SOPHOS

Cybersecurity made simple.

Sophos Enterprise Console

advanced startup guide

product version: 5.5

Contents

1 About this guide

This guide tells you how to upgrade to .

2 Planning installation

You protect your computers by following these key steps:

1. Install .
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

(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 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 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 . 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 .

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 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

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

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

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).

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

3.2 Microsoft system software

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

The 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 4 (SP4), 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.

.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

requires certain ports to be open. For more information, go to http://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 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 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).
- 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 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 components

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 components on different servers, we recommend that the servers are joined to the same domain.

We recommend that you do not install the 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 components are distributed across the network differently.

5.1 Databases installed on a separate server

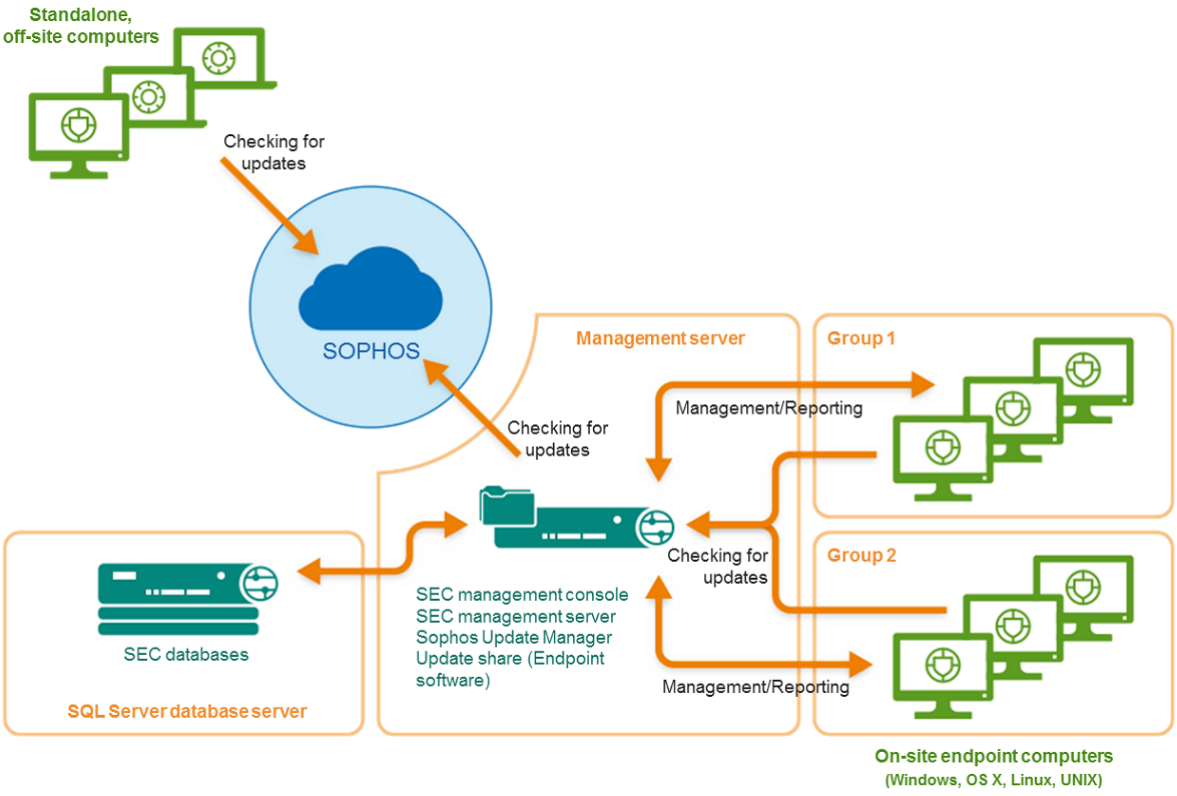

Figure 1: Deployment scenario example: Databases installed on a separate server

To follow this scenario, go to Download the installer (page 13).

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.

