

SOPHOS

Sophos Endpoint Security and Control network startup guide

Document date: June 2009



Contents

1 About this guide.....	4
2 Plan installation.....	5
3 System requirements.....	9
4 Install the management tools.....	10
5 Download software and set up updating.....	12
6 Set up a remote management console.....	14
7 Create groups for your computers.....	16
8 Set up policies.....	17
9 Search for computers and add them to groups.....	20
10 Protect computers.....	21
11 Check computers are protected.....	25
12 Ensure new computers will be protected automatically.....	26
13 Set up a firewall policy.....	27
14 Detect suspicious behavior.....	28
15 Scan for suspicious files.....	30
16 Scan for adware and potentially unwanted applications (PUAs).....	31
17 Scan for controlled applications.....	33
18 Set up network access control.....	35
19 Check the health of your network.....	36
20 Clean up viruses, PUAs and suspicious files.....	38
21 Protect Windows computers with manual installation.....	39
22 Protect Mac OS X computers.....	40
23 Protect Linux computers.....	41
24 Protect NetWare servers.....	44
25 Protect UNIX computers with Sophos Anti-Virus version 4.....	47

26	Protect UNIX computers with Sophos Anti-Virus version 7.....	49
27	Protect standalone computers.....	55
28	Protect computers with a command-line installation.....	56
29	Protect computers with a script.....	57
30	Appendix: Advanced setup.....	59
31	Technical support.....	65
32	Copyright.....	66

1 About this guide

This guide is for customers who

- Want to install Sophos software for the first time or reinstall it.
- Have a Windows-based network (workgroups or domains).
- Have Windows, Mac, Linux, NetWare or UNIX computers on that network.

If this does not describe you, you need a different guide, as shown below.

If you are upgrading from earlier versions of the software, see the *Sophos Endpoint Security and Control network upgrade guide*.

If you have a NetWare-based network, that is, you do not use Microsoft networking, see the *Sophos Endpoint Security and Control network startup guide: NetWare edition*.

You can find Sophos documentation on the Sophos website (www.sophos.com/support/docs/) or on the User documentation page of the Sophos Endpoint Security and Control Network Install CD.

2 Plan installation

You protect your computers with the following key steps:

- Install the Sophos management tools.
- Set up automatic downloading of Sophos software and updates.
- Create groups for computers.
- Set up security policies for those groups.
- Search for computers on the network and put them into groups.
- Protect computers.

Note: If you are an Active Directory user, some steps can be handled for you automatically, as indicated in the sections below.

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

2.1 Plan the installation of management tools

The Sophos management tools are:

- Sophos Enterprise Console.
- Sophos NAC server.
- Sophos role-based administration tools.

2.1.1 Sophos Enterprise Console

Sophos Enterprise Console includes four components:

Management console	Enables you to protect and manage computers.
Management server	Handles updating and communications.
Database	Stores data about computers on the network.
EM Library	Downloads updates from Sophos automatically.

This guide assumes that you:

- Place all the components on one computer.
- Install another copy of the management console on a workstation, so that you can manage networked computers conveniently.

Note: You can install some components separately, for example, you may want to install the database on a server with plenty of space. In that case, see the *Sophos Endpoint Security and Control large networks configuration guide*.

2.1.2 Sophos NAC server

If you want to use Sophos Network Access Control, you need to install the Sophos NAC server.

You can install the Sophos NAC server and Enterprise Console on the same computer or on separate computers. If you have more than 1000 computers, you should do the latter.

The order in which you install the management tools depends on the type of database you want to use.

- If you want to use an MSDE database for both tools, you must install Enterprise Console first.
- If you want to use SQL server, you can install Sophos NAC first.

For information about installing Sophos NAC, see the *Sophos NAC for Endpoint Security and Control installation guide*.

2.1.3 Sophos role-based administration tools

Role-based administration allows you to specify which computers a user can access and which tasks they can carry out, depending on their role in your organization.

Sophos provides two role-based administration tools:

Sophos Helpdesk Console

This console enables a user, such as an IT help desk administrator, to monitor selected parts of your network and to carry out remedial actions.

Sophos Enterprise Read-only Console

This console enables a user to monitor your network and generate reports, but not to carry out any remedial actions.

For information on how to install and run these consoles, see *Sophos Endpoint Security and Control role-based administration guide*.

2.2 Plan how to set up automatic downloading and updating

Enterprise Console downloads the latest software to a “software library” and places it in central installation directories. This makes it available to networked computers.

This guide describes how to set up a single software library and a default set of central installation directories. If you have a large network, you may want to make updating more efficient by creating:

- Multiple central installation directories.

- Additional software libraries.

See the *Sophos Endpoint Security and Control large networks configuration guide*, available from the Sophos website or from the Sophos Endpoint Security and Control Network Install CD.

2.3 Plan the computer groups

Note: If you use Active Directory, you may not need to set up computer groups. Enterprise Console can use your existing Active Directory groups.

Think about whether you group computers according to location, operating system, or other criteria. For example, you could put Exchange servers in a group of their own, as you do not want to run on-access scanning on them. See support knowledgebase article 12421 (<http://www.sophos.com/support/knowledgebase/article/12421.html>).

You should normally have no more than 1000 computers in a group.

2.4 Plan the security policies

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

When you create groups, default policies are applied to them. You can edit these policies or create new ones. The policies are as follows:

Updating policy

If you have more than one group with the same policy (or just the default policy), you should normally have no more than 1000 computers altogether updating from the same location. The optimum number updating from the same location is 600-700.

Note: The number of computers that can update from the same directory depends on the server holding that directory and on the network connectivity.

Anti-virus and HIPS policy

Note: *Host Intrusion Prevention System (HIPS)* is a security technology that protects computers from suspicious files, unidentified viruses, and suspicious behavior.

By default, all files likely to contain viruses/spyware are scanned on access. But you might also want to:

- Turn off on-access scanning on Exchange servers or other servers where performance might be affected. See Sophos support knowledgebase article 12421 (<http://www.sophos.com/support/knowledgebase/article/12421.html>).
- Scan for adware/PUAs. See *Scan for adware and potentially unwanted applications (PUAs)* (page 31).

Application control policy

By default, all applications are allowed to run. However, you can configure Sophos Anti-Virus to detect and block “controlled applications,” that is, legitimate applications that are not a security threat, but that you decide are unsuitable for use in your office environment. See [Scan for controlled applications](#) (page 33).

Firewall policy

By default, the firewall blocks all non-essential connections. Therefore, you must create your own firewall policy. Sophos recommends that you install the firewall on a few sample computers, customize it and use these settings as your policy. See [Set up a firewall policy](#) (page 27).

NAC policy

By default, computers are allowed to access the network (unless you have modified the default policy or changed the “policy mode” in the NAC server). If you want to set conditions that computers must comply with before they can access the network, you configure and apply one of the NAC policies. See [Set up network access control](#) (page 35).

2.5 Plan the search for networked computers

Note: If you use Active Directory, you do not have to search for the computers on your network. If you wish, Enterprise Console can import your existing Active Directory groups and computers.

Before you can install security software on networked computers, they must be added to the computer list in Enterprise Console. You can do this by using one of the following:

- Active Directory.
- Microsoft network browsing.
- IP range.

Searching for computers can take some time, especially if you do not use Active Directory, so you may want to search by stages (for example, by domain).

2.6 Plan how to protect computers

You can install security software on Windows NT, Windows 2000 or later automatically from the console.

Note: You cannot install Sophos Client Firewall or Sophos NAC (the agent component) 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 Windows, Mac OS X, Linux, UNIX and NetWare, as well as scripted installation.

3 System requirements

For system requirements, see the system requirements page of the Sophos website (<http://www.sophos.com/products/all-sysreqs.html>).

4 Install the management tools

This section describes installation of Sophos Enterprise Console. For information about installing the Sophos NAC server, see the *Sophos NAC for Endpoint Security and Control installation guide*.

Go to a server that meets the system requirements. Ensure that you are connected to the internet.

If the server is running **Windows Server 2008**, do the following before you start:

- Install SQL Server 2005 or SQL Server 2005 Express (if it isn't already installed) and create a 'SOPHOS' instance.
- Turn off User Account Control (UAC) and restart the server. You can turn UAC on again after you have installed Enterprise Console and subscribed to Sophos updates.

If the server is running **Windows 2000**, be prepared to restart it after installation.

1. Log on as follows:

- *If the computer is in a domain*, Sophos recommends that you log on as a domain administrator (you need to be a domain administrator to allow other users to use Enterprise Console).
- *If the computer is in a workgroup*, log on as a local administrator.

2. Go to the Sophos website, download the Sophos Endpoint Security and Control Network Installer and run it.

Alternatively, insert the Sophos Endpoint Security and Control Network Install CD. The CD should auto-run. When the home page is displayed, click **Install**.

3. An installation wizard is launched. In the welcome dialog box, click **Next**.

4. In the **License Agreement** dialog box, accept the terms of the license agreement if you want to continue. Click **Next**.

5. In the **Destination folder** dialog box, accept the default and click **Next**.

6. In the **Setup type** dialog box, **Complete** is selected by default. Click **Next**.

7. In the **Feedback to Sophos** dialog box, you specify whether you are willing for Enterprise Console to send details of the number and type of managed computers to Sophos each week.

- If you are willing, select **I agree** and click **Next**.
- If you are not, leave this option unselected and go to step 9.

8. If you agreed to send feedback to Sophos, you are prompted to enter the username printed on your license schedule and an email contact address. Both are optional. Click **Next**.

9. In the **Ready to install** dialog box, click **Install**.

If the computer is in a domain and you are logged in as domain administrator, you see the dialog in step 10. Otherwise, you see the message box described in step 11.

10. If the computer is in a domain, the **Enterprise Console user group** dialog box is displayed. This lets you specify who can use Enterprise Console. Select an existing global group. Click **Next**.
11. When installation is complete, you are prompted to log off or restart. Click **Yes** or **Finish** to continue with the setup.

The management tools have been installed.

Note: If you installed in a domain but with local administrator rights, add the Enterprise Console user group to the Sophos Console Administrators and SophosDBUsers local groups.

Note: If ever you replace the server, ensure the replacement has the same name and IP address, so that Enterprise Console can continue to manage computers.

Next you download the software you need and set up automatic updating (see next section).

5 Download software and set up updating

When you log on for the first time after installing the management tools, you are prompted to set up downloads and updating.

Note: If you installed Sophos Enterprise Console by using Remote Desktop, you are not prompted to continue the setup. You should select **Start|Programs|Sophos|EM Library** and then go to the section [Appendix: Advanced setup](#) (page 59).

1. In the **Welcome to Sophos Endpoint Security and Control** dialog box, select the type of setup you prefer.

Quick setup is recommended for most users. It enables you to:

- Download the Sophos software you need to default locations, ready for distribution to networked computers.
- Set up automatic, hourly updating of that software.
- Create groups for your networked computers (if you are using Active Directory).

Advanced setup gives you more control over the download and updating settings. If you select advanced setup, go to the section [Appendix: Advanced setup](#) (page 59).

