



# Sophos Endpoint Security and Control 9.5 advanced startup guide for Windows and Mac OS X

Document date: June 2010



# Contents

|   |    |
|---|----|
| 1 About this guide.....   | 3  |
| 2 Planning installation.....  | 4  |
| 3 System requirements.....  | 9  |
| 4 Deciding where to install the management tools.....   | 10 |
| 5 Installing the management tools with the databases on a separate server.....                | 14 |
| 6 Installing the management tools with an additional update manager on a separate server..... | 25 |
| 7 Publish security software on a web server.....  | 42 |
| 8 Create computer groups.....   | 43 |
| 9 Setting up security policies.....   | 44 |
| 10 Search for computers.....  | 48 |
| 11 Protecting Windows computers and Macs.....   | 49 |
| 12 Check the health of your network.....  | 54 |
| 13 Protecting standalone computers.....   | 55 |
| 14 Technical support.....   | 56 |
| 15 Legal notices.....   | 57 |

# 1 About this guide

This guide describes the advanced procedure for installing Sophos Endpoint Security and Control software on a complex network or one that has more than 1000 workstations. It covers installation on Windows computers and Macs.

To install on a simple network of less than 1000 Windows and Mac workstations, see the *Sophos Endpoint Security and Control 9.5 quick startup guide* instead of this guide.

To install on Linux, NetWare, and UNIX computers, see the *Sophos Endpoint Security and Control 9.5 startup guide for Linux, NetWare, and UNIX* as well as this guide.

To upgrade, go to the **Endpoint Security and Control 9.5 Upgrade Center** at <http://www.sophos.com/support/upgrades/>, instead of reading this guide.

Sophos documentation is published at <http://www.sophos.com/support/docs/>.

## 2 Planning installation

You protect your computers by following these key steps:

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

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

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

### 2.1 Planning the installation of management tools

The Sophos management tools are:

- **Sophos Enterprise Console (SEC).** This enables you to install and manage security software on your computers.
- **Sophos NAC Server.** This enables you to use network access control, which can prevent access by unauthorized computers or computers that do not comply with your security standards.

**Important:** We recommend that the servers on which you install SEC are in the same Active Directory forest as those on which you install NAC Server.

#### 2.1.1 Planning the installation of Enterprise Console

Enterprise Console includes four components:

|                           |  |
|---------------------------|--|
| <b>Management console</b> | Enables you to protect and manage computers.   |
| <b>Management server</b>  | Handles updating and communications.   |
| <b>Database</b>           | Stores data about computers on the network.  |
| <b>Update manager</b>     | Downloads Sophos software and updates from Sophos automatically to a central location. |

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

## Management console

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

- *Role-based access* to the management console involves setting up roles, adding rights to the roles, and then assigning Windows users and groups to the roles. For example, a Help Desk engineer can update or clean up computers, but cannot configure policies, which is the responsibility of an Administrator.
- *Sub-estates* can be used to restrict the computers and groups that users can perform operations on. You can split your IT estate into sub-estates and assign management console groups of computers to the sub-estates. You can then control access to the sub-estates by assigning Windows users and groups to them. The Default sub-estate contains all management console groups and the **Unassigned** group.

This guide explains how to install an additional management console. For advice about setting up role-based access and creating sub-estates, go to <http://www.sophos.com/support/bestpractice/esc>.

## Database

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

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

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

## Update manager

An update manager enables you to create shares that contain the endpoint software that you want to deploy. The computers that you want to protect update themselves from these shares. An update manager is always installed as part of Enterprise Console. However, you can install additional update managers on other servers and create additional shares to download and deploy software on larger networks. This guide explains how to install an additional update manager and create shares. For advice on how to organize update managers and shares on larger networks, go to <http://www.sophos.com/support/bestpractice/esc>.

### 2.1.2 Planning the installation of NAC Server

If you want to use Sophos Network Access Control (NAC), you need to install NAC Server. It includes two components:

|                             |   |
|-----------------------------|---|
| <b>Sophos NAC Manager</b>   | Enables you to manage and configure NAC on your network.                |
| <b>Sophos NAC databases</b> | Store NAC data about your network, which is viewable using NAC Manager. |

