SOPHOS

Security made simple.

Sophos Enterprise Console advanced startup guide

For distributed installations

Product version: 5.5

Contents

1 About this guide

This guide describes how to install Sophos security software for the first time on a complex network or one that has more than 1000 workstations. It covers installation on Windows computers and Macs.

Note: Some features will be unavailable if your license does not include them.

If you are installing on a simple network of less than 1000 Windows and Mac workstations, see the *Sophos Enterprise Console quick startup guide* instead of this guide.

If you are installing on Linux or UNIX computers, see the *Sophos Enterprise Console startup guide for Linux and UNIX* as well as this guide.

If you are upgrading, see the *Sophos Enterprise Console upgrade guide* instead.

Sophos Enterprise Console documentation is published at www.sophos.com/en-us/support/documentation/enterprise-console.aspx.

2 Planning installation

You protect your computers by following these key steps:

1. Install Sophos Enterprise Console.
2. Download security software to a central location on your network.
3. Publish security software on a web server, if desired.
4. Create groups for computers.
5. Set up security policies for those groups.
6. Search for computers on the network and put them into groups.
7. Protect computers.
8. Check the health of your network.
9. Protect any standalone computers.

Note: If you are an Active Directory user, some steps can be handled for you automatically.

This section helps you to think about the choices that you will make at each step.

2.1 Planning the installation of Enterprise Console

Sophos Enterprise Console (SEC) enables you to install and manage security software on your computers.

Enterprise Console includes four components:

Management console	Enables you to protect and manage computers.
Management server	Handles updates and communications.
Databases	Store data about computers on the network.
Update manager	Downloads Sophos software and updates from Sophos automatically to a central location.

Management console

You might want to install another instance of the management console on another server, so that you can manage networked computers conveniently. This is related to how you want to configure role-based administration for the management console and how you want to split your IT estate into sub-estates:

- *Role-based administration* for the management console involves setting up roles, adding rights to the roles, and then assigning Windows users and groups to the roles. For example, a Help Desk engineer can update or clean up computers, but cannot configure policies, which is the responsibility of an Administrator.

- *Sub-estates* can be used to restrict the computers and groups that users can perform operations on. You can split your IT estate into sub-estates and assign management console groups of computers to the sub-estates. You can then control access to the sub-estates by assigning Windows users and groups to them. The Default sub-estate contains all management console groups and the **Unassigned** group.

This guide explains how to install an additional management console. For advice about setting up role-based administration and creating sub-estates, go to www.sophos.com/en-us/support/knowledgebase/63556.aspx.

Databases

You might want to install the databases on another server, perhaps because:

- You need more space for the databases.
- You have a dedicated SQL Server server.
- You want to spread processing load across a number of servers.

This guide explains how to install the databases either on the same server as the other Enterprise Console components or on a separate, dedicated database server.

Note: If you need to install the databases on a secure server with a script, or in a clustered SQL Server environment, go to www.sophos.com/en-us/support/knowledgebase/33980.aspx.

Important: The Sophos Auditing database, **SophosSecurity**, must be present and running side by side with the other 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.

Update manager

An update manager enables you to create shares that contain the endpoint software that you want to deploy. The computers that you want to protect update themselves from these shares. An update manager is always installed as part of Enterprise Console. By default, it places endpoint software and updates in a UNC share SophosUpdate. You can install additional update managers on other servers and create additional shares to download and deploy software on larger networks.

As a general rule, you should install an additional update manager for each 25,000 client computers on your network. We also recommend that you install an additional update manager in a remote location. This would help you to save the bandwidth when updating update shares in that location and ensure that the shares don't become incomplete if the link goes down.

If you use a UNC path for your update share, it should be used by a maximum of 1,000 computers, unless it is on a dedicated file server. If you set up a web location for updating, it can handle up to about 10,000 computers updating from it.

2.2 Planning database security

Audit the database

In addition to the protection built into the 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 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.

2.3 Planning the computer groups

You need to decide how to group the computers that you want to protect. For advice, go to www.sophos.com/en-us/support/knowledgebase/63556.aspx.

2.4 Planning the security policies

A *security policy* is a collection of settings that can be applied to the computers in a group or groups.

When you create groups, Enterprise Console applies default policies to them. You can edit these policies or create new ones, as explained in this guide. For advice about what settings to use, see the *Sophos Enterprise Console policy setup guide*.

2.5 Planning the search for networked computers

Before you can install security software on networked computers, they must be added to the computer list in Enterprise Console. For information about how to search for computers so that they are added to the computer list, see the Enterprise Console Help.

2.6 Planning how to protect computers

You can install security software automatically from Enterprise Console on Windows computers.

Note: You cannot install Sophos Client Firewall on computers running server operating systems.

If you have other operating systems on your network, you must install the software manually or by using scripts, or by another method (for example, Active Directory). This guide gives details of manual installation for the following operating systems:

- Windows
- Mac OS X

The *Sophos Enterprise Console startup guide for Linux and UNIX* gives details of manual installation for other operating systems.

3 System requirements

Tip: You can run the Enterprise Console installer to check if the server meets the requirements for the installation of Enterprise Console, even if you do not want to proceed with the installation immediately. You can view the results of the system check on the **System Property Checks** page of the installation wizard. After you have reviewed the results, click **Cancel** to close the wizard. If you need more information about the system check results, see http://www.sophos.com/en-us/support/knowledgebase/113945.aspx.

3.1 Hardware and operating system

For hardware and operating system requirements, see the system requirements page of the Sophos website (www.sophos.com/en-us/products/all-system-requirements.aspx).

3.2 Microsoft system software

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

The 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. For more information, go to https://www.sophos.com/en-us/support/knowledgebase/65190.aspx.

SQL Server installation

The installer attempts to install SQL Server 2012 Express Edition with Service Pack 2 (SP2), unless you choose to use an existing instance of SQL Server 2005 Express or later. Note that:

- We recommend that you do not install SQL Server on a domain controller.
- If you want to install the Enterprise Console databases on a separate server, ensure that the SQL Server instance can be accessed remotely. For more information, go to https://www.sophos.com/en-us/support/knowledgebase/118473.aspx.