Note: To protect Mac OS X version 10.4 or later computers, Sophos recommends that you select **Advanced setup** and download Sophos Anti-Virus version 7. To protect Mac OS X version 10.2 or 10.3 computers, you must use Sophos Anti-Virus version 4.9, which is available via **Quick setup**.

2. If you selected **Quick setup**, the **Subscribe to Sophos Updates** wizard is launched. In the welcome dialog box, click **Next**.
3. In the **Select software** dialog box, select the Sophos software that you want to download and keep updated automatically. Click **Next**.

Select only the software you need now. If your needs change later, you can change your selection at any time.

4. In the **Enter Sophos Download Account Details** dialog box, enter the username and password printed on your license schedule. Click **Next**.
5. In the **Download Software** dialog box, you see the steps that the wizard will take. If you use Active Directory and want Enterprise Console to use your existing computer groups, select **Set up groups for your computers**. Click **Next**.

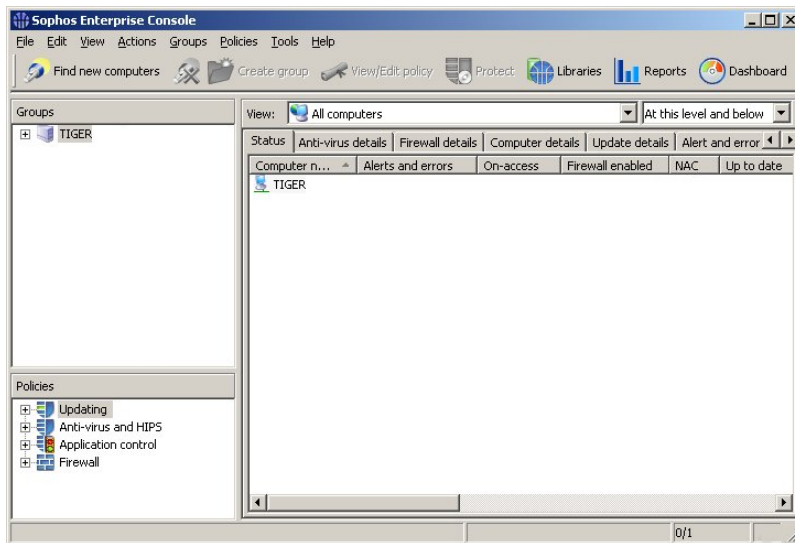
The **Download Progress** dialog box is displayed. Wait for the download to be completed.

6. In the **Completing the Subscribe to Sophos Updates Wizard** dialog box, click **Finish** to close the wizard.

Enterprise Console is launched for the first time.

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

Note: To open Enterprise Console in future, on the Windows taskbar, click **Start|Programs|Sophos|Sophos Enterprise Console**.



You are ready to pre-configure your security software and install it on your networked computers.

If you want to install and manage the software from another computer, for example, a workstation, go to that computer and continue to the next section.

If you want to do everything from this computer, keep Enterprise Console open and go to [Create groups for your computers](#) (page 16).

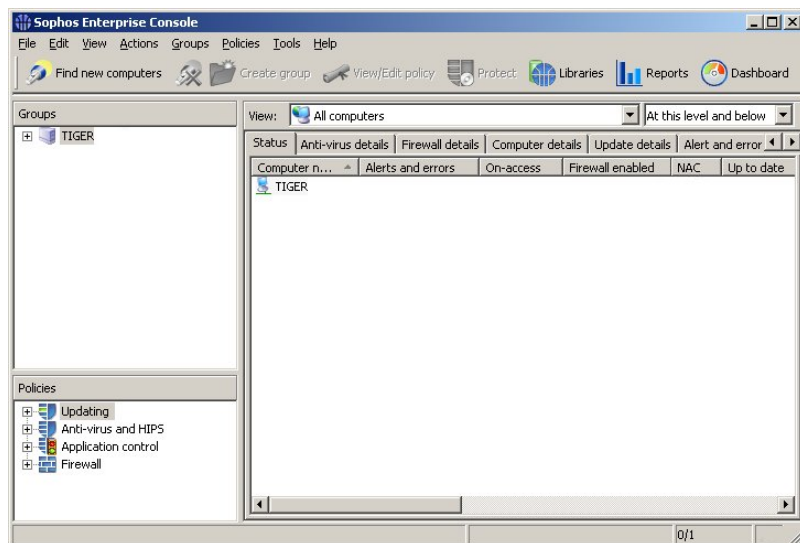
6 Set up a remote management console

To set up a remote management console, you run the same installer that you used in the section [Install the management tools](#) (page 10).

1. Go to the computer from which you want to manage Sophos software on your network. Visit the Sophos website, download the Sophos Endpoint Security and Control Network Installer and run it.
Alternatively, insert the Sophos Endpoint Security and Control Network Install CD. The CD should auto-run. When the home page is displayed, click **Install**.
2. An installation wizard is launched. In the welcome dialog box, click **Next**.
3. In the **License Agreement** dialog box, accept the terms of the license agreement if you want to continue. Click **Next**.
4. In the **Destination folder** dialog box, accept the default folder and click **Next**.
5. In the **Setup type** dialog box, select **Custom**. The **Management console** is selected by default. Click **Next**.
6. In the **Management service** dialog box, browse to the computer where the management server was installed (if you made a “Complete” installation, this is the computer in [Install the management tools](#) (page 10)). Click **Next**.
7. If the computer is in a domain, the **Enterprise Console user group** dialog box is displayed. This enables you to specify who can use Enterprise Console. Select an existing global group.
8. In the **Ready to install** dialog box, click **Install**.
9. After installation, you are prompted to log on again.
You must log on as a member of the user group that is allowed to use Enterprise Console.

When you log on again, Enterprise Console is launched for the first time.

Note: To open Enterprise Console in future, on the Windows taskbar, click **Start|Programs|Sophos|Sophos Enterprise Console**.



Note: You can allow other users to use the console. If the computer is in a domain, add the user to the group you selected in step 7. If the computer is in a workgroup, add the user to the Sophos Console Administrators group and the Sophos DB users group on the computer where you installed the management server.

You are ready to create computer groups.

7 Create groups for your computers

Note: If you use Active Directory, and you completed the **Subscribe to Sophos Updates** wizard, you can skip this section. Go straight to [Set up policies](#) (page 17).

You can protect computers only if they are in groups, with policies applied to them. A group holds a number of computers (which do not all have to run the same operating system). The computers in the group use the same policies and update from the same location.

You can use groups to put together computers that need a special configuration. For example, you could have a group for Exchange servers on which you do not want to run on-access scanning.

Note: The computers on which you want to install Sophos Anti-Virus for Mac OS X, version 4.9 must be in a different group from those computers on which you want to install Sophos Anti-Virus for Mac OS X, version 7.

1. To create your first group, click the **Create group** icon.
2. A **New Group** is added in the left-hand pane, with its name highlighted. Type in the name you want to use for the group.



3. 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 repeat step 1.

Each new top-level group has a set of default policies applied to it. A new sub-group initially uses the same settings as the group it is within.

Now you can create policies.

8 Set up policies

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

When groups are created, default policies are applied. You can edit these policies or create new policies. This section describes:

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

8.1 Create or edit a policy

Note: You cannot create NAC policies. You can only edit them.

To create or edit a policy:

1. In the **Policies** pane (bottom, left-hand side of the window), do one of the following:
 - To create a new policy, right-click the type of policy you want, for example, Updating Policy, and select **Create policy**.
 - To edit a default policy, double-click the type of policy you want to edit. Then highlight **Default**.

If you created a policy, a **New Policy** is added to the list, with its name highlighted. Type a name.

2. Double-click the policy. Enter the settings you want.

Now you need to apply your policy to a computer group (see next section).

8.2 Apply policies to groups

1. In the **Policies** pane, highlight the policy.
2. Click the policy and drag it onto the group to which you want to apply the policy.

8.3 Default policies

This section tells you about the default policies and about any changes you should make.

8.3.1 Updating policy

If you used **Quick setup** (as described in [Download software and set up updating](#) (page 12)), you do not need to set up an updating policy. Computers will update from the default central installation directories which were created on the computer where you installed Enterprise Console.

If you used **Advanced setup**, you must set up updating policies as follows:

1. In the **Policies** pane, double-click **Updating** and then double-click **Default**. This enables you to edit the default policy, which is already applied to your new group(s).

Alternatively, you can create a new policy. Right-click **Updating** and select **Create policy**.

Note: The computers on which you want to install Sophos Anti-Virus for Mac OS X, version 4.9 must use a different updating policy from those computers on which you want to install Sophos Anti-Virus for Mac OS X, version 7.

2. In the **Updating policy** dialog box, select an operating system used by computers in that group, for example, **Windows 2000 and later**. Click **Configure**.
3. Click the **Primary server** tab. In the **Address** field, click the drop-down arrow and select the directory from which computers will fetch updates, for example, the \\Servername\InterChk\SAVSCFXP directory for Windows 2000 or later. Enter the **User name** and **Password** for the account that will be used for updating.

The account must be able to:

- Run on the computers in the group.
- Have read access to the address you have just entered.

If the **User name** needs to be qualified to indicate the domain, use the form domain\username.

Note: Sophos Anti-Virus for Mac OS X, version 4.9 must update from the directory ESOSX, and version 7 must update from ESCOSX.

8.3.2 Anti-virus and HIPS policy

By default, Sophos Anti-Virus will

- Deny access to any file that contains viruses/spyware.
- Detect suspicious behavior by programs that are running.
- Send an alert to the console whenever a threat is detected.

You may want to

- Turn off on-access scanning on Exchange servers or other servers where performance might be affected. See support knowledgebase article 12421 (<http://www.sophos.com/support/knowledgebase/article/12421.html>).

- Block suspicious behavior. See [Detect suspicious behavior](#) (page 28).
- Scan for suspicious files. See [Scan for suspicious files](#) (page 30).
- Scan for adware/potentially unwanted applications. See [Scan for adware and potentially unwanted applications \(PUAs\)](#) (page 31).

To edit the anti-virus and HIPS policy:

1. Check which anti-virus and HIPS policy is used by the group(s) of computers you want to configure. To do this, find the group in the **Groups** pane, right-click it and select **View group policy details**.
2. In the **Policies** pane, double-click **Anti-virus and HIPS**. Then double-click the policy you want to change.
3. In the **Anti-virus and HIPS policy** dialog box, edit the settings.

8.3.3 Application control policy

By default, application control is not enabled. For details of how to set it up, see [Scan for controlled applications](#) (page 33).

8.3.4 Firewall policy

By default, the firewall blocks all non-essential connections. Therefore, you must create your own firewall policy. For details of how to do this, see [Set up a firewall policy](#) (page 27).

8.3.5 NAC policy

By default, computers are allowed to access the network (unless you have modified the default policy or changed the “policy mode” in the NAC server). If you want to set conditions that computers must comply with before they can access the network, you configure and apply one of the NAC policies. See [Set up network access control](#) (page 35).

9 Search for computers and add them to groups

Note: If you use Active Directory, and you completed the **Subscribe to Sophos Updates** wizard, you can skip this section. Go straight to [Protect computers](#) (page 21).