**Important:** If you install the components on different servers, the servers must be joined to the same domain.

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

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

To help you decide, the approximate sizes of the databases are shown in the following tables:

| Number of workstations | ReportStore database size guidelines |
|------------------------|--------------------------------------|
| 1500                   | 300 MB                               |
| 3000                   | 379 MB                               |
| 5000                   | 485 MB                               |
| 7500                   | 616 MB                               |
| 10,000                 | 748 MB                               |
| 15,000                 | 1011 MB                              |
| 20,000                 | 1274 MB                              |
| 25,000                 | 1536 MB                              |

| Number of workstations | ReportStore log size guidelines |
|------------------------|---------------------------------|
| 1500                   | 150 MB                          |
| 3000                   | 206 MB                          |
| 5000                   | 281 MB                          |
| 7500                   | 374 MB                          |
| 10,000                 | 467 MB                          |
| 15,000                 | 653 MB                          |
| 20,000                 | 839 MB                          |

| Number of workstations | ReportStore log size guidelines |
|------------------------|---------------------------------|
| 25,000                 | 1024 MB                         |

This guide explains how to install the databases either on the same server as NAC Manager or on the same server as the Enterprise Console database.

NAC supports HTTPS communication between NAC Server and Sophos Compliance Agent. Compliance Agent is installed on workstations and assesses them for compliance. If you want to enable HTTPS with NAC, contact Sophos technical support. For information about contacting technical support, see [Technical support](#) (page 56). This must be done before you begin installation.

## 2.2 Planning the computer groups

You need to decide how to group the computers that you want to protect. For advice, go to <http://www.sophos.com/support/bestpractice/esc>.

## 2.3 Planning the security policies

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

When you create groups, Enterprise Console applies default policies to them. You can edit these policies or create new ones, as explained in this guide. For advice about what settings to use, see the *Sophos Endpoint Security and Control 9.5 policy setup guide*.

## 2.4 Planning the search for networked computers

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

## 2.5 Planning how to protect computers

You can install security software automatically from Enterprise Console on Windows 2000 or later.

**Note:** You cannot install Sophos Client Firewall or Sophos Compliance Agent on computers running server operating systems.

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

- Windows

■ Mac OS X

The *Sophos Endpoint Security and Control 9.5 startup guide for Linux, NetWare, and UNIX* gives details of manual installation for other operating systems.

## 3 System requirements

The following Microsoft system software must be installed to enable the Enterprise Console installer to run:

- Microsoft Windows Installer version 4.5, patched to KB958655
- Security Update for Microsoft XML Core Services 6.0
- Microsoft .NET Framework 3.5 SP1
- Microsoft SQL Server 2005 Express Edition

If you do not already have these, or later, versions of the Microsoft system software, the Enterprise Console installer will install them for you.

Before you install the NAC databases, you must ensure that you have the appropriate version of SQL Server installed on the server on which you want to install the databases:

- For installations up to 1500 workstations, we recommend that you use SQL Server 2005/2008 Express. Such databases are limited to 4 GB.
- For installations over 1500 workstations, we recommend that you use SQL Server 2005/2008.

For a list of system requirements for Sophos Enterprise Console and Sophos Network Access Control, see the release notes for those products.

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

### Notes

The installer installs SQL Server 2008 Express, unless you already have SQL Server 2005 Express or later. SQL Server 2008 Express is not compatible with Windows Server 2003 SP1 or Windows Essential Business Server 2008. On Windows Server 2008 R2 Datacenter, you must raise the domain functional level to Windows Server 2003, as explained at <http://support.microsoft.com/kb/322692>.

The installer cannot install .NET Framework 3.5 on a server running Windows Server 2008 R2. You must add it from the Features section of Server Manager.

After you install the required system software, you may need to restart your computers. For more information about computer restart requirements, see Sophos support knowledgebase article 65190 (<http://www.sophos.com/support/knowledgebase/article/65190.html>).

## 4 Deciding where to install the management tools

The Sophos management tools are Sophos Enterprise Console (SEC) and NAC Server.

SEC includes four components:

|                           |  |
|---------------------------|--|
| <b>Management console</b> | Enables you to protect and manage computers.   |
| <b>Management server</b>  | Handles updating and communications.   |
| <b>Database</b>           | Stores data about computers on the network.  |
| <b>Update manager</b>     | Downloads Sophos software and updates from Sophos automatically to a central location. |