.NET Framework installation

The installer installs .NET Framework 4.5.2, unless version 4.x is already installed.

Important: As part of the .NET Framework 4.5.2 installation some system services (such as IIS Admin Service) may restart.

After .NET Framework 4.5.2 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), unless it is already installed.

Important: 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.

3.3 Port requirements

Enterprise Console requires certain ports to be open. For more information, go to www.sophos.com/en-us/support/knowledgebase/38385.aspx.

4 The accounts you need

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

- **Database account.** This is a Windows user account that enables Enterprise Console's 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 Enterprise Console puts software updates.

  We recommend that you name the Update Manager account **SophosUpdateMgr**.

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 https://docs.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/protected-users-security-group. This is not supported and you must remove user accounts from this group.

4.1 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 Enterprise Console).
- Be able to read and write to the system temporary directory e.g. "\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, go to https://www.sophos.com/en-us/support/knowledgebase/113954.aspx.

4.2 Update Manager account

The Update Manager account should have Read access to the folder where 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, go to https://www.sophos.com/en-us/support/knowledgebase/113954.aspx.

5 Deciding where to install the Enterprise Console components

Sophos Enterprise Console (SEC) includes four components:

Management console	Enables you to protect and manage computers.
Management server	Handles updates and communications.
Databases	Store data about computers on the network.
Update manager	Downloads Sophos software and updates from Sophos automatically to a central location.

If you install the SEC components on different servers, we recommend that the servers are joined to the same domain.

We recommend that you do not install the SEC databases on a domain controller.

This guide covers two installation scenarios:

- Databases installed on a separate server
- Additional update manager installed on a separate server

In each scenario, the SEC components are distributed across the network differently.

5.1 Databases installed on a separate server

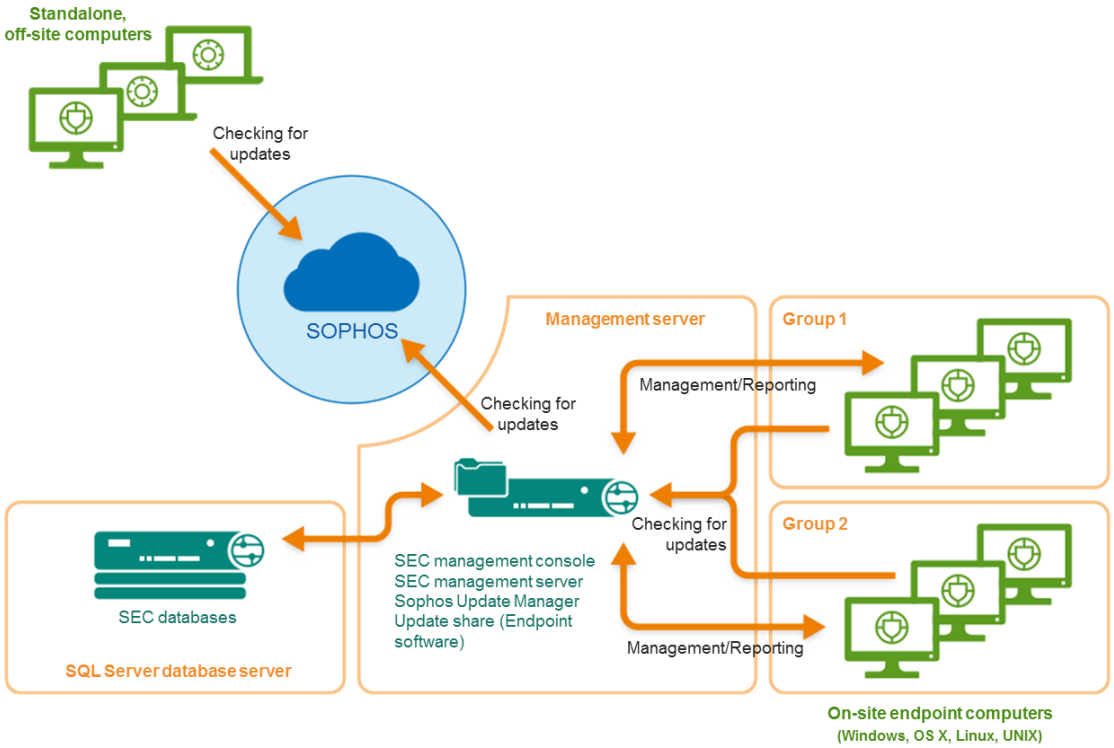

Figure 1: Deployment scenario example: Databases installed on a separate server

To follow this scenario, go to Scenario 1: Databases installed on a separate server (page 16).

5.2 Additional update manager installed on a separate server

In this scenario, there are two methods of configuring the update sources of the update managers.

The first method is to:

- Configure the main update manager that is installed alongside the SEC management console to update from Sophos directly.
- Configure the additional update manager to update from the main update manager.