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

1. Click the **Find new computers** icon on the toolbar.
2. Select the method you want to use to search for computers. Sophos recommends that you use **Import from Active Directory**. This enables you to import your existing groups and computers. You will be able to keep these groups synchronized in future, and ensure that new computers on the network are protected automatically.

*If you select **Import from Active Directory**, a wizard is launched to guide you through the process. Complete the wizard and go to section 10.*

*If you select **Find with Active Directory**, **Find on the network** or **Find by IP range**, continue to step 3.*

3. If you selected one of the **Find** options, you are prompted to enter a username and password. You need to do this if you have computers (for example, Windows XP Service Pack 2) that cannot be accessed without account details. The account must be a domain administrator's account, or have full administrative rights on the target XP computer.

If you are using a domain account, you must enter the username in the form domain\user.

4. Next select the domains or workgroups where you want to search for computers. Click **OK**.
The console searches for computers and adds them to the **Unassigned** folder.

5. Click the **Unassigned** folder. Select the computers you want and drag and drop them onto your chosen group in the **Groups** pane.

You can put computers with different operating systems in the same group.

A wizard is launched to help you protect the computers (see next section).

10 Protect computers

Now you protect your computers by installing Sophos security software on them.

10.1 Prepare to install security software

Before you begin, you may need to:

- Prepare for removal of third-party security software.
- Prepare for removal of a third-party update tool.
- Prepare for anti-virus software installation.
- Prepare for firewall installation.

10.1.1 Prepare for removal of third-party software

The Sophos installer can remove previously installed security software automatically.

Note: The installer cannot remove all third-party products. To see which it can remove, open a command prompt, go to the CRT directory in your central installation directory, and run

```
avremove -l
```

Note: If you have another vendor's network access control software installed, you must remove it before you begin. The Sophos installer cannot remove it automatically.

If you plan to use the automatic removal option, you should do as follows first:

- If computers are running another vendor's software, ensure that its user interface is closed.
- If computers are running another vendor's firewall or HIPS product, ensure that it is turned off or configured to allow the Sophos installer to run.
- If computers have another vendor's update tool installed and you wish to remove it, follow the instructions in [Prepare for removal of a third-party update tool](#) (page 21). This ensures that the tool does not reinstall another vendor's software automatically.

Note: You will have to restart any computers from which you remove third-party anti-virus software.

10.1.2 Prepare for removal of a third-party update tool

If you want to remove another vendor's update tool, you must edit the configuration file that the Sophos installer will use.

Note: If computers are running another vendor's firewall or HIPS product, you may need to leave that vendor's update tool intact. See that vendor's documentation for clarification.

1. In the Central Installation Directory from which computers will install and update Sophos software, find the data.zip file.
2. Extract the crt.cfg configuration file from data.zip.
3. Edit the crt.cfg file to change the line reading "RemoveUpdateTools=0" to "RemoveUpdateTools=1".
4. Save your changes and save crt.cfg to the same directory that contains data.zip.
Don't put crt.cfg back into data.zip or it will be overwritten the next time the data.zip file is updated.

The Sophos installer is now configured to remove any update tool.

10.1.3 Prepare for anti-virus software installation

As well as ensuring that computers meet the general system requirements, you must perform further steps before you can install software on them automatically.

Windows 2000, XP Pro, 2003 and NT computers

Ensure that these computers:

- Run the Remote Registry, Server, Computer Browser and Task Scheduler services.
- Have the C\$ admin share enabled.
- Have "Simple File Sharing" turned off (XP only).

Windows XP Service Pack 2 computers

On Windows XP Service Pack 2 computers, you must:

- Enable "File and Printer Sharing for Microsoft Networks."
- Make sure TCP ports 8192, 8193 and 8194 are open.
- Restart the computer to make the changes effective.

Windows Vista computers

On Windows Vista computers, you must:

- Ensure that the **Remote Registry Service** is started and that its startup type is set to **Automatic**. This service is not on by default on Windows Vista.
- Turn off **User Account Control**. This is accessed via Start|Control Panel|User Accounts|Turn User Account Control on or off. When installation is complete, you should turn this back on.

- Open **Windows Firewall with Advanced Security**. This is accessed via Start|Control Panel|Administrative Tools. Change the **Inbound rules** to enable the processes below. When installation is complete, disable them again.

Remote Administration (NP-In) Domain

Remote Administration (NP-In) Private

Remote Administration (RPC) Domain

Remote Administration (RPC) Private

Remote Administration (RPC-EPMAP) Domain

Remote Administration (RPC-EPMAP) Private

10.1.4 Prepare for firewall installation

If you want to use Sophos Client Firewall, you should plan to install it on only a few sample computers first. The firewall initially prevents network access and must be configured before you install it on all computers.

For full details, see support knowledgebase article 14197 (<http://www.sophos.com/support/knowledgebase/article/14197.html>).

Note: You have to restart any computers on which you install Sophos Client Firewall.

10.2 Install security software

1. Select the computers you want to protect. Right-click and select **Protect computers** to launch a wizard.
The wizard is launched automatically if you move unprotected computers into a group.
2. In the **Welcome** dialog box, click **Next**.
3. In the **Select security software** dialog box, select the software you want. Leave **Remove third-party security software** selected if you want to have another vendor's software removed automatically. Click **Next**.

Before you can install Sophos Network Access Control, you must click the link to **Set up the NAC server URL**. Enter the URL if it is not already displayed.

Note: If Sophos NAC is installed on more than one server, use the URL of the computer running the application, not the computer with the database.

The third-party security software removal tool uninstalls only products with the same functionality as those you install.

4. If you selected the firewall or network access control software, you are prompted to check that your license entitles you to use it. Click **OK** to continue.

5. In the **Protection summary** dialog box, any problems with installation are shown in the **Protection issues** column. Note the problems and Click **Next**.

Common problems are:

- Automatic installation is not possible on that operating system. Perform a manual installation. See [Protect Windows computers with manual installation](#) (page 39) or [Protect Mac OS X computers](#) (page 40) or [Protect Linux computers](#) (page 41).
 - Operating system could not be determined. This may be because you did not enter your username in the format domain\username when finding computers.
 - The computers are running a firewall (usually this is the case on Windows XP SP2 computers).
6. In the **Protect computers credentials** dialog box, enter details of an account that can be used to install software on the computers. Click **Finish**.

This account is typically a domain administrator account. It must:

- Have local administrator rights on computers you want to protect.
- Be able to log on to the computer where you installed the management server.
- Have read access to the location that computers will update from (to check this location, in the **Policies** pane, double-click **Updating**, then double-click **Default**).

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

7. When installation is complete, look at the list of computers again. In the **On-access column**, you should see the word “Active”: this shows that the computer is running on-access virus scanning.

If you have installed the firewall for the first time, make sure you follow the instructions in [Set up a firewall policy](#) (page 27).

Computers need to be restarted to scan files accessed by DFS (Windows 2000/XP) or via non-Microsoft file systems (Windows 2000).

8. Repeat the above steps for each group of computers.

You should now check that computers are fully protected and up to date (see next section).

If you are an Active Directory user, you can also configure Enterprise Console to protect new computers automatically when they are added to the network. See [Ensure new computers will be protected automatically](#) (page 26).

11 Check computers are protected

To check that computers are protected, do as follows:

1. Select the group of computers you want to check.
2. If you want to check computers in sub-groups of the group, select **At this level and below** in the drop-down menu.
3. Check the status computers as follows:
 - a) Look in the **On-access** column. If you see “Active”, the computer is protected by on-access scanning. If you see a gray shield and “Inactive”, it is not.
You may decide to have on-access scanning disabled on Exchange servers or other servers where performance might be affected.
 - b) Look in the **Firewall enabled** column. If you see “Yes”, the computer is protected by the firewall. If you see a grayed-out firewall icon and “No”, it is not.
 - c) Look in the **NAC** column. If you see “Installed”, network access control is installed. If the column is blank, it is not.
 - d) Look in the **Up to date** column. If you see “Yes”, the computer is up to date. If you see a clock icon and “Not since ...”, it is not.

Computer name	Alerts	On-access	Firewall enabled	NAC	Up to date
TIGER		Active	Yes	Installed	Yes
MOTH		Inactive	No		Not si...

If any computers are unprotected, see the help files for advice. Open the “How do I check whether my network is protected?” section and click “Find computers that are unprotected”.

If you want new computers protected automatically, see [Ensure new computers will be protected automatically](#) (page 26).

12 Ensure new computers will be protected automatically

You can synchronize your groups with Active Directory, so that Enterprise Console will:

- Check Active Directory regularly for new computers and groups and add them to the computer list automatically.
- Protect new computers automatically.

To set up synchronization, do as follows:

1. On the **Groups** menu, select **Synchronize with Active Directory**.

A wizard is launched to guide you through the process.

2. In the **Overview** dialog box, click **Next**.
3. In the **Choose an Enterprise Console Group** dialog box, select a group. Click **Next**.
4. In the **Choose an Active Directory Container** dialog box, select an Active Directory container which you want to synchronize the group with. Enter the name of the container, for example, `LDAP://CN=Computers,DC=domain_name,DC=local` or click **Browse** to browse to the container in Active Directory. Click **Next**.
5. In the **Protect Computers Automatically** dialog box, select the software you want to install. Leave **Remove third-party security software** selected if you want to have another vendor's software removed automatically. Click **Next**.

Before you can install Sophos Network Access Control, you must click the link to **Set up the NAC server URL**.

All Windows 2000 or later workstations discovered during this and future synchronizations will be protected automatically, in compliance with their respective group policies.

Note: You can disable automatic protection or change your settings later. Right-click the group, select **Synchronization Properties** and edit the settings.

Note: Computers running Windows 95/98/Me, Windows server operating systems, Mac OS X, or Linux will not be protected automatically. You must protect such computers manually.

6. If you chose to protect computers automatically, the **Enter Active Directory Credentials** dialog box is displayed. Enter the details of an administrator account that will be used to install software on the computers. Click **Next**.
7. In the **Choose the Synchronization Interval** dialog box, choose how often you want to synchronize the Enterprise Console group with the Active Directory container. The default is 60 minutes.
8. In the **Confirm Your Choices** dialog box, check the details, and then click **Next** to proceed.

In the last dialog box, you can view the details of the groups and computers that have been synchronized.

13 Set up a firewall policy

By default, the firewall blocks all non-essential connections. Therefore, you must create your own firewall policy. Sophos recommends that you install the firewall on a few sample computers, customize it and use these settings as your policy.

Once you have installed the firewall on computers that are typical of your network (using the steps in [Protect computers](#) (page 21)), do as follows:

1. Go to each computer and restart it to activate the firewall.
2. Right-click the firewall icon in the system tray and select **Configure**.
3. In the **SCF Configuration Editor** dialog box, click the **Applications** tab.
 - a) Click **Add** and browse to each application you want. The application is then “trusted.”
 - b) For greater security, highlight the program, click **Custom** (bottom right-hand of the dialog box) and create a rule.

Alternatively, on the **General** tab, select **Interactive**. The firewall will prompt you to allow or block each application when it is used.