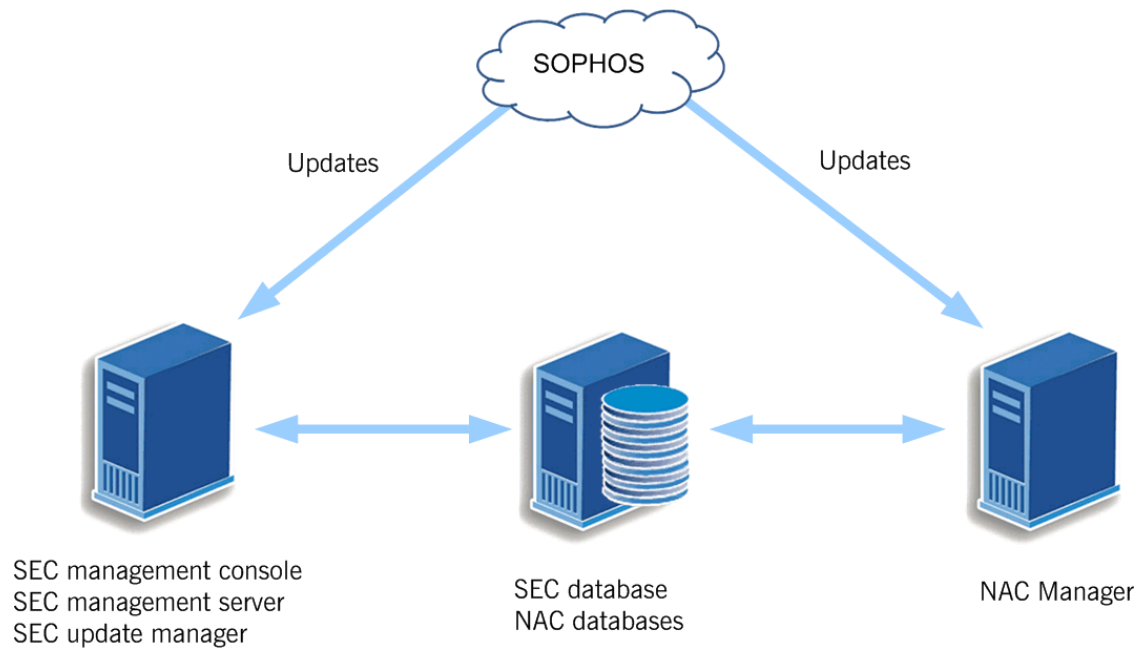
NAC Server includes two components:

|                             |   |
|-----------------------------|---|
| <b>Sophos NAC Manager</b>   | Enables you to manage and configure NAC on your network.                |
| <b>Sophos NAC databases</b> | Store NAC data about your network, which is viewable using NAC Manager. |

**Note:** If you do not want to use network access control, you do not have to install the NAC Server components.

This guide covers two installation scenarios. In each scenario, the management tool components are distributed across the network differently.

### Databases installed on a separate server



**Note:** The servers on which you install the NAC databases and NAC Manager must be joined to the same domain.

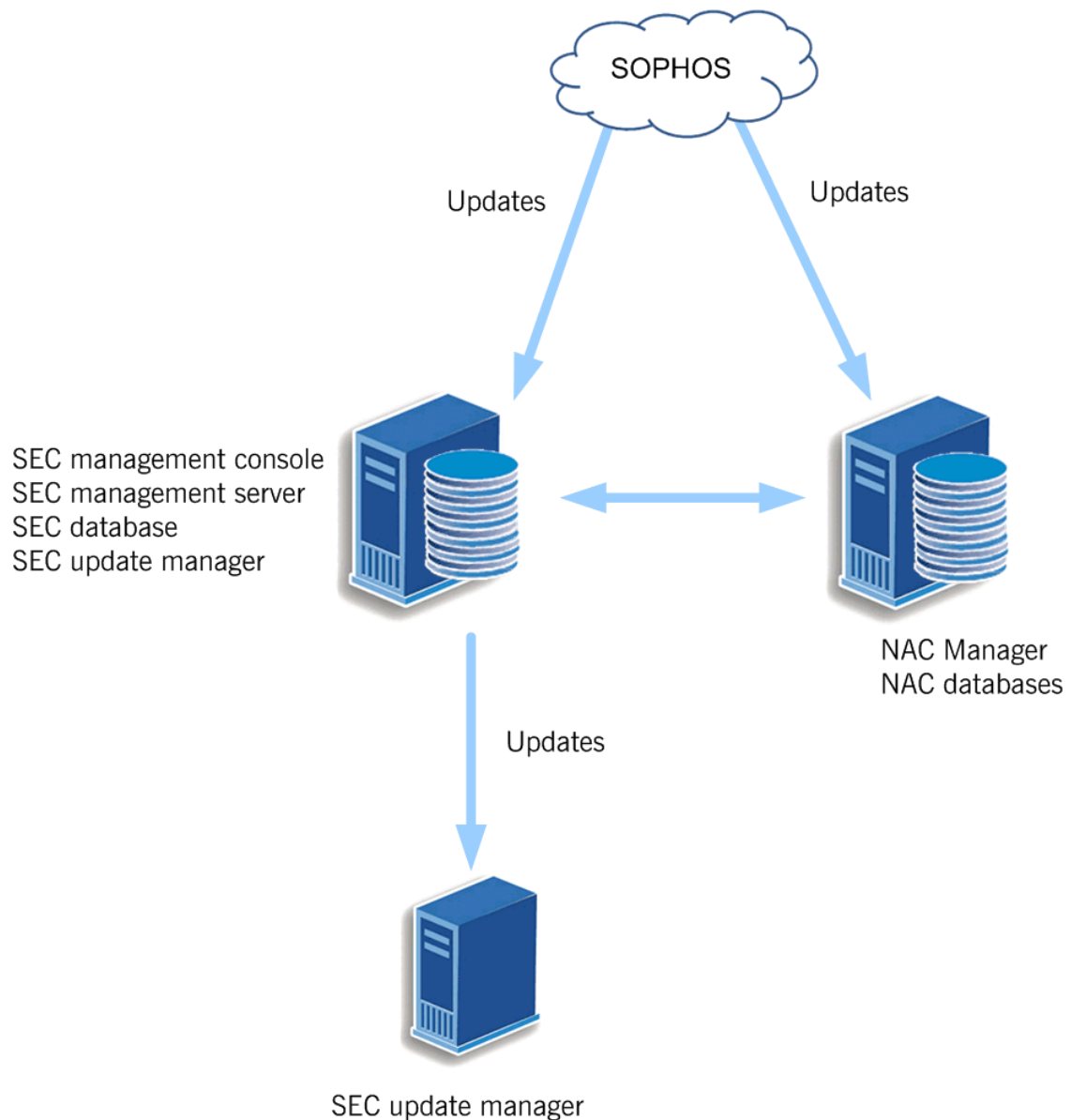
To follow this scenario, go to [Installing the management tools with the databases on a separate server](#) (page 14).