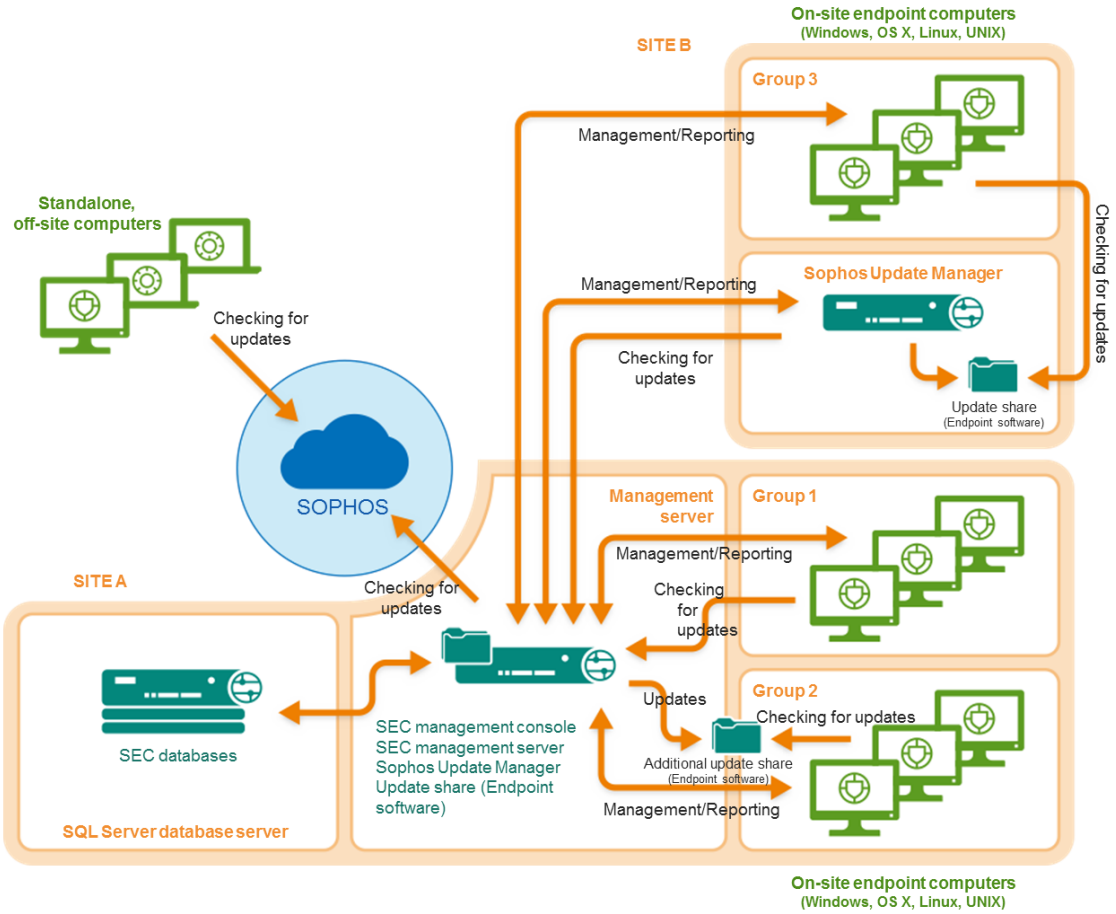

Figure 2: Deployment scenario example: Additional update manager updating from the main update manager

The second method is to:

- Configure the additional update manager to update from Sophos directly.
- Configure the update manager that is installed alongside the SEC management console to update from the additional update manager.

Regardless of which method you choose, to follow this scenario, go to Scenario 2: Additional update manager installed on a separate server (page 22).

6 Scenario 1: Databases installed on a separate server

6.1 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.

6.2 Install the SEC databases

Note: If you need to install the databases on a secure server with a script, or in a clustered SQL Server environment, go to www.sophos.com/en-us/support/knowledgebase/33980.aspx.

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

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.

1. Locate the 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 server.

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

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

   b) On the **Database Details** page, enter the details of an account that can log onto both this server and the server on which you will install the Enterprise Console management server. If the servers are in a *domain*, you can use a domain account. If the servers are in a *workgroup*, use a local account that exists on both servers. This should not be an administrator account.

Note: You created the database account in Database account (page 11).

When the Enterprise Console wizard has finished, restart the server if you are prompted to do so.

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

6.3 Install SEC: management console, management server, update manager

Go to the server on which you want to install the Enterprise Console management console, management server, and update manager. Ensure that it is connected to the internet.

The hostname of this server must be different to that of the other servers on which you install an update manager.

If User Account Control (UAC) (on Windows Server 2008 or later) is turned on, turn it off and restart the server. You can turn UAC on again after you have installed Enterprise Console and subscribed to Sophos updates.

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.

1. Locate the 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 server.

   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** and **Management Server** are selected and **Database** is not selected.

   b) On the **Database Details** page, enter the location and name of the Enterprise Console databases that you created on the other server. Enter the details of an account that can log onto both this server and the server on which you installed the Enterprise Console databases. If the servers are in a *domain*, you can use a domain account. If the servers are in a *workgroup*, use a local account that exists on both servers. This should not be an administrator account.

      Note: You created the database account in Database account (page 11).

When installation is complete, log off or restart the server (the final page in the wizard shows which). When you log on again, Enterprise Console opens automatically and the Download Security Software Wizard runs. Cancel this and run it later when instructed to do so by this guide.

6.4 Install an additional SEC 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.

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

Note: The new console will need to access the server on which you installed the 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 knowledgebase article 49028.

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. Locate the 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 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 Enterprise Console databases.

      The account is the one that you entered when you installed the Enterprise Console databases. It is the same as that used by the Sophos Management Host service on the server on which you installed the 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, 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 Enterprise Console role and sub-estate.

6.5 Downloading security software

To download security software to a central location, ready for deployment to workstations, you must configure the update manager that you installed. You can use one or both of the following methods.

Configure the update manager automatically (page 19) explains how to run a wizard, which enables you to download:

- Security software for all supported platforms.
- Only the currently recommended version.
- Only to subfolders of the share `\\`*`server name`*`\SophosUpdate`, where *server name* is the name of the server on which the update manager is installed.

Configure the update manager manually (page 20) explains how to configure the update manager directly, to enable you to download:

- Security software for all supported platforms.
- Preview or earlier versions.
- To other shares, perhaps on other servers.

6.5.1 Configure the update manager automatically

1. In Enterprise Console, on the **Actions** menu, click **Run the Download Security Software Wizard**.
2. On the **Sophos download account details** page, enter the username and password that are printed on your license schedule. If you access the internet via a proxy server, select the **Access Sophos via a proxy server** check box.
3. On the **Platform selection** page, select the platforms that you want to protect.

   When you click **Next**, Enterprise Console begins downloading your software.

4. On the **Downloading software** page, downloading progress is displayed. Click **Next** at any time.
5. On the **Import computers from Active Directory** page, select the **Set up groups for your computers** check box if you want Enterprise Console to use your existing Active Directory computer groups.

   Note: If a computer is added to more than one Active Directory container, it will cause a problem, with messages being exchanged continually between the computer and Enterprise Console.

The software that you have selected is downloaded to the share `\\server name\SophosUpdate`, where *server name* is the name of the server on which the update manager is installed.