4. When the firewall is configured, on the **General** tab, click **Export** to export the configuration to your chosen location.
5. Repeat the above steps on each computer you want to use as a sample.
6. Now go to Enterprise Console. In the **Policies pane**, double-click **Firewall** and then double-click the policy you want to edit.
7. In the **Firewall policy** dialog box, on the **General** tab, click **Import** and import a configuration you developed earlier.

When you import each configuration, you are given the option to merge it with other configurations you have already imported.
8. Now you are ready to protect the rest of your computers. Repeat the steps in [Protect computers](#) (page 21).

14 Detect suspicious behavior

By default, Sophos Anti-Virus analyzes the behavior of all programs running on a computer and can detect the following:

- Suspicious behavior, for example, changes to the registry that could allow a virus to run automatically when the computer is restarted.
- Buffer overflow attacks.

Note: Buffer overflow detection is not available for Windows Vista and 64-bit versions of Windows. These operating systems are protected against buffer overflows by Microsoft's Data Execution Prevention (DEP) feature.

When Sophos Anti-Virus is first installed, it detects such behavior and sends alerts to Enterprise Console. However, it does not block any of the programs detected.

Sophos recommends that you introduce blocking of suspicious behavior as follows:

- Pre-authorize any programs you want to continue to run in future.
- When you are ready, configure Sophos Anti-Virus to block programs that are detected from now on.

This approach avoids blocking programs that your users may need.

14.1 Authorize programs you want

If suspicious behavior is detected, an alert icon is displayed next to the computer name in Enterprise Console. To see more details, click the **Alert and error details** tab.

Authorize programs you want as follows:

1. Check which anti-virus and HIPS policy is used by the group(s) of computers you want to configure. To do this, find the group in the **Groups** pane, right-click it and select **View group policy details**.
2. In the **Policies** pane, double-click **Anti-virus and HIPS**. Then double-click the policy you want to change.
3. In the **Anti-virus and HIPS policy** dialog box, click **Authorization**.
4. In the **Authorization Manager** dialog box, select the tab for the type of behavior that has been detected, for example, Buffer overflow.
5. Find the program that has been detected and move it from the **Known** list to the **Authorized** list. Click **OK**.

When you have run Sophos Anti-Virus in alert-only mode for a time and are confident that you have authorized the programs you need, you are ready to enable automatic blocking of suspicious behavior.

14.2 Turn on blocking of suspicious behavior

To block suspicious behavior:

1. Open the **Anti-virus and HIPS policy** dialog box (as in step 2 in the previous section). Click **HIPS runtime behavior**.
2. In the **HIPS runtime behavior analysis settings** dialog box, ensure that the forms of detection you want to use are enabled. Then clear the **Alert only** check box. Click **OK**.

From now on, Sophos Anti-Virus will block programs that are behaving suspiciously, according to the rules set by Sophos.

Sophos updates the behavioral rules regularly to respond to new threats. You may want to be notified in advance of any changes, so that you can decide whether you need to authorize programs that might otherwise be blocked. To subscribe to the “Behavioral rule notification,” go to <http://www.sophos.com/security/notifications>.

15 Scan for suspicious files

By default, Sophos Anti-Virus detects known and unknown viruses, Trojans, worms, and spyware. You can also configure it to detect suspicious files.

Note: A suspicious file is a file that contains certain characteristics that are common to malware but not sufficient for the file to be identified as a new piece of malware (for example, a file containing dynamic decompression code commonly used by malware).

Note: This option applies only to Sophos Anti-Virus 7 or later for Windows 2000 or later.

1. Check which anti-virus and HIPS policy is used by the group(s) of computers you want to configure. To do this, find the group in the **Groups** pane, right-click it and select **View group policy details**.
2. In the **Policies** pane, double-click **Anti-virus and HIPS**. Then double-click the policy you want to change.
3. In the **Anti-virus and HIPS policy** dialog box, ensure the **Enable on-access scanning** check box is selected. Click **On-access**.
4. On the **Scanning** tab, in the **Scanning options** panel, select the **Scan for suspicious files (HIPS)** check box. Click **OK**.

If you want to authorize suspicious files to run on computers, open the **Anti-virus and HIPS** policy that applies to them, click **Authorization**, and then select the **Suspicious files** tabbed page.

16 Scan for adware and potentially unwanted applications (PUAs)

By default, Sophos Anti-Virus detects viruses, Trojans and worms. You can also configure it to detect adware and potentially unwanted applications (PUAs).

Note: This option applies only to Sophos Anti-Virus 6 or later running on Windows 2000 or later.

When you first use this form of scanning, it may generate many alerts and cause problems for applications that are already running on your network. Sophos recommends that you:

- Use a full system scan to detect adware/PUAs.
- Authorize or remove any applications that are detected.
- Enable on-access scanning to protect your computers in future.

16.1 Run a full system scan

Sophos recommends a full system scan, which scans computers now.

Note: If you prefer, you can set up a scheduled scan, as described in the Sophos Enterprise Console help files. Open the “How do I change anti-virus and HIPS settings?” section and click “Scan computers at set times.”

1. Select the computers you want to scan in the computer list or the group in the **Groups** pane. Right-click and select **Full system scan**.
2. In the **Full system scan** dialog box, review the details of the computers to be scanned and click **OK** to start the scan.

When the scan is carried out, Sophos Anti-Virus may report some adware/PUAs.

Now you can authorize such applications for use or remove them.

16.2 Authorize applications you want

If you want your computers to run the applications, do as follows:

1. In the **Anti-virus and HIPS policy** dialog box, click **Authorization**.
2. In the **Authorization Manager** dialog box, select the **Adware/PUAs** tab.
3. In the **Known adware/PUAs** list, applications that have been detected are shown. Select the applications that you want and add them to the **Authorized adware/PUAs** list. Click **OK**.
If you want to remove applications, see [Clean up viruses, PUAs and suspicious files](#) (page 38).

Now you can enable on-access scanning for adware/PUAs.

16.3 Enable on-access scanning

To enable on-access scanning for adware/PUAs, do as follows.

Note: Some applications monitor files and attempt to access them frequently. If you have on-access scanning enabled, it detects each access and sends multiple alerts.

1. In the **Anti-virus and HIPS policy** dialog box, click **On-access**.
2. In the **On-access scan settings** dialog box, select **Scan for adware/PUAs**.

If you want full detection and cleanup of potentially unwanted applications or multi-component threats on external disk drives, you must configure Windows to report such drives as local.

17 Scan for controlled applications

You can configure Sophos Anti-Virus to detect and block “controlled applications,” that is, legitimate applications that are not a security threat, but that you decide are unsuitable for use in your office environment, for example, games or instant messaging programs.

This option applies only to Sophos Anti-Virus 7 or later running on Windows 2000 or later.

When Sophos Anti-Virus is first installed, all applications are allowed by default. Sophos recommends that you introduce application control as follows:

- Select the applications that you want to control.
- Run a full system scan for controlled applications.
- Remove any applications you don't want.
- Enable on-access scanning for controlled applications.

By taking this approach, you avoid generating large numbers of alerts and blocking applications that your users may need.

17.1 Select the applications you want to control

To select applications to control, do as follows:

1. In the **Policies** pane, double-click **Application control**. Then double-click the policy you want to change.
2. In the **Application control policy** dialog box, click the **Authorization** tab.
3. On the **Authorization** tabbed page, select an **Application type**, for example, **File sharing application**. A full list of the applications included in that group is displayed in the **Authorized** list below.
 - To block an application, select it and move it to the **Blocked** list.
 - To block any new applications that Sophos adds to that type in the future, move **All added by Sophos in the future** to the **Blocked** list.

Sophos recommends that you leave applications installed with Windows (such as games) unblocked until after you run a scan to find out which other applications are in use. This is because these common applications will give rise to a large number of alerts.

4. On the **Scanning** tabbed page, select **Enable on-demand and scheduled scanning**. Click **OK**.

Now run a full system scan.

17.2 Run a full system scan

Sophos recommends a full system scan, which scans computers now.

Note: If you prefer, you can set up a scheduled scan, as described in the Sophos Enterprise Console help files. Open the “How do I change anti-virus and HIPS settings?” section and click “Scan computers at set times.”

1. Select the computers you want to scan in the computer list or the group in the **Groups** pane. Right-click and select **Full system scan**.
2. In the **Full system scan** dialog box, review the details of the computers to be scanned and click **OK** to start the scan.

When the scan is carried out, alerts are displayed in Enterprise Console for any controlled applications that are found.

17.3 Uninstall applications you don't want

Before you uninstall controlled applications, ensure that on-access scanning for controlled applications is disabled. This type of scanning blocks the programs used to install and uninstall applications, so it may interfere with uninstallation.

You can remove an application in one of two ways:

- Go to each computer and run the uninstaller for that product. You can usually do this by opening the Windows **Control Panel** and using **Add/Remove Programs**.
- At the server, use your usual script or administration tool to run the uninstaller for that product on your networked computers.

Now you can enable on-access scanning.

17.4 Enable on-access scanning

To enable on-access scanning for controlled applications:

1. In the **Policies** pane, double-click **Application control**. Then double-click a policy.
2. In the **Application control policy** dialog box, on the **Scanning** tab, select **Enable on-access scanning**.

On-access scanning is enabled. Your anti-virus and HIPS policy settings determine which files are scanned (that is, the extensions and exclusions).

You can also have alerts sent to particular users if a controlled application is found on any of the computers in the group. For instructions, see the Sophos Enterprise Console help files. Open the “How do I set up alerts?” section and click “Set up application control alerts.”

18 Set up network access control

You can set up network access control (NAC), so that computers are only allowed to log on to the network if they comply with conditions you set.

Enterprise Console works together with Sophos NAC to provide this network protection. You need to have installed the following:

- The Sophos NAC server. You install this separately from Enterprise Console.
- The Sophos NAC agent. You install this on your networked computers, so that they can communicate with the NAC server. You perform the installation with the **Protect computers** wizard, as described in *Protect computers* (page 21).

This section assumes you have installed both.

If you are using the default policy supplied with the NAC server and have not changed the “policy mode,” network access is not blocked.

If you want to set conditions that computers must comply with before they can access the network, you configure and apply one of the NAC policies.

18.1 Configure and apply a NAC policy

You can change the settings for any of the pre-defined NAC policies:

- The **Default** and **Managed** policies can be used for computers that are managed by Enterprise Console.
- The **Unmanaged** policy can be used for computers from outside the company, which are not managed by Enterprise Console and do not have Sophos NAC installed. For more information, see “Using predefined policies” in the *Sophos NAC for Endpoint Security and Control NAC Manager Guide*.

To configure a NAC policy:

1. In the **Policies** pane, double-click **NAC**. Double-click the policy you want to configure.
Sophos NAC Manager is launched.
2. In NAC Manager, log in with your credentials.
3. In the page for the policy, edit the options.
For information on the options, see “Updating policies” in the *Sophos NAC for Endpoint Security and Control NAC Manager Guide*.
4. In Enterprise Console, click the policy and drag it onto the group to which you want to apply the policy.

19 Check the health of your network

You can check the health of your network at a glance. You do this by viewing the Enterprise Console dashboard.

