1. On each computer that you want to protect, browse to the bootstrap location, find setup.exe and double-click it.
2. In the Sophos Setup dialog box, in the User account details, enter details of the Update Manager account, SophosUpdateMgr, that you created to access the share where Sophos Enterprise Console puts software updates.

   **Tip**
   You can also use any low-privilege account that can access the bootstrap location. Sophos Enterprise Console will apply an updating policy that includes the right user account details later.

**Note**
For information about command line parameters for the setup.exe file, see [knowledge base article 12570](#).

**Related concepts**
Update Manager account (page 8)
The Update Manager account should have read access to the folder where Sophos Enterprise Console puts software updates.

**Related information**
[knowledge base article 12570](#)
16.2.3 Protect Macs

You can protect Macs.

You must use an administrator account on the Macs that you want to protect.

To protect Macs:

1. On each Mac that you want to protect, browse to the bootstrap location. Copy the Sophos Installer.app installer file and the Sophos Installer Components directory to a preferred location (for example, the Desktop) and double-click it.

   A wizard guides you through installation.

2. Accept the default options. When prompted, enter the details of a user account that can install software on the Mac.

16.3 Protecting Linux computers

For details of how to protect Linux computers (if your license permits this), see Sophos Enterprise Console startup guide for Linux and UNIX.
17 Check the health of your network

You should review the health of your network regularly.

To check the health of your network from Sophos Enterprise Console, do as follows.

On the menu bar, click the **Dashboard** icon (if the dashboard is not already displayed).

The dashboard shows you how many computers:

- Have detected threats.
- Are out of date.
- Do not comply with policies.
18 Troubleshooting

When you run the Protect computers wizard, installation of security software can fail for a number of reasons.

- Automatic installation is not possible on that operating system. Perform a manual installation. For other operating systems (if your license permits you to protect them), see the Sophos Enterprise Console startup guide for Linux and UNIX.

- Operating system could not be determined. This may be because you did not enter your username in the format domain\username when finding computers.

- Firewall rules are blocking access needed to deploy the security software.
19 Get help with common tasks

This section tells you where you can find information on how to carry out common tasks.

Sophos Enterprise Console documentation can be found at Sophos documentation.

<table>
<thead>
<tr>
<th>Task</th>
<th>Document</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protect standalone computers</td>
<td>advanced startup guide: Protecting standalone computers.</td>
</tr>
<tr>
<td>Configure Sophos Enterprise Console policies</td>
<td>help: Configuring policies.</td>
</tr>
<tr>
<td>Deal with alerts</td>
<td>help: Dealing with alerts and errors.</td>
</tr>
<tr>
<td>Clean up computers</td>
<td>help: Clean up computers now.</td>
</tr>
<tr>
<td>Generate Sophos Enterprise Console reports</td>
<td>help: Generating reports.</td>
</tr>
</tbody>
</table>

Related information
Sophos documentation
20 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.
- Open a ticket with our support team at https://secure2.sophos.com/support/contact-support/support-query.aspx.
21 Legal notices

Copyright © 2009 - 2020 Sophos Limited. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the documentation can be reproduced in accordance with the license terms or you otherwise have the prior permission in writing of the copyright owner.

Sophos, Sophos Anti-Virus and SafeGuard are registered trademarks of Sophos Limited, Sophos Group and Utimaco Safeware AG, as applicable. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.