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

Now configure the update manager manually, if necessary. Then go to Publish security software on a web server (page 32).

6.5.2 Configure the update manager manually

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

1. In Enterprise Console, on the **View** menu, click **Update Managers**.
2. If you have *not* configured the update manager automatically, configure it to use Sophos as its update source:
   a) In the **Update managers** pane, select the update manager that is installed on this server. Right-click it and click **View/Edit configuration**.
   b) In the **Configure update manager** dialog box, on the **Sources** tab, click **Add**.
   c) In the **Source Details** dialog box, in the **Address** box, select **Sophos**. In the **Username** and **Password** boxes, type the download credentials that were supplied by Sophos.
   d) If you access the update source via a proxy server, select the **Use a proxy server to connect** check box. Type the proxy server **Address** and **Port** number. In the **Username** and **Password** boxes, type the credentials that give access to the proxy server. If the username needs to be qualified to indicate the domain, use the form domain\username.
   e) Click **OK** to close the **Source Details** dialog box.

      Sophos is listed on the **Sources** tab of the **Configure update manager** dialog box.

   f) Click **OK** to close the **Configure update manager** dialog box.
3. Subscribe to the software that you want to download:
   a) In the **Software Subscriptions** pane:
      - To change an existing subscription, double-click it.
      - To add a new subscription, click **Add** at the top of the pane.

   b) In the **Software Subscription** dialog box, if you are adding a new subscription, type a name for it in the **Subscription name** box.
   c) In the platform list, select the check box next to the software that you want and in the version box select the version that you want.

      Normally, you subscribe to the **Recommended** version to ensure that your software is kept up to date automatically. For information about what other types of version are available, see the Enterprise Console Help, in the section about configuring software subscriptions.

   d) Click **OK** to close the **Software Subscription** dialog box.
   e) Repeat these steps for each subscription that you want to change or add.

4. Configure the update manager to use these subscriptions:
   a) In the **Update managers** pane, select the update manager that is installed on this server. Right-click it and click **View/Edit configuration**.
   b) In the **Configure update manager** dialog box, on the **Subscriptions** tab, make sure that the subscriptions are in the **Subscribed to** list. If not, select the subscriptions in the **Available** list and click the **>** button to move them to the **Subscribed to** list.
5. If you want to download to shares other than `\\server name\SophosUpdate`:
   a) Click the **Distribution** tab.
   b) Make sure that the subscription that you want to use is selected in the list at the top of the tab.
   c) Click **Add**.
   d) In the **Browse For Folder** dialog box, browse to one of the shares. Click **OK**.
   e) Select the share in the **Available** list and click the **>** button to move it to the **Update to** list.
   f) To enter a description for the share, or credentials to write to it, select the share and click **Configure**. In the **Share Manager** dialog box, enter the description and credentials.
   g) Repeat these steps for each share.
6. Click **OK** to close the **Configure update manager** dialog box.

   The software that you have selected is downloaded to the shares that you have specified.

You have finished installing the management tools. Now go to Publish security software on a web server (page 32).

7 Scenario 2: Additional update manager installed on a separate server

In this scenario, there are two methods of configuring the update sources of the update managers.

The first method is to:

- Configure the main update manager that is installed alongside the management console to update from Sophos directly.
- Configure the additional update manager to update from the main update manager.

The second method is to:

- Configure the additional update manager to update from Sophos directly.
- Configure the update manager that is installed alongside the management console to update from the additional update manager.

The second method can be used if you do not want to connect the main Enterprise Console server to the internet.

The method that you choose affects:

- Which servers need to be connected to the internet. In the following installation sections, you are told when the server that you are installing on needs an internet connection.
- Which method you choose to download security software to a central location, ready for deployment to workstations. Choose the appropriate section when you get to that point.
- Whether you can use the patch assessment feature in Enterprise Console. To use this feature, you must choose the first method.

7.1 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.

7.2 Install SEC: all components

Go to the server on which you want to install all components of Enterprise Console. If you want the update manager that you will install on this server to update directly from Sophos, ensure that the server is connected to the internet.

The hostname of this server must be different to that of the other servers on which you install an update manager.

If User Account Control (UAC) (on Windows Server 2008 or later) is turned on, turn it off and restart the server. You can turn UAC on again after you have installed Enterprise Console and subscribed to Sophos updates.

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.

1. Locate the 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 server.

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

   a) On the **Components Selection** page, make sure that *all* the components are selected.

   b) On the **Database Details** page, enter the details of an account that can log onto this server. If the server is in a *domain*, you can use a domain account. If the server is in a *workgroup*, use a local account that exists on the server. This should not be an administrator account.

      Note: You created the database account in Database account (page 11).

When installation is complete, log off or restart the server (the final page in the wizard shows which). When you log on again, Enterprise Console opens automatically and the Download Security Software Wizard runs. Cancel this and run it later when instructed to do so by this guide.

7.3 Install an additional SEC 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.

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

Note: The new console will need to access the server on which you installed the 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 knowledgebase article 49028.

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. Locate the 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 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 Enterprise Console databases.

      The account is the one that you entered when you installed the Enterprise Console databases. It is the same as that used by the Sophos Management Host service on the server on which you installed the 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, 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 Enterprise Console role and sub-estate.

7.4 Install an additional update manager

Important: If you want to install an additional SEC management console on the server on which you want to install an additional update manager, you must install the additional console first, as explained in Install an additional SEC management console (page 23).

Go to the server on which you want to install an additional update manager. If you want the update manager that you will install on this server to update directly from Sophos, ensure that the server is connected to the internet.

The hostname of this server must be different to that of the other servers on which you install an update manager.

If Network Discovery (on Windows Server 2008 or later) is turned off, turn it on and restart the server.

If User Account Control (UAC) (on Windows Server 2008 or later) is turned on, turn it off and restart the server. You can turn UAC on again after you have installed the update manager and subscribed to Sophos updates.

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.

1. Find the `SUMInstallSet` shared folder on the server on which you installed Enterprise Console.
2. Double-click `Setup.exe` to run the installer.