On the menu bar, click the **Dashboard** icon. The **Dashboard** is displayed in the upper part of the window.



In the left-hand panel, the dashboard shows you


- How many computers are managed by Enterprise Console.
- When your software was last updated from Sophos.

In the centre and right-hand panels, it also shows statistics for computers that

- Have detected threats or controlled applications.
- Are out of date.
- Do not comply with your policies.
- Have reported errors.

To see a list of the affected computers, click the heading for each section. In each section, the **Dashboard** displays a health indicator as follows:

 Healthy

 Warning level

 Critical level

If you want to, you can

- Customize the threshold at which Enterprise Console will display each of these indicators.
- Configure Enterprise Console to send email alerts when the thresholds are exceeded.

To do this, on the menu bar, click **Tools|Configure dashboard**.

You can find more information in the Enterprise Console help files. See the “How do I check whether my network is protected?” section, which includes a “Configure the dashboard” page.

20 Clean up viruses, PUAs and suspicious files

You can use Enterprise Console to clean up computers that report viruses/spyware or adware/potentially unwanted applications (PUAs).

1. In the list of computers, right-click the computer(s) that you want to clean up. Select **Clean up detected items**.
2. In the **Clean up detected items** dialog, select the check box for each threat you want to clean up, or click **Select all**. Click **OK** to clean the computer(s).

If the cleanup is successful, the alert(s) shown in the list of computers will no longer be displayed.

If cleanup is not successful, go to www.sophos.com/security/analyses and look for information about the threat and advice on cleanup. Then go to each computer and clean it up manually.

If you want Sophos Anti-Virus to attempt to clean up computers automatically in future, see the Enterprise Console help files. Open the “How do I clean up computers?” section and click on “Set up automatic cleanup.”

21 Protect Windows computers with manual installation

You can protect Windows 2000 and later computers automatically from Enterprise Console, as described in [Protect computers](#) (page 21).

If you cannot protect Windows computers automatically, or if you have Windows 95/98/Me or NT computers, you can protect them by running the installation program manually.

Note: If you have many computers, use a script or a program like Microsoft SMS to run the installation program automatically. See [Protect computers with a script](#) (page 57).

1. Find the installation program. The program is in the central installation directory from which computers will update in future.

To check which directory this is select the computer(s) you want to protect. Click the **Update details** tab and look in the **Primary server** column.

If your licence includes the firewall or network access control, you can install these, along with the anti-virus software, on Windows 2000 or later computers. Look for the directory called SAVSCFXP.

2. Go to each computer and log on with local administrator rights.
3. Locate setup.exe in the central installation directory and double-click it.
4. In the **Setup** dialog box, do as follows:
 - a) In the **Select security software** dialog pane, select the software you want to install. Leave **Remove third-party security software** selected if you want to have another vendor's software removed automatically.
 - b) In the **Credentials** pane, enter the details of an account that can fetch updates from the server. The account can be the one you used in [Protect computers](#) (page 21).

The account used must:

 - Be able to log on to the computers you want to protect.
 - Have read access to central installation directories (see step 1).

After installation, Windows computers need to be restarted to scan files accessed by DFS (Windows 2000/XP) or via non-Microsoft file systems (Windows 2000).

22 Protect Mac OS X computers

22.1 Prepare to install Sophos Anti-Virus

To protect Mac OS X version 10.4 or later computers, Sophos recommends that you use Sophos Anti-Virus version 7. To protect Mac OS X version 10.2 or 10.3 computers, you must use Sophos Anti-Virus version 4.9.

To use Sophos Anti-Virus version 7, ensure that you have done the following:

1. Download Sophos Anti-Virus version 7. If you selected **Quick setup** when you downloaded software earlier, you have only version 4.9. To download version 7, on the toolbar, click the **Libraries** icon and follow the instructions in [Select the software you want to download](#) (page 62) and [Download software](#) (page 63).
2. If you want to protect Mac OS X computers with both version 4.9 and 7 of Sophos Anti-Virus:
 - a) Add the computers on which you want to install version 7 to a different group from those computers on which you want to install version 4.9.
 - b) Create an updating policy for the computers on which you want to install version 7 that is different to that for those computers on which you want to install version 4.9. For information, see [Updating policy](#) (page 18).

22.2 Install Sophos Anti-Virus

1. Find the installation program, Sophos Anti-Virus.mpkg. The program is in the central installation directory from which computers will update in future. The default paths of the program are shown in the following table:

Sophos Anti-Virus version	Path of installation program
7	\\server name\Interchk\ESCOSX
	smb://server name/Interchk/ESCOSX
4.9	\\server name\Interchk\ESOSX
	smb://server name/Interchk/ESOSX

2. Copy Sophos Anti-Virus.mpkg to each computer that you want to protect.
3. Go to each computer and log on with local administrator rights.
4. Double-click Sophos Anti-Virus.mpkg.
5. Follow the instructions in the installation program.

23 Protect Linux computers

To protect Linux computers, you must:

- Download Sophos Anti-Virus for Linux.
- Create a deployment package.
- Install Sophos Anti-Virus on the Linux computer(s).

23.1 Download Sophos Anti-Virus for Linux

If you have not already downloaded the Sophos Anti-Virus for Linux software, do as follows:

1. Go to the Windows computer where you installed Enterprise Console. Open Enterprise Console and click the **Libraries** icon.
2. In Sophos EM Library, select **Library|Select Packages**.
3. In the **Select Packages** dialog box, do as follows:
 - a) Ensure that you have cleared the **Show default packages only** check box.
 - b) Select the **Sophos Anti-Virus for Linux (on-access)** package. Click **OK**.
4. On the **Library** menu, select **Download Packages**.

By default, Sophos EM Library creates a shared directory for the latest Sophos software at:

[servername]\InterChk\savlinux

Now create a deployment package.

23.2 Create a deployment package

You can use the **mkinstpkg** script to create a deployment package for your end-users. This script prompts you for information about how Sophos Anti-Virus will be installed on your Linux computers, and the answers gathered are inserted into the deployment package. When the end-user installs from this deployment package, it will not prompt for any information and will set up both the update location and credentials correctly. You can create a package in tar or RPM format.

Note: The **mkinstpkg** script is for use within your organization only. Please read the license agreement and legal notice displayed by the **mkinstpkg** script.

1. Log on to your Linux server as root.
2. Mount the shared directory in which the Sophos Anti-Virus for Linux software has been placed (the central installation directory or CID).

By default this directory is the \InterChk\savlinux directory on the server where Enterprise Console is installed. (To enable this directory to be mounted automatically on system boot, use distribution-specific tools for doing so, or edit fstab.)

3. Change to the CID.
4. To create the package, do as follows:
 - To create a deployment package in tar format, called savinstpkg.tgz, run
`./mkinstpkg.sh`
 - To create a deployment package in RPM format, called savinstpkg-0.0-1.i586.rpm, run
`./mkinstpkg.sh -r`
- Note:** The filename might differ depending on the RPM setup.
5. When prompted, choose to have the computers managed by Enterprise Console.
6. When prompted for the location, enter the location of the CID (as seen from the Linux computers).

Now you are ready to install Sophos Anti-Virus using this deployment package.

23.3 Install Sophos Anti-Virus using the deployment package

You use the package to install Sophos Anti-Virus in one of two ways:

- Automatically across the network. This approach can be used only with a package in RPM format.
- Manually on each computer. This approach can be used with a package in RPM or tar format.

23.3.1 Install Sophos Anti-Virus manually

You can install Sophos Anti-Virus manually as follows:

1. Use your own tools to copy the deployment package to the computers where you want to install Sophos Anti-Virus.
2. Go to each computer and log in as root.
3. Place the deployment package in a temporary directory and change to that directory.
4. To perform the installation, do as follows:
 - To untar the tar package and run the manual update script, enter

```
tar -zxvf savinstpkg.tgz
./sophos-av/install.sh
```
 - To install from the RPM package, enter

```
rpm -i <RPM package>
```

This copies the necessary files from the server and installs Sophos Anti-Virus. From now on, Sophos Anti-Virus will be updated automatically whenever the CID is updated.

23.3.2 Install Sophos Anti-Virus automatically

You can install Sophos Anti-Virus automatically from the deployment package by using one of the Linux administration tools that support remote deployment. Refer to the documentation for that tool.

Once Sophos Anti-Virus is installed, it will be started and will be updated automatically whenever the CID is updated.

24 Protect NetWare servers

To protect NetWare servers, you must:

- Create a directory for Sophos updates.
- Download Sophos Anti-Virus.
- Install Sophos Anti-Virus.
- Load Sophos Anti-Virus.

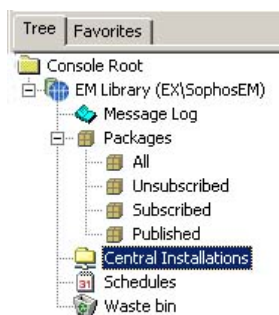
24.1 Create a directory for Sophos updates

On each NetWare server you want to protect, you must create a directory into which EM Library can put the latest Sophos software.

This directory should be \\[NetWare server]\SYS\SWEEP where [NetWare server] is the name of the NetWare server.

24.2 Download Sophos Anti-Virus for NetWare

1. On the Windows computer where you installed Enterprise Console and EM Library, open EM Library and select **Library|Select Packages**.
2. In the **Packages** dialog box, ensure that you have unchecked **Show default packages only**. Select the Sophos Anti-Virus for NetWare package. Click **OK**.
3. Select **Library|Download Packages**.
4. In the console tree, click **Central Installations**.



The default CIDs created by EM Library are displayed.

5. Right-click the Sophos Anti-Virus for NetWare CID and select **Properties**.

6. In the **Properties** dialog box, click the **Location** tab. Select **Custom CID location** and enter \\[NetWare server]\SYS\SWEEP\NLMINST

Note: EM Library will create the NLMINST subdirectory for you.

24.3 Install Sophos Anti-Virus

To install Sophos Anti-Virus:

1. Log on to the NetWare server with write access rights equivalent to ADMIN.
2. Go to \\[NetWare server]\SYS\SWEEP\NLMINST where [NetWare server] is the name of the NetWare server.
3. Copy all the files there to \\[NetWare server]\SYS\SWEEP

You have installed Sophos Anti-Virus.

Now load Sophos Anti-Virus.