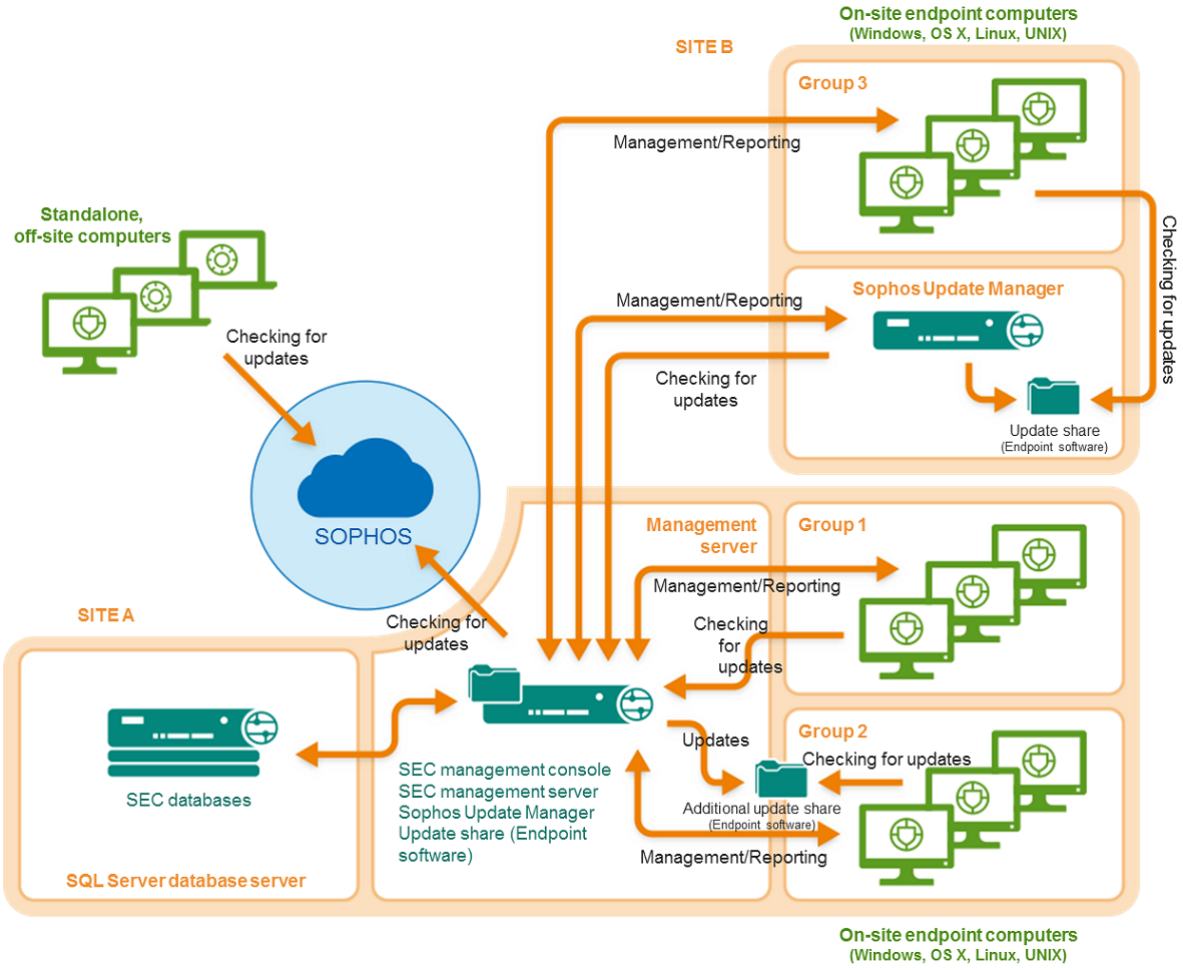

Figure 2: Deployment scenario example: Additional update manager updating from the main update manager

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 19).

6 Scenario 1: Installing the management tools with the databases 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 and download the installer.

6.2 Install the 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 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 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 8).

When the 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 : management console, management server, update manager

Go to the server on which you want to install the 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 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 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 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 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 8).

When installation is complete, log off or restart the server (the final page in the wizard shows which). When you log on again, 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 remote management console

You might want to install another instance of the 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 as is running on your management server.

Note
The new console will need to access the server on which you installed the management server. If that server runs a 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.

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 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 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 databases.

      The account is the one that you entered when you installed the databases. It is the same as that used by the Sophos Management Host service on the server on which you installed the 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, 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 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 16) 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 17) 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 , 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**, 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 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 .

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 , you can now turn it on again.

Now configure the update manager manually, if necessary.

6.5.2 Configure the update manager manually

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

1. In , 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 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 Create computer groups (page 28).

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 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 and download the installer.

7.2 Install SEC: all components

Go to the server on which you want to install all components of . 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 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 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 8).

When installation is complete, log off or restart the server (the final page in the wizard shows which). When you log on again, 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 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 as is running on your management server.

Note
The new console will need to access the server on which you installed the management server. If that server runs a 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.

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 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 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 databases.

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

7.4 Install an additional update manager

Important
If you want to install an additional 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 20).

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 .
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 .

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 22)
- Additional update manager updating from Sophos (page 25)

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 23) 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 23) 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 Help.

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

Configure the additional update manager (page 24) explains how to configure the additional update manager to update from the main update manager.

Configure the main update manager automatically

1. In , 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**, 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 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 .

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 , you can now turn it on again.

Now configure the update manager manually, if necessary. Then go to Configure the additional update manager (page 24).

Configure the main update manager manually

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

1. In , 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 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.

Configure the additional update manager

1. In , 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.

7.5.2 Additional update manager updating from Sophos

Additional update manager updating from Sophos (page 25) explains how to configure the additional update manager to update from Sophos directly.

Configure the main update manager (page 26) explains how to configure the main update manager that you installed alongside the SEC management console to update from the additional update manager.

Configure the additional update manager

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

1. In , 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 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.

Configure the main update manager

1. In , 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.

8 Create computer groups

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

1. If 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.

9 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.

9.1 Default policies

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 .

9.2 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**.

9.3 Create or edit a policy

1. In , 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.

9.4 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.

10 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.

You must search for computers on the network before 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.

11 Preparing to protect computers

11.1 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.

11.2 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 , consider disabling any firewall exceptions created specifically to allow remote deployment on the computers.

12 Protecting Windows computers and Macs

12.1 Protect Windows computers automatically

This section describes how to use Sophos 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 , 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 , 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 33).

   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.

12.1.1 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 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.

12.2 Protect Windows computers or Macs manually

12.2.1 Protect Windows computers manually

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

1. At 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 puts software updates. You did this in Update Manager account (page 8).

Tip
You can also use any low-privilege account that can access the bootstrap location. 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 https://www.sophos.com/en-us/support/knowledgebase/12570.aspx.

12.2.2 Protect Macs

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

1. At 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.

12.3 Protect Linux computers

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

13 Check the health of your network

To check the health of your network from , 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.

14 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.

14.1 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 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.

15 Technical support

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

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

16 Legal notices