   An installation wizard guides you through installation. Accept the default options.

You have installed an update manager that is managed by Enterprise Console.

7.5 Downloading security software

In this scenario, there are two methods of configuring the update sources of the update managers. Choose the one that is most appropriate for you:

- Main update manager updating from Sophos (page 25)
- Additional update manager updating from Sophos (page 29)

7.5.1 Main update manager updating from Sophos

Configuring the main update manager to update from Sophos

You must configure the main update manager that you installed alongside the SEC management console to update from Sophos directly. You can use one or both of the following methods.

Configure the main update manager automatically (page 26) explains how to run a wizard, which enables you to download:

- Security software for all supported platforms.
- Only the latest version.
- Only to subfolders of the share `\\`*`server name`*`\SophosUpdate`, where *server name* is the name of the server on which the main update manager is installed.

Configure the main update manager manually (page 26) explains how to configure the main update manager directly, to enable you to download:

- Security software for all supported platforms.
- Earlier versions.

- To other shares, perhaps on other servers.

For information about what other types of version are available, see the Enterprise Console Help, in the section about configuring subscriptions.

Configuring the additional update manager to update from the main update manager

Configure the additional update manager (page 28) explains how to configure the additional update manager to update from the main update manager.

7.5.1.1 Configure the main update manager automatically

1. In Enterprise Console, on the **Actions** menu, click **Run the Download Security Software Wizard**.
2. On the **Sophos download account details** page, enter the username and password that are printed on your license schedule. If you access the internet via a proxy server, select the **Access Sophos via a proxy server** check box.
3. On the **Platform selection** page, select the platforms that you want to protect.

   When you click **Next**, Enterprise Console begins downloading your software.

4. On the **Downloading software** page, downloading progress is displayed. Click **Next** at any time.
5. On the **Import computers from Active Directory** page, select the **Set up groups for your computers** check box if you want Enterprise Console to use your existing Active Directory computer groups.

   Note: If a computer is added to more than one Active Directory container, it will cause a problem, with messages being exchanged continually between the computer and Enterprise Console.

The software that you have selected is downloaded to the share `\\`*`server name`*`\SophosUpdate`, where *server name* is the name of the server on which the update manager is installed.

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

Now configure the update manager manually, if necessary. Then go to Configure the additional update manager (page 28).

7.5.1.2 Configure the main update manager manually

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

1. In Enterprise Console, on the **View** menu, click **Update Managers**.

2. If you have *not* configured the update manager automatically, configure it to use Sophos as its update source:

   a) In the **Update managers** pane, select the update manager that is installed on this server. Right-click it and click **View/Edit configuration**.

   b) In the **Configure update manager** dialog box, on the **Sources** tab, click **Add**.

   c) In the **Source Details** dialog box, in the **Address** box, select **Sophos**. In the **Username** and **Password** boxes, type the download credentials that were supplied by Sophos.

   d) If you access the update source via a proxy server, select the **Use a proxy server to connect** check box. Type the proxy server **Address** and **Port** number. In the **Username** and **Password** boxes, type the credentials that give access to the proxy server. If the username needs to be qualified to indicate the domain, use the form domain\username.

   e) Click **OK** to close the **Source Details** dialog box.

      Sophos is listed on the **Sources** tab of the **Configure update manager** dialog box.

   f) Click **OK** to close the **Configure update manager** dialog box.

3. Subscribe to the software that you want to download:

   a) In the **Software Subscriptions** pane:

      - To change an existing subscription, double-click it.
      - To add a new subscription, click **Add** at the top of the pane.

   b) In the **Software Subscription** dialog box, if you are adding a new subscription, type a name for it in the **Subscription name** box.

   c) In the platform list, select the check box next to the software that you want and in the version box select the version that you want.

      Normally, you subscribe to the **Recommended** version to ensure that your software is kept up to date automatically. For information about what other types of version are available, see the Enterprise Console Help, in the section about configuring software subscriptions.

   d) Click **OK** to close the **Software Subscription** dialog box.

   e) Repeat these steps for each subscription that you want to change or add.

4. Configure the update manager to use these subscriptions:

   a) In the **Update managers** pane, select the update manager that is installed on this server. Right-click it and click **View/Edit configuration**.

   b) In the **Configure update manager** dialog box, on the **Subscriptions** tab, make sure that the subscriptions are in the **Subscribed to** list. If not, select the subscriptions in the **Available** list and click the **>** button to move them to the **Subscribed to** list.

5. Click **OK** to close the **Configure update manager** dialog box.

   The software that you have selected is downloaded to the update manager that is installed on this server.

7.5.1.3 Configure the additional update manager

1. In Enterprise Console, on the **View** menu, click **Update Managers**.
2. Configure the additional update manager to use the main update manager as its update source:
   a) In the **Update managers** pane, select the additional update manager. Right-click it and click **View/Edit configuration**.
   b) In the **Configure update manager** dialog box, on the **Sources** tab, click **Add**.
   c) In the **Source Details** dialog box, in the **Address** box, select the share to which the main update manager downloads software.

      The **Username** and **Password** boxes are automatically populated with the credentials that are needed to access this share.

   d) If you access the update source via a proxy server, select the **Use a proxy server to connect** check box. Type the proxy server **Address** and **Port** number. In the **Username** and **Password** boxes, type the credentials that give access to the proxy server. If the username needs to be qualified to indicate the domain, use the form domain\username.
   e) Click **OK** to close the **Source Details** dialog box.

      The share to which the main update manager downloads software is listed on the **Sources** tab of the **Configure update manager** dialog box.

3. Configure the update manager to use the subscriptions that you set up earlier:
   - On the **Subscriptions** tab, make sure that the subscriptions are in the **Subscribed to** list. If not, select the subscriptions in the **Available** list and click the **>** button to move them to the **Subscribed to** list.
4. If you want to download to shares other than `\\server name\SophosUpdate`:
   a) Click the **Distribution** tab.
   b) Make sure that the subscription that you want to use is selected in the list at the top of the tab.
   c) Click **Add**.
   d) In the **Browse For Folder** dialog box, browse to one of the shares. Click **OK**.
   e) Select the share in the **Available** list and click the **>** button to move it to the **Update to** list.
   f) To enter a description for the share, or credentials to write to it, select the share and click **Configure**. In the **Share Manager** dialog box, enter the description and credentials.
   g) Repeat these steps for each share.
5. Click **OK** to close the **Configure update manager** dialog box.