24.4 Load Sophos Anti-Virus

To load Sophos Anti-Virus:

1. At the server console, or using RCONSOLE from a workstation, do as follows.
 - a) Add the default installation directory to the search path: `SEARCH ADD SYS:\SWEEP\`
 - b) Then type `LOAD SWEEP`

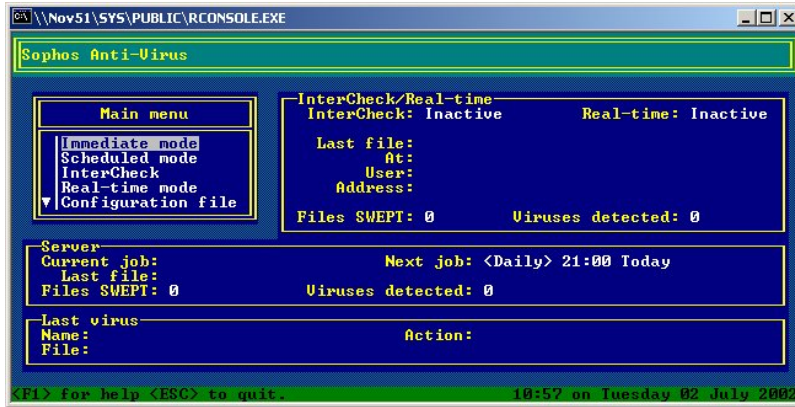
Sophos recommends that you add these commands in the same order to the AUTOEXEC.NCF file, so that Sophos Anti-Virus will be restarted if the server is restarted.
2. The first time you load Sophos Anti-Virus, it prompts you to enter Administrator details. Press any key.
3. At the login prompt, type the fully qualified distinguished name of an Administrator, and press **Return**.

```
Enter administrator complete name (e.g. CN=Admin.O=Company)
cn=admin.o=sophos
```

4. Type the Administrator password and press **Return**.

Make a note of the fully qualified distinguished name of the Administrator and (in a secure place) the password. Sophos Anti-Virus will log in as this user every time it is started, enabling it to see the complete eDirectory tree.

The **Sophos Anti-Virus** screen is displayed.



You have loaded Sophos Anti-Virus. From now on Sophos Anti-Virus will be updated automatically.

25 Protect UNIX computers with Sophos Anti-Virus version 4

Sophos provides two versions of Sophos Anti-Virus for UNIX.

Version 4:

- Supports a wide range of platforms.
- Cannot be managed using Enterprise Console.

Version 7:

- Supports a narrow range of platforms.
- Can be managed using Enterprise Console.
- Can be automatically updated.
- Can be scheduled to scan.

For information about the platforms that are supported by each version, go to the system requirements page of the Sophos website (<http://www.sophos.com/products/all-sysreqs.html>).

To protect computers with version 7, see [Protect UNIX computers with Sophos Anti-Virus version 7](#) (page 49) instead of this section.

To protect UNIX computers, you must:

- Use Enterprise Console and EM Library to download Sophos Anti-Virus for UNIX to a central installation directory (CID).
- Install Sophos Anti-Virus from the CID.

25.1 Download Sophos Anti-Virus for UNIX

If you have not already downloaded the Sophos Anti-Virus for UNIX software, follow these steps:

1. Go to the Windows computer where you installed Enterprise Console. Open Enterprise Console and click the **Libraries** icon.
2. In Sophos EM Library, select **Library|Select Packages**.
3. In the **Select Packages** dialog box, do as follows:
 - a) Ensure that you have cleared the **Show default packages only** check box.
 - b) Select the **Sophos Anti-Virus for <platform>** package, where <platform> is your UNIX platform. Click **OK**.
4. On the **Library** menu, select **Download Packages**.

By default, Sophos EM library creates a shared central installation directory (CID) for the latest Sophos software at \\Servername\InterChk\<platform>.
5. Share the CID, to enable your UNIX computers to access it and update from it.

Refer to the documentation for your Windows operating system for detailed information about sharing a directory. For example:

- *If the CID is located on a computer running Windows Server 2003 R2*, use Microsoft Services for NFS to enable access to the CID by UNIX clients. For more information, refer to the documentation for Services for NFS on Windows Server 2003 R2.
- *If the CID is located on a computer running Windows XP*, using Windows Services for UNIX, share the CID as NFS share and then mount it on UNIX. For more information, refer to the documentation for Windows Services for UNIX.

Now install Sophos Anti-Virus on a UNIX computer.

25.2 Install Sophos Anti-Virus

1. Go to the root of the directory where EM Library has placed the Sophos Anti-Virus files (the CID).
2. Copy the file `emininstall.sh` into an executable path location such as `/etc` on each UNIX client. From now on, this location is shown as `<path>`.
3. Enter `cd <path>`
4. To change the permissions, enter `chmod +x emininstall.sh`
5. Create a file called `/etc/emininstall.conf`
6. Add the following lines to it:

```
EM install CID=<install_cid>
EM cache dir=<cache_path>
SAV install dir=<install_path>
```

`<install_cid>` is the location of the CID.

`<cache_path>` is the location of the cache where a copy of the installation files is placed when performing an update.

`<install_path>` is the root location where Sophos Anti-Virus is going to be installed, or has previously been installed.

Note: The files in `<cache_path>` must not be deleted as this will cause them to be downloaded again. For this reason, you should not place the files in the `/tmp` directory, which is sometimes purged by the UNIX system.

7. Run
`emininstall.sh`
8. Create a cron job to run `emininstall` periodically. This will check for updates and install them automatically. See support knowledgebase article 12176 (<http://www.sophos.com/support/knowledgebase/article/12176.html>).

26 Protect UNIX computers with Sophos Anti-Virus version 7

Sophos provides two versions of Sophos Anti-Virus for UNIX.

Version 4:

- Supports a wide range of platforms.
- Cannot be managed using Enterprise Console.

Version 7:

- Supports a narrow range of platforms.
- Can be managed using Enterprise Console.
- Can be automatically updated.
- Can be scheduled to scan.

For information about the platforms that are supported by each version, go to the system requirements page of the Sophos website (<http://www.sophos.com/products/all-sysreqs.html>).

To protect computers with version 4, see [Protect UNIX computers with Sophos Anti-Virus version 4](#) (page 47) instead of this section.

To protect UNIX computers, you can use one of the following methods:

- Install Sophos Anti-Virus using a deployment package.
- Download and use a tarball.

If you have an earlier version of Sophos Anti-Virus or a third-party product using SAV Interface, read the following subsections.

Working with an earlier version of Sophos Anti-Virus

If you install Sophos Anti-Virus for UNIX, version 7 on a computer where Sophos Anti-Virus, version 4 is installed, this will not uninstall Sophos Anti-Virus 4. If you want to remove Sophos Anti-Virus 4 from the computer, uninstall it before installing Sophos Anti-Virus 7.

If you uninstall Sophos Anti-Virus 4, Sophos Anti-Virus 7 will install the **sweep** command as well as **savscan**. You can use either command for on-demand scans. Both commands will send reports to Enterprise Console.

If you do not uninstall Sophos Anti-Virus 4 before installing Sophos Anti-Virus 7, both versions will coexist on the computer. In this case, **sweep** will start a Sophos Anti-Virus 4 on-demand scan and will not report to Enterprise Console. To scan on demand with Sophos Anti-Virus 7, use **savscan**. Sophos Anti-Virus 4 will not be updated by the Sophos Anti-Virus 7 updating mechanism.

Working with an earlier version of Sophos Anti-Virus and a third-party product using SAV Interface

When Sophos Anti-Virus for UNIX, version 7 is installed on a computer which has an earlier version of Sophos Anti-Virus installed, together with a third-party product using SAV Interface,

it may be necessary to edit the Sophos Anti-Virus configuration file `sav.conf` to specify the correct path to the shared Sophos Anti-Virus libraries (`libsavi.*`).

After installing Sophos Anti-Virus 7, open the `/etc/sav.conf` file in a text editor. If necessary, edit the file to specify the correct path to the `libsavi.*` files. Check that the correct location is given for the SAV virus data directory. The default location is *Sophos Anti-Virus 7 install path/lib/sav*.

26.1 Protect UNIX computers using a deployment package

To protect UNIX computers, you must:

- Use Enterprise Console and EM Library to download Sophos Anti-Virus for UNIX to a central installation directory (CID).
- Install Sophos Anti-Virus on a UNIX computer for the first time manually.
- Update the computer to download the `mkinstpkg` script used to create a deployment package.
- Create a deployment package.
- Install Sophos Anti-Virus on the UNIX computer(s) using the deployment package.

26.1.1 Download Sophos Anti-Virus for UNIX

If you have not already downloaded the Sophos Anti-Virus for UNIX software, follow these steps:

1. Go to the Windows computer where you installed Enterprise Console. Open Enterprise Console and click the **Libraries** icon.
2. In Sophos EM Library, select **Library|Select Packages**.
3. In the **Select Packages** dialog box, do as follows:
 - a) Ensure that you have cleared the **Show default packages only** check box.
 - b) Select the **Sophos Anti-Virus for <platform> (Manageable)** package, where `<platform>` is your UNIX platform. Click **OK**.
4. On the **Library** menu, select **Download Packages**.

By default, Sophos EM library creates a shared central installation directory (CID) for the latest Sophos software at `\\Servername\InterChk\EESAVUNIX`.

5. Share the CID, to enable your UNIX computers to access it and update from it.

Refer to the documentation for your Windows operating system for detailed information about sharing a directory. For example:

- *If the CID is located on a computer running Windows Server 2003 R2*, use Microsoft Services for NFS to enable access to the CID by UNIX clients. For more information, refer to the documentation for Services for NFS on Windows Server 2003 R2.
- *If the CID is located on a computer running Windows XP*, using Windows Services for UNIX, share the CID as NFS share and then mount it on UNIX. For more information, refer to the documentation for Windows Services for UNIX.

Now Install Sophos Anti-Virus on a UNIX computer for the first time manually and update it.

26.1.2 Install Sophos Anti-Virus for the first time

To install Sophos Anti-Virus on a UNIX computer for the first time manually, follow these steps:

1. Log on to your UNIX server as root.
2. Mount the shared CID in which the Sophos Anti-Virus for UNIX software has been placed.

By default, this directory is `\InterChk\EESAVUNIX\<platform>` on the server where Enterprise Console is installed.

3. Change to the CID.
4. Run the install script:

```
./install.sh
```
5. When prompted, choose to enable remote management.
6. If you have not done so already, in Enterprise Console create a new group where you want to put the UNIX computer.
7. Drag the computer from the **Unassigned** folder and drop it onto the group.
8. If you have not already set up updating for UNIX computers in Enterprise Console, follow these steps:

- a) In the **Policies** pane, double-click **Updating** and then double-click the policy you want to update.
- b) In the **Updating policy** dialog box, select **UNIX** and click **Configure**.
- c) On the **Primary server** tab, in the **Address** field enter the directory from which computers will fetch updates, for example:

```
\\Servername\InterChk\EESAVUNIX
```

- d) Enter the **User name** and **Password** for the account that will be used for updating.

9. On the UNIX computer, trigger the first update:

```
/opt/sophos-av/bin/savupdate
```

Now you are ready to create a deployment package.

26.1.3 Create a deployment package

After you install Sophos Anti-Virus on the computer and update it for the first time, you can create a deployment package for your end-users.

You can use the **mkinstpkg** script to create a deployment package in tar format. This script prompts you for information about how Sophos Anti-Virus will be installed on your UNIX computers, and the answers gathered are inserted into the deployment package. When the end-user installs from this deployment package, it will not prompt for any information and will set up both the update location and credentials correctly.

Note: The **mkinstpkg** script is for use within your organization only. Please read the license agreement and legal notice displayed by the **mkinstpkg** script.

1. On the UNIX computer where you installed Sophos Anti-Virus, change to the directory

```
/opt/sophosav/update/cache/Primary-unpacked
```

2. To create a deployment package called savinstpkg.tar, run

```
./mkinstpkg.sh
```

3. When prompted, choose to have the computers managed by Enterprise Console.

4. When prompted for the location, enter the location of the CID:

```
\\Servername\InterChk\EESAVUNIX
```

Now you are ready to install Sophos Anti-Virus using this deployment package.