   The software that you have selected is downloaded to the shares that you have specified during the next scheduled update.

You have finished installing the management tools. Now go to Publish security software on a web server (page 32).

7.5.2 Additional update manager updating from Sophos

Configure the additional update manager (page 29) explains how to configure the additional update manager to update from Sophos directly.

Configure the main update manager (page 30) explains how to configure the main update manager that you installed alongside the SEC management console to update from the additional update manager.

7.5.2.1 Configure the additional update manager

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

1. In Enterprise Console, on the **View** menu, click **Update Managers**.
2. Configure the additional update manager to use Sophos as its update source:
   a) In the **Update managers** pane, select the additional update manager. Right-click it and click **View/Edit configuration**.
   b) In the **Configure update manager** dialog box, on the **Sources** tab, click **Add**.
   c) In the **Source Details** dialog box, in the **Address** box, select **Sophos**. In the **Username** and **Password** boxes, type the download credentials that were supplied by Sophos.
   d) If you access the update source via a proxy server, select the **Use a proxy server to connect** check box. Type the proxy server **Address** and **Port** number. In the **Username** and **Password** boxes, type the credentials that give access to the proxy server. If the username needs to be qualified to indicate the domain, use the form domain\username.
   e) Click **OK** to close the **Source Details** dialog box.

      Sophos is listed on the **Sources** tab of the **Configure update manager** dialog box.

   f) Click **OK** to close the **Configure update manager** dialog box.
3. Subscribe to the software that you want to download:
   a) In the **Software Subscriptions** pane:
      - To change an existing subscription, double-click it.
      - To add a new subscription, click **Add** at the top of the pane.

   b) In the **Software Subscription** dialog box, if you are adding a new subscription, type a name for it in the **Subscription name** box.
   c) In the platform list, select the check box next to the software that you want and in the version box select the version that you want.

      Normally, you subscribe to the **Recommended** version to ensure that your software is kept up to date automatically. For information about what other types of version are available, see the Enterprise Console Help, in the section about configuring software subscriptions.

   d) Click **OK** to close the **Software Subscription** dialog box.
   e) Repeat these steps for each subscription that you want to change or add.

4. Configure the update manager to use these subscriptions:
   a) In the **Update managers** pane, select the additional update manager. Right-click it and click **View/Edit configuration**.
   b) In the **Configure update manager** dialog box, on the **Subscriptions** tab, make sure that the subscriptions are in the **Subscribed to** list. If not, select the subscriptions in the **Available** list and click the **>** button to move them to the **Subscribed to** list.
5. Click **OK** to close the **Configure update manager** dialog box.

   The software that you have selected is downloaded to the additional update manager.

7.5.2.2 Configure the main update manager

1. In Enterprise Console, on the **View** menu, click **Update Managers**.
2. Configure the main update manager to use the additional update manager as its update source:
   a) In the **Update managers** pane, select the update manager that is installed on this server. Right-click it and click **View/Edit configuration**.
   b) In the **Configure update manager** dialog box, on the **Sources** tab, click **Add**.
   c) In the **Source Details** dialog box, in the **Address** box, select the share to which the additional update manager downloads software.

      The **Username** and **Password** boxes are automatically populated with the credentials that are needed to access this share.

   d) If you access the update source via a proxy server, select the **Use a proxy server to connect** check box. Type the proxy server **Address** and **Port** number. In the **Username** and **Password** boxes, type the credentials that give access to the proxy server. If the username needs to be qualified to indicate the domain, use the form domain\username.
   e) Click **OK** to close the **Source Details** dialog box.

      The share to which the additional update manager downloads software is listed on the **Sources** tab of the **Configure update manager** dialog box.

3. Configure the update manager to use the subscriptions that you set up earlier:
   - On the **Subscriptions** tab, make sure that the subscriptions are in the **Subscribed to** list. If not, select the subscriptions in the **Available** list and click the **>** button to move them to the **Subscribed to** list.

4. If you want to download to shares other than `\\server name\SophosUpdate`:
   a) Click the **Distribution** tab.
   b) Make sure that the subscription that you want to use is selected in the list at the top of the tab.
   c) Click **Add**.
   d) In the **Browse For Folder** dialog box, browse to one of the shares. Click **OK**.
   e) Select the share in the **Available** list and click the **>** button to move it to the **Update to** list.
   f) To enter a description for the share, or credentials to write to it, select the share and click **Configure**. In the **Share Manager** dialog box, enter the description and credentials.
   g) Repeat these steps for each share.
5. Click **OK** to close the **Configure update manager** dialog box.

   The software that you have selected is downloaded to the shares that you have specified during the next scheduled update.

You have finished installing the management tools. Now go to Publish security software on a web server (page 32).

8 Publish security software on a web server

You might want to publish Sophos security software on a web server for computers to access via HTTP. This can be especially useful for computers that are not always connected to the network.

- To publish security software on a web server, go to www.sophos.com/en-us/support/knowledgebase/38238.aspx.

9 Create computer groups

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 Setting up security policies (page 34).

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

1. If the **Groups** pane (left-hand side of the window) is not displayed, on the **View** menu, click **Endpoints**.
2. Click anywhere within the **Groups** pane. Ensure that the **Unassigned** group is not selected.
3. On the **Groups** menu, click **Create Group**.

   A **New Group** is added in the left-hand pane, with its name highlighted.
4. Enter the name that you want to use for the group.
5. To create another top-level group, select the server shown at the top of the **Groups** pane, and repeat steps 3 and 4.

   To create a sub-group of an existing group, select the existing group, and repeat steps 3 and 4.

10 Setting up security policies

A *security policy* is a collection of settings that can be applied to the computers in a group or groups.

Enterprise Console applies default policies to your computer groups. This section explains:

- What the default policies are and whether you need to change them.
- How to create or edit a policy.
- How to apply a policy to your computer groups.