26.1.4 Install Sophos Anti-Virus using the deployment package

You can install Sophos Anti-Virus from the deployment package as follows:

1. Use your own tools to copy the deployment package to the computers where you want to install Sophos Anti-Virus.
2. Go to each computer and log in as root.
3. Place the deployment package in a temporary directory and change to that directory.
4. To perform the installation, untar the tar package and run the install script. Enter:

```
tar -xvf savinstpkg.tar  
./sophos-av/install.sh
```

This copies the necessary files from the server and installs Sophos Anti-Virus. From now on, Sophos Anti-Virus will be updated automatically whenever the CID is updated.

26.2 Protect UNIX computers using a tarball

To update your UNIX computers and manage them from Enterprise Console after the installation, you must:

- Create a shared update location (the central installation directory or CID).
By default, this directory is the \InterChk\EESAVUNIX directory on the server where Enterprise Console is installed.
- Set up updating for UNIX computers in Enterprise Console.

Then you can install Sophos Anti-Virus on UNIX computers and manage them from Enterprise Console.

26.2.1 Create a central installation directory

If you have not already created a central installation directory, follow these steps:

1. Go to the Windows computer where you installed Enterprise Console. Open Enterprise Console and click the **Libraries** icon.
2. In Sophos EM Library, select **Library|Select Packages**.
3. In the **Select Packages** dialog box, do as follows:
 - a) Ensure that you have cleared the **Show default packages only** check box.
 - b) Select the **Sophos Anti-Virus for <platform> (Manageable)** package, where <platform> is your UNIX platform. Click **OK**.
4. On the **Library** menu, select **Download Packages**.

By default, Sophos EM library creates a shared central installation directory (CID) for the latest Sophos software at \\Servername\InterChk\EESAVUNIX.

26.2.2 Set up updating

If you have not already set up updating for UNIX computers in Enterprise Console, follow these steps:

1. In the **Policies** pane, double-click **Updating** and then double-click the policy you want to update.
2. In the **Updating policy** dialog box, select **UNIX** and click **Configure**.

3. On the **Primary server** tab, in the **Address** field, enter the directory from which computers will fetch updates, for example:

```
\\Servername\InterChk\EESAVUNIX
```

4. Enter the **User name** and **Password** for the account that will be used for updating.

26.2.3 Install Sophos Anti-Virus using a tarball

1. Log on to your UNIX server as root.
2. Download the Sophos Anti-Virus for UNIX tarball from the Sophos Anti-Virus for UNIX download web page to a temporary directory.
3. Change to the temporary directory and untar the tarball:

```
tar -xvf <tarball>
```

4. Run the install script:

```
./sophos-av/install.sh
```

5. When prompted for an update location, enter the managed CID address or UNC path.

Your UNIX computer will become managed after the first update.

Note: You can start an update immediately by entering:

```
/opt/sophos-av/bin/savupdate
```

27 Protect 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” setup program. The software is then kept up to date via the internet. There are three possible approaches:

- The user can download the software from Sophos. Thereafter it is updated automatically from the same location. See support knowledgebase article 12391 (<http://www.sophos.com/support/knowledgebase/article/12391.html>).
- You can republish the software and all subsequent updates on your own website. The user downloads the software and updates from that site. For information on how to republish Sophos updates on your own website, see support knowledgebase article 12134 (<http://www.sophos.com/support/knowledgebase/article/12134.html>).
- You can copy the software onto a CD and send it to the user. The user installs the software and configures it to update from the location you prefer. See support knowledgebase article 13093 (<http://www.sophos.com/support/knowledgebase/article/13093.html>).

27.1 What standalone users will need

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

- The location from which they can download Sophos Anti-Virus (unless you are providing it on CD).
- The Sophos Endpoint Security and Control standalone startup guide. This is an electronic document available from the Sophos website or the Sophos Endpoint Security and Control Network Install CD.
- The username and password they need (whether they are downloading from Sophos directly or from your own web site).

When you send the username and password, note the following:

- Do not send the credentials to an infected computer by email, as they might be stolen.
- If necessary, send credentials by fax or letter post.
- For Sophos credentials, the correct username begins with “em”.

28 Protect computers with a command-line installation

You can protect computers by running the installation program manually from a command line.

Note: If you have a previous version of Sophos Anti-Virus on Windows 95, 98 or Me, you must uninstall it before installing the latest version.

1. Locate setup.exe in the central installation directory.
2. Run setup.exe with the relevant options (see below).

28.1 Command-line options for the installer program

By default, the installation program install anti-virus software. You can also use command-line options to install other security software or remove third-party software.

Note: Sophos Client Firewall and Sophos Network Access Control (NAC) are available only for Windows 2000 or later.

Note: Third-party software removal uninstalls only products with the same functionality as those you install.

-scf	installs the firewall
-nac http://<nacserveraddress>	installs network access control and specifies the address of the Sophos NAC server
-crt R	removes third-party security software automatically

29 Protect computers with a script

This section describes in brief how to protect computers by using a script.

You can protect computers with anti-virus software (and with the firewall if your licence includes it) by running the installation program with a script or a program like Microsoft SMS.

Enterprise Console will subsequently manage and update these installations, provided that you have put the computers into a group or groups.

You need to:

- Find the appropriate installation program.
- Follow the instructions for your operating system or systems.

29.1 Finding the installation program you need

The installation program is in the directory where EM Library places Sophos updates. To check which directory this is, look in the computer list and find the computer(s) you want to protect. Click the **Update details** tab and look in the “Primary server” column.

29.2 Protect Windows 95/98/Me computers

For Windows 95/98/Me computers, use a login script to run setup.exe.

Add the following line to the login script:

```
<Path>\setup.exe -user <domain\name> -pwd <password> -login -s
```

where <Path> is the location of the central installation directory.

Note: If you have any Windows 95 computers, you must install the Windows Sockets 2 update on them before installation. You should visit <http://download.microsoft.com/download/0/e/0/0e05231b-6bd1-4def-a216-c656fbd22b4e/W95ws2setup.exe> and place a copy of the update on your server. Then insert a line in the login script, before the line shown above, to run this utility.

Note:

If you want to force a reinstallation of Sophos Anti-Virus, use **-rlogin** instead of **-login**.

The user account you specify must be able to

- log on to the computers you want to protect
- have read access to the central installation directories (see details in [Protect computers](#) (page 21)).

If you want to remove third-party security software automatically, run the setup program with the option **-crt R**.

29.3 Protect Windows 2000 or later computers

If you want to protect Windows 2000 or later computers with the firewall and/or network access control, as well as anti-virus software, you must:

- Ensure that you use the correct setup program. This is the setup program for Sophos Endpoint Security and Control and it is in a directory called SAVSCFXP.
- Run the setup program with the relevant options (see below).

Option	Description
-scf	Installs the firewall.
-nac http://<nacserveraddress>	Installs network access control and specifies the address of the Sophos NAC server.
-crt R	Removes third-party security software automatically.

29.4 Protect Mac OS X computers

For Mac OS X computers, use Apple Remote Desktop. Go to the central installation directory and copy the installer to the computer running Apple Remote Desktop before using it.

30 Appendix: Advanced setup

After you install Sophos Enterprise Console, you are offered a **Quick setup** or an **Advanced setup**. If you choose **Advanced setup**, Sophos EM Library is displayed. The **Welcome to EM Library** view is open.

Follow the instructions in the following sections.

30.1 Create a software library

1. In the **Welcome to EM Library** view, click **Create library**.
2. In the **Setup - EM Library (Welcome)** dialog box, **Local Installation** is selected by default. Click **Next**.
If you want to install a library on a remote computer, select **Remote Installation** and follow the instructions.
3. In the **Location** dialog box, you can specify the folder where the library is installed and the share name used for that folder. Click **Next**.
4. In the **Central Installation** dialog box, you specify the location of the shared folder where EM Library will place downloaded Sophos software, ready for distribution to networked computers. The share name and the local path to the folder are displayed. You can change the local path. Click **Next**.
5. In the **Install Files** dialog box, click **Install** to begin installing the library. A progress bar is displayed. When the process is complete, click **Finish**.

When installation is complete, a **SETUP** message box is displayed. Click **OK**. This starts a wizard that guides you through setting up an account that EM Library can use (see next section).

30.2 Select a user account

To select the account that EM Library uses to place software in central locations on your network:

1. In the **Welcome to the Network Account Configuration Wizard** dialog box, click **Next**.
2. In the **Select network account type** dialog box, specify an account and click **Next**.
 - *If you intend to have a single library and to let all computers update from the same “central installation directory,”* click **Create a new local account**. EM Library will create an account called EMLibUser1. This is a member of “Administrators.”
 - *If you intend to have multiple libraries, or central installation directories on other computers,* click **Select an existing account**. Enter the details of a domain account with domain Administrator rights.

For advice on setting up an account, go to the Sophos website and see support knowledgebase article 12522 (<http://www.sophos.com/support/knowledgebase/article/12522.html>).

Note: If your library is on a Windows NT domain controller server, you must select an account already created in the Domain User Manager.

3. In the **Enter account password** dialog box, enter and confirm the password. If you are using the EMLibUser1 account, you make up this password now. Click **Next**.
4. In the **Completing the Network Account Configuration Wizard** dialog box, click **Finish**.

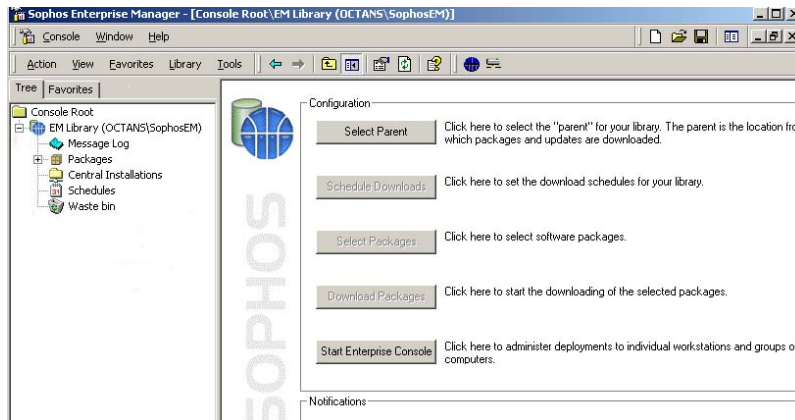
Now you set up automatic downloading of software (see next section).

30.3 Set the library to download updates automatically

Now you configure the library to download and update software automatically.

30.3.1 Select where you will download updates from

1. In the console, in the details pane, the **Configuration** view is displayed. Click **Select Parent**. The parent is the location from which you download software.