10.1 Default policies

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:

- You must set up a firewall policy now.
- You must edit the application control, data control, device control, tamper protection, patch, exploit prevention or web control policies if you want to use these features. You can do this any time.

For recommended policy settings, see the *Sophos Enterprise Console policy setup guide*.

10.2 Set up a firewall policy

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 printer sharing** page, select **Allow file and printer sharing**.

10.3 Create or edit a policy

1. In Enterprise Console, if the **Policies** pane (bottom left-hand side of the window) is not displayed, on the **View** menu, click **Endpoints**.
2. In the **Policies** pane, do one of the following:
   - To create a new policy, right-click the type of policy that you want to create, for example **Updating**, and click **Create Policy**.
   - To edit a default policy, double-click the type of policy that you want to edit. Then select **Default**.

   If you created a policy, a **New Policy** is added to the list, with its name highlighted. Type the name that you want to use for the policy.
3. Double-click the policy. Enter the settings that you want.

If you created a policy, you need to apply your policy to a computer group.

10.4 Apply a policy to a group

- In the **Policies** pane, drag the policy to the group to which you want to apply the policy.

  Note: Alternatively, you can right-click a group and select **View/Edit Group Policy Details**. You can then select policies for that group from drop-down menus.

11 Search for computers

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

1. If the **Groups** pane (left-hand side of the window) is not displayed, on the **View** menu, click **Endpoints**.
2. On the **Actions** menu, click **Discover Computers**.
3. Select the method that you want to use to search for computers.
4. 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.

12 Preparing to protect computers

12.1 Prepare for removal of third-party software

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

1. On computers that are running another vendor's anti-virus software, ensure that the anti-virus software user interface is closed.

   Note: HitmanPro.Alert may already be installed either as a standalone product or from Sophos Central. You should remove HitmanPro.Alert before applying on-premise management from Sophos Enterprise Console.

2. On computers that are running another vendor's firewall or HIPS product, ensure that the firewall or HIPS product 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. For more information, see the Enterprise Console Help.

12.2 Check that you have an 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 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 computers where Enterprise Console, additional update managers, or message relays are 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.

12.3 Prepare for installation of anti-virus software

You may need to prepare computers prior to installation of anti-virus software. For advice, see the Sophos endpoint deployment guide (https://docs.sophos.com/esg/enterprise-console/tools/deployment_guide/en-us/index.html), the section about preparing computers for deployment.

We recommend that the computers being protected have a firewall enabled.

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

13 Protecting computers

13.1 Protect Windows computers automatically

This section describes how to use Enterprise Console to protect Windows computers automatically.

You can also use your own tools or scripts for installing protection on Windows computers. For details, go to www.sophos.com/en-us/support/knowledgebase/114191.aspx.

Note: When you install Sophos Client Firewall, all network adapters are temporarily disconnected. This results in network connections being unavailable for up to 20 seconds and the disconnection of networked applications such as Microsoft Remote Desktop.

1. In Enterprise Console, select the computers that you want to protect.
2. Do one of the following:
   - If the computers have been placed in groups, right-click the selection and click **Protect computers**.
   - If the computers are in the **Unassigned** group, simply drag them to your chosen groups.

   A wizard guides you through installation of Sophos security software. Accept the default options, except as shown below:

   a) On the **Select features** page, select additional features you want to install.

   b) On the **Protection summary** page, check the details of any installation problems. For help, see Troubleshooting (page 39).

   c) On the **Credentials** page, enter details of an account that can be used to install software on computers.

The computers that you have selected are protected with security software. Installation is staggered, so that the process may not be complete on all the computers for some time. Some computers might need to be restarted to complete the installation.

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

13.1.1 Troubleshooting

When you try to protect Windows computers automatically, installation of security software can fail for a number of reasons:

- Automatic installation is not possible on that operating system. Perform a manual installation. See Protect Windows computers or Macs manually (page 40). For other operating systems, see the later sections of this guide.
- The 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.

- On Windows XP computers, Simple File Sharing has not been turned off.
- On Windows Vista computers, Sharing Wizard has not been turned off.
- You selected to install a feature that is not supported on that operating system.

13.2 Protect Windows computers or Macs manually

If you have computers that you cannot protect automatically, you 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.

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

To protect Windows computers or Macs manually:

1. In Enterprise Console, on the **View** menu, click **Bootstrap Locations**.

   A list of locations is displayed. Make a note of the location for each operating system you want to protect.

2. At each computer that you want to protect, browse to the bootstrap location and do as follows:

   - For Windows computers, find `setup.exe` and double-click it.
   - For Macs, 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. Accept the default options, except as shown below:

   - On Windows computers, in the **User account details**, enter details of the account that you specified for access to Update Manager. You did this when you installed Enterprise Console, in Update Manager account (page 11).

     Tip: If you're not sure which account this is, use any low-privilege account that can access the bootstrap location. Enterprise Console will apply an updating policy that includes the right user account details later.

13.3 Protect Linux or UNIX computers

For details of how to protect Linux or UNIX computers, see the *Enterprise Console startup guide for Linux and UNIX*.

14 Check the health of your network

To check the health of your network from Enterprise Console:

1. View the Enterprise Console Dashboard.
   If it is not already displayed, on the **View** menu, click **Dashboard**.

   The Dashboard shows you how many computers:

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

15 Protecting standalone computers

Some computers are never on the network and are not easy to access, for example computers that staff use at home. To protect these computers, you ask each user to install Sophos security software individually using a “standalone” installer. The software is then kept up to date via the internet. There are two possible approaches:

- The user can download the software from www.sophos.com/en-us/support/downloads/standalone-installers/esc-for-windows-2000-up.aspx. They install the software and configure it to update from Sophos.
- You can republish the software and all subsequent updates on your own website. The user downloads the software from that website, installs it, and configures it to update from that website. For information on how to republish Sophos updates on your own website, go to www.sophos.com/en-us/support/knowledgebase/38238.aspx.

15.1 Send standalone users the information they need

Send any users who are not on your network the following:

- The location from which they can download the security software (unless you are providing it on CD).
- The *Sophos Endpoint Security and Control standalone startup guide*.
- The username and password that they need (whether they are downloading from Sophos directly or from your own website).

When you send the username and password:

- Do not send them to an infected computer by email, as they might be stolen.
- If necessary, send them by fax or letter post.

16 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 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.

17 Legal notices

ACE™, TAO™, CIAO™, DAnCE™, and CoSMIC™

DOC software is provided with no support and without any obligation on the part of Washington University, UC Irvine, Vanderbilt University, their employees, or students to assist in its use, correction, modification, or enhancement. A number of companies around the world provide commercial support for DOC software, however. DOC software is Y2K-compliant, as long as the underlying OS platform is Y2K-compliant. Likewise, DOC software is compliant with the new US daylight savings rule passed by Congress as "The Energy Policy Act of 2005," which established new daylight savings times (DST) rules for the United States that expand DST as of March 2007. Since DOC software obtains time/date and calendaring information from operating systems users will not be affected by the new DST rules as long as they upgrade their operating systems accordingly.

The names ACE™, TAO™, CIAO™, DAnCE™, CoSMIC™, Washington University, UC Irvine, and Vanderbilt University, may not be used to endorse or promote products or services derived from this source without express written permission from Washington University, UC Irvine, or Vanderbilt University. This license grants no permission to call products or services derived from this source ACE™, TAO™, CIAO™, DAnCE™, or CoSMIC™, nor does it grant permission for the name Washington University, UC Irvine, or Vanderbilt University to appear in their names.

If you have any suggestions, additions, comments, or questions, please let me know.

Douglas C. Schmidt

Apache

The Sophos software that is described in this document may include some software programs that are licensed (or sublicensed) to the user under the Apache License. A copy of the license agreement for any such included software can be found at http://www.apache.org/licenses/LICENSE-2.0

Boost Software License

Permission is hereby granted, free of charge, to any person or organization obtaining a copy of the software and accompanying documentation covered by this license (the "Software") to use, reproduce, display, distribute, execute, and transmit the Software, and to prepare derivative works of the Software, and to permit third-parties to whom the Software is furnished to do so, all subject to the following:

The copyright notices in the Software and this entire statement, including the above license grant, this restriction and the following disclaimer, must be included in all copies of the Software, in whole or in part, and all derivative works of the Software, unless such copies or derivative works are solely in the form of machine-executable object code generated by a source language processor.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Common Public License

The Sophos software that is referenced in this document includes or may include some software programs that are licensed (or sublicensed) to the user under the Common Public License (CPL), which, among other rights, permits the user to have access to the source code. The CPL requires for any software licensed under the terms of the CPL, which is distributed in object code form, that the source code for such software also be made available to the users of the object code form. For any such software covered under the CPL, the source code is available via mail order by submitting a request to Sophos; via email to support@sophos.com or via the web at https://www.sophos.com/en-us/support/contact-support.aspx. A copy of the license agreement for any such included software can be found at http://opensource.org/licenses/cpl1.0.php

ConvertUTF

Copyright 2001–2004 Unicode, Inc.

This source code is provided as is by Unicode, Inc. No claims are made as to fitness for any particular purpose. No warranties of any kind are expressed or implied. The recipient agrees to determine applicability of information provided. If this file has been purchased on magnetic or optical media from Unicode, Inc., the sole remedy for any claim will be exchange of defective media within 90 days of receipt.

Unicode, Inc. hereby grants the right to freely use the information supplied in this file in the creation of products supporting the Unicode Standard, and to make copies of this file in any form for internal or external distribution as long as this notice remains attached.

Loki

The MIT License (MIT)

Copyright © 2001 by Andrei Alexandrescu

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Microsoft Public License (MS-PL)

This license governs use of the accompanying software. If you use the software, you accept this license. If you do not accept the license, do not use the software.

1. Definitions

   The terms "reproduce," "reproduction," "derivative works," and "distribution" have the same meaning here as under U.S. copyright law.

   A "contribution" is the original software, or any additions or changes to the software.

   A "contributor" is any person that distributes its contribution under this license.

   "Licensed patents" are a contributor's patent claims that read directly on its contribution.

2. Grant of Rights

   (A) Copyright Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free copyright license to reproduce its contribution, prepare derivative works of its contribution, and distribute its contribution or any derivative works that you create.

   (B) Patent Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free license under its licensed patents to make, have made, use, sell, offer for sale, import, and/or otherwise dispose of its contribution in the software or derivative works of the contribution in the software.

3. Conditions and Limitations

   (A) No Trademark License- This license does not grant you rights to use any contributors' name, logo, or trademarks.

   (B) If you bring a patent claim against any contributor over patents that you claim are infringed by the software, your patent license from such contributor to the software ends automatically.

   (C) If you distribute any portion of the software, you must retain all copyright, patent, trademark, and attribution notices that are present in the software.

   (D) If you distribute any portion of the software in source code form, you may do so only under this license by including a complete copy of this license with your distribution. If you distribute any portion of the software in compiled or object code form, you may only do so under a license that complies with this license.

   (E) The software is licensed "as-is." You bear the risk of using it. The contributors give no express warranties, guarantees or conditions. You may have additional consumer rights under your local laws which this license cannot change. To the extent permitted under your local laws, the contributors exclude the implied warranties of merchantability, fitness for a particular purpose and non-infringement.

A copy of the MS-PL terms can be found at https://opensource.org/licenses/MS-PL.

OpenSSL Cryptography and SSL/TLS Toolkit

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually

both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL license

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

   “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)”

4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

   “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay license

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscape’s SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this

distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

   The word "cryptographic" can be left out if the routines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

   "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

WilsonORMapper

Copyright © 2007, Paul Wilson

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Windows Template Library (WTL)

Copyright © Microsoft Corporation. All rights reserved.

The use and distribution terms for this software are covered by the Common Public License. Source code for this component is available here: https://sourceforge.net/projects/wtl/files/

zlib data compression library

Copyright © 1995–2013 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly jloup@gzip.org

Mark Adler madler@alumni.caltech.edu