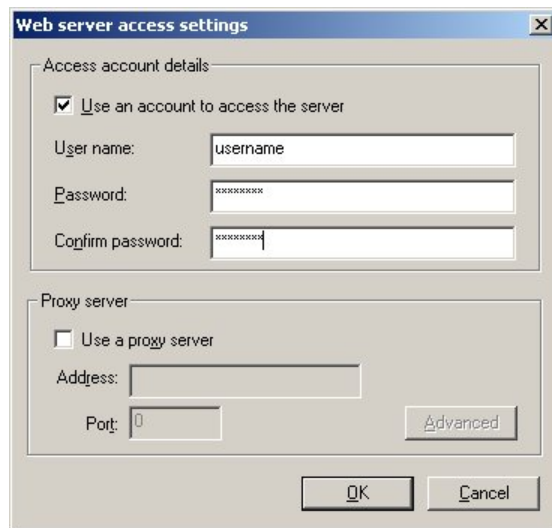
2. In the **Primary parent** tabbed page, select **Website**. Click the drop-down arrow and select <http://es-latest-3.sophos.com/update/>. Click **Set access**.



3. In the **Web server access settings** dialog box, do as follows:

- a) Select **Use an account to access the server**.
- b) Enter the EM Library **User name** and **Password** that Sophos has given you. Both are case sensitive.
- c) If you access the internet through a proxy server, select **Use a proxy server** and enter the server's address and port number. If you need to enter credentials to use the proxy, click **Advanced** and enter the proxy username and password.

If you access the internet via a dial-up connection, make sure you have changed your internet connection settings as described in *EM Library supplement for companies with a dial-up connection to the internet*.



EM Library attempts to validate your account details. If it cannot (for example, because the details are incorrect, or because no network connection has been made), it prompts you to make changes and try again.

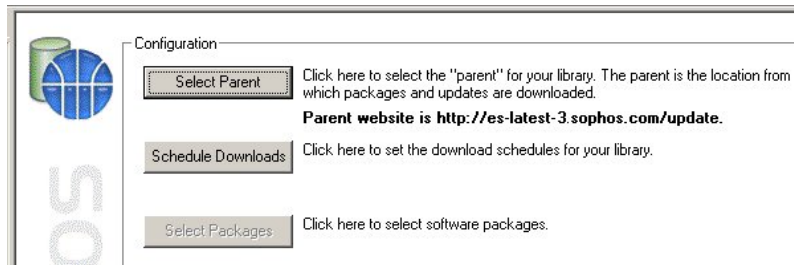
When the account details are validated, the primary parent is displayed in the **Configuration** view.

Next you schedule downloads (see next section).

30.3.2 Schedule the downloads

To schedule downloads:

1. In the **Configuration** view, click **Schedule Downloads**.



2. In the **Update schedules** tabbed page, click **New schedule**. A wizard guides you through the steps for creating a schedule.

In the **Schedule type** dialog box, Sophos recommends that you select **Frequent updates**, as this ensures that you have the most up-to-date protection possible.

3. When the schedule has been set up, it is displayed in the list on the **Update schedules** tabbed page. Ensure that the check box beside it is selected and click **OK**.

Note: You can activate only one schedule (by selecting its check box) at a time.

Next select the software you want EM Library to download and update (see next section).

30.3.3 Select the software you want to download

1. In the **Configuration** view, click **Select Packages**.

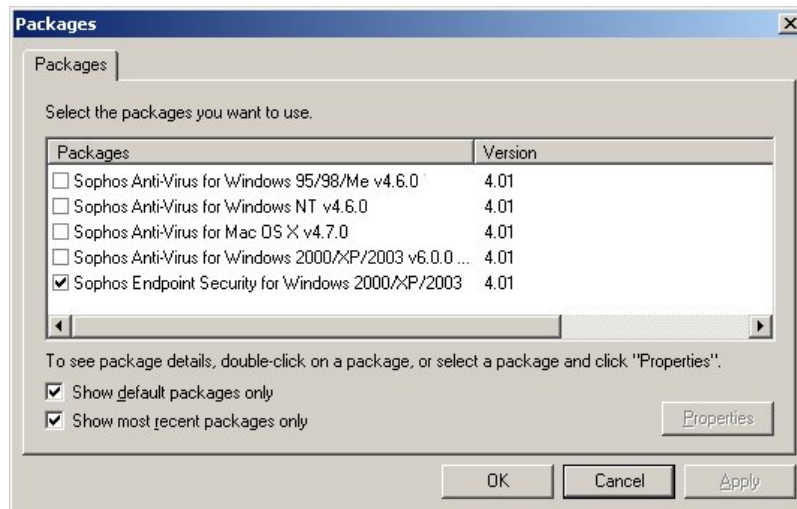
Packages are the files needed to install and update Sophos Anti-Virus and Sophos Client Firewall. There is a package for each operating system.

2. In the **Packages** dialog box, the default packages for Windows and Mac are shown. Do as follows:

- a) If you need to see other packages, for example, for Linux, clear the **Show default packages only** check box.

- b) Select the check box(es) beside the packages you want. Click **OK**.

The Sophos Endpoint Security and Control package includes Sophos Anti-Virus, Sophos Client Firewall, and Sophos Network Access Control.



When EM Library downloads software, it places it in central installation directories (CIDs), from which it can be distributed across your network. By default, EM Library creates these CIDs on the same computer as the library, and assigns the correct access rights to them.

Note: If you want to place downloads in a different folder, you can find instructions in the EM Library help files. Open the “How do I make updates available on the network?” section and click “Change where updates are placed.”

Note: If the CIDs are on a computer with FAT partition, you must set the access rights for that share manually, as follows: Read for Everyone, Full access for Administrator and Full access for the selected EEM Library network account.

Now download the software for the first time (see next section).

30.4 Download software

Now download Sophos software and place it in a central installation directory or directories, as follows:

1. In the **Configuration** view, click **Download Packages**.
2. In the **EM Library** message box, click **Yes**.

The **Updating packages from the parent** progress bar is displayed.

When downloading is complete, the **Updating your central installations** progress bar is displayed.

You are ready to pre-configure your anti-virus software and install it on your networked computers.

If you want to install and manage the software from another computer, for example, a workstation, go to that computer and read [Set up a remote management console](#) (page 14).

If you want to do everything from this computer, click the **Start Enterprise Console** button in the **Configuration** view and go to [Create groups for your computers](#) (page 16).

31 Technical support

For technical support, visit <http://www.sophos.com/support>.

If you contact technical support, provide as much information as possible, including the following:

- Sophos software version number(s)
- Operating system(s) and patch level(s)
- The exact text of any error messages

32 Copyright

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

Sophos and Sophos Anti-Virus are registered trademarks of Sophos Plc and Sophos Group. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

OpenSSL cryptographic 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

Copyright © 1998–2006 The OpenSSL Project. All rights reserved.

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 SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS” AND ANY EXPRESSED 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 OpenSSL PROJECT OR ITS 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.

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

Copyright © 1995–1998 Eric Young (eay@cryptsoft.com) All rights reserved.

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 licence 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 licence [including the GNU Public Licence.]

ACE™, TAO™, CIAO™, and CoSMIC™

ACE¹, TAO², CIAO³, and CoSMIC⁴ (henceforth referred to as “DOC software”) are copyrighted by Douglas C. Schmidt⁵ and his research group⁶ at Washington University⁷, University of California⁸, Irvine, and Vanderbilt University⁹, Copyright © 1993–2005, all rights reserved.

Since DOC software is open-source¹⁰, free software, you are free to use, modify, copy, and distribute—perpetually and irrevocably—the DOC software source code and object code produced from the source, as well as copy and distribute modified versions of this software. You must, however, include this copyright statement along with code built using DOC software.

You can use DOC software in commercial and/or binary software releases and are under no obligation to redistribute any of your source code that is built using DOC software. Note, however, that you may not do anything to the DOC software code, such as copyrighting it yourself or claiming authorship of the DOC software code, that will prevent DOC software from being distributed freely using an open-source development model. You needn’t inform anyone that you’re using DOC software in your software, though we encourage you to let us¹¹ know so we can promote your project in the DOC software success stories¹².

DOC software is provided as is with no warranties of any kind, including the warranties of design, merchantability, and fitness for a particular purpose, noninfringement, or arising from a course of dealing, usage or trade practice. Moreover, 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 companies¹³ 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.

Washington University, UC Irvine, Vanderbilt University, their employees, and students shall have no liability with respect to the infringement of copyrights, trade secrets or any patents by DOC software or any part thereof. Moreover, in no event will Washington University, UC Irvine, or Vanderbilt University, their employees, or students be liable for any lost revenue or profits or other special, indirect and consequential damages.

The ACE¹⁴, TAO¹⁵, CIAO¹⁶, and CoSMIC¹⁷ web sites are maintained by the DOC Group¹⁸ at the Institute for Software Integrated Systems (ISIS)¹⁹ and the Center for Distributed Object Computing of Washington University, St. Louis²⁰ for the development of open-source software as part of the open-source software community²¹. By submitting comments, suggestions, code, code snippets, techniques (including that of usage), and algorithms, submitters acknowledge that they have the right to do so, that any such submissions are given freely and unreservedly, and that they waive any claims to copyright or ownership. In addition, submitters acknowledge that any such submission might become part of the copyright maintained on the overall body of code, which comprises the DOC software. By making a submission, submitter agree to these terms. Furthermore, submitters acknowledge that the incorporation or modification of such submissions is entirely at the discretion of the moderators of the open-source DOC software projects or their designees.

The names ACE, TAO, CIAO, 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. Further, products or services derived from this source may not be called ACE, TAO, CIAO, or CoSMIC nor may the name Washington University, UC Irvine, or Vanderbilt University appear in their names, without express written permission from Washington University, UC Irvine, and Vanderbilt University.

If you have any suggestions, additions, comments, or questions, please let me²² know.

Douglas C. Schmidt²³

The ACE home page is <http://www.cs.wustl.edu/ACE.html>

References

1. <http://www.cs.wustl.edu/~schmidt/ACE.html>
2. <http://www.cs.wustl.edu/~schmidt/TAO.html>
3. <http://www.dre.vanderbilt.edu/CIAO/>
4. <http://www.dre.vanderbilt.edu/cosmic/>
5. <http://www.dre.vanderbilt.edu/~schmidt/>
6. <http://www.cs.wustl.edu/~schmidt/ACE-members.html>
7. <http://www.wustl.edu/>
8. <http://www.uci.edu/>
9. <http://www.vanderbilt.edu/>
10. <http://www.the-it-resource.com/Open-Source/Licenses.html>
11. mailto:doc_group@cs.wustl.edu
12. <http://www.cs.wustl.edu/~schmidt/ACE-users.html>
13. <http://www.cs.wustl.edu/~schmidt/commercial-support.html>
14. <http://www.cs.wustl.edu/~schmidt/ACE.html>
15. <http://www.cs.wustl.edu/~schmidt/TAO.html>
16. <http://www.dre.vanderbilt.edu/CIAO/>
17. <http://www.dre.vanderbilt.edu/cosmic/>
18. <http://www.dre.vanderbilt.edu/>

19. <http://www.isis.vanderbilt.edu/>
20. <http://www.cs.wustl.edu/~schmidt/doc-center.html>
21. <http://www.opensource.org/>
22. <mailto:d.schmidt@vanderbilt.edu>
23. <http://www.dre.vanderbilt.edu/~schmidt/>