### Additional update manager installed on a separate server

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

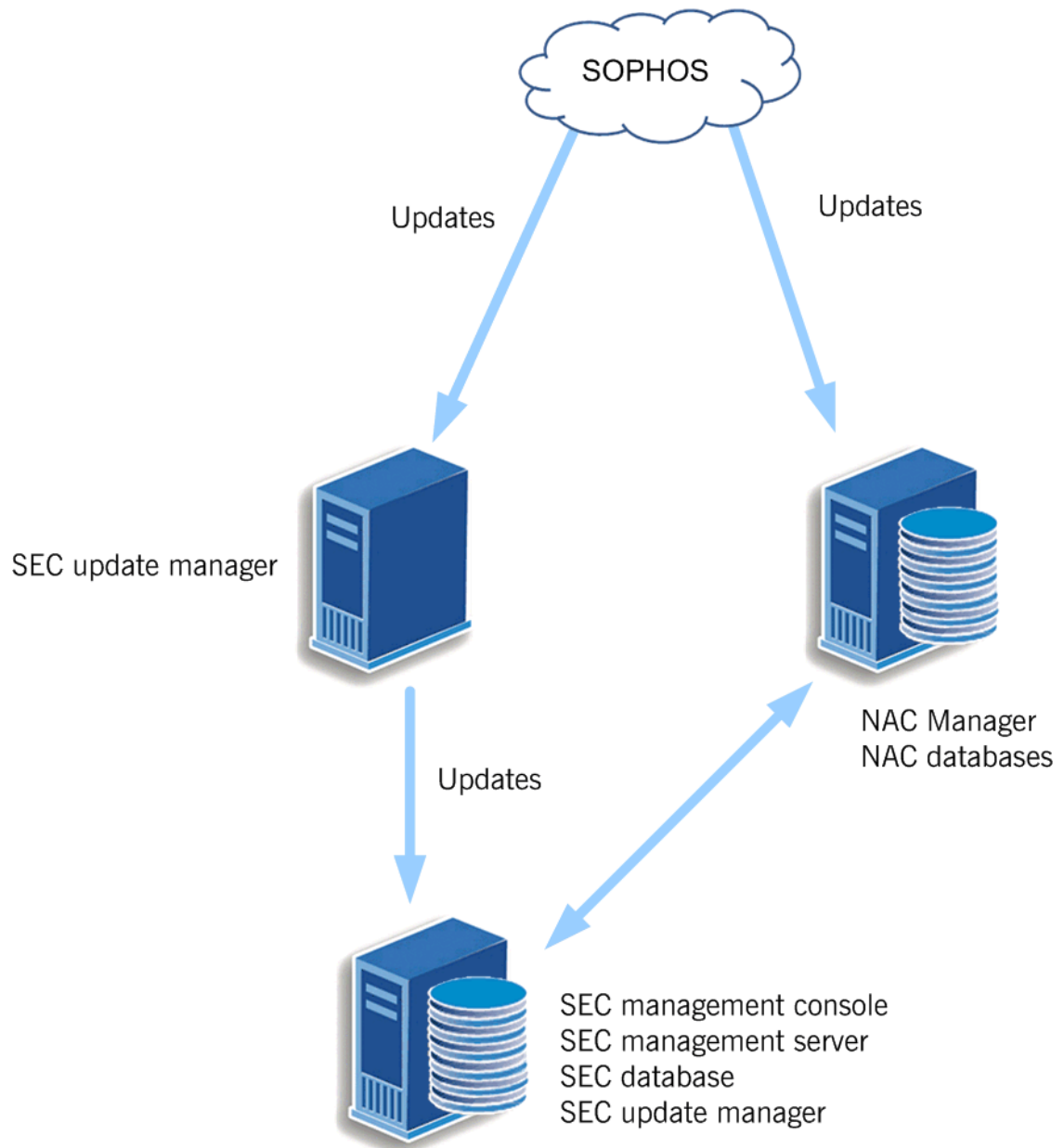
The first method is to:

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



The second method is to:

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



Regardless of which method you choose, to follow this scenario, go to [Installing the management tools with an additional update manager on a separate server](#) (page 25).

## 5 Installing the management tools with the databases on a separate server

### 5.1 Download the installers

1. Go to <http://www.sophos.com/support/updates/>.
2. Type your MySophos username and password.
3. On the web page for Endpoint Security and Data Protection downloads, download the Enterprise Console installer.
4. Download the NAC Manager installer.
5. Download the Sophos Compliance Dissolvable Agent installer.
6. Ensure that the installers are in a location that can be accessed from the servers on which you want to install the software.

Alternatively, copy them to a CD or DVD.

### 5.2 Install the NAC databases

The NAC installation wizard guides you through the installation of the NAC system requirements. As part of the NAC installation, you must have the appropriate operating system CD available to install certain system requirements. Other system requirements are installed automatically by the NAC installation wizard.

1. On the domain controller, manually create one standard domain account, specify that the password never expires, and specify that the user cannot change the password.  
The NAC installation wizard adds this account to the local administrators group on the NAC Manager server so that NAC Manager can access the NAC databases.
2. Go to the server on which you want to install the databases.
3. Locate the NAC installer that you downloaded earlier and double-click it.

An installation wizard starts.

4. Click **Install**.
5. On the **Welcome** page, click **Next**.
6. On the **Select Features** page, click **Advanced**.
7. Clear all check boxes, and then select the **Sophos NAC Databases** check box. Click **Next**.

If you want to change the folder where the scripts that create the NAC databases are installed, click **Browse**. If you want to change the SQL server instance that NAC will use, click **Select**. The **Select** button only appears when the NAC installer detects more than one SQL server instance.

8. On the **Service Account Information** page, type the service account information in the appropriate fields. Click **Next**.  
This is the standard domain account required by the NAC databases and NAC Manager. You created this service account in step 1.
9. On the **Sophos Download Account Details** page, type your Sophos download account details in the appropriate fields. Click **Next**.  
Sophos download account details are provided to you when you purchase Sophos NAC. The username and password are required to download the latest detection data for security applications. If you mistype the details, you can correct them later using NAC Manager. For more information, see the NAC Manager Help.
10. On the **Ready to Install** page, click **Install** to begin the installation.  
The NAC databases are configured, and the installation progress is displayed. A portion of the installation takes several minutes, during which time the progress indicator may not move. Do not cancel the installation, and it will progress.
11. Click **Finish**.  
**Important:** If installation errors occur, use the application event log to view additional information. If the database installation fails, you must delete the following databases if they have been created: AlertStore, AuditStore, GeneralStore, PolicyStore, ReportStore, and SecurityStore. Once you have deleted the databases, you can attempt a re-installation.

## 5.3 Sizing the NAC databases

For installations up to 1500 workstations, the NAC installation process sizes the NAC databases appropriately. You can skip this section.

For larger installations, you must increase the sizes of the NAC databases: the ReportStore database and the ReportStore log, as explained in this section.

### 5.3.1 ReportStore database sizing guidelines

Use this table to determine how to specify the size of the ReportStore database.

| Number of workstations | ReportStore database size guidelines |
|------------------------|--------------------------------------|
| 1500                   | 300 MB                               |
| 3000                   | 379 MB                               |
| 5000                   | 485 MB                               |
| 7500                   | 616 MB                               |

| Number of workstations | ReportStore database size guidelines |
|------------------------|--------------------------------------|
| 10,000                 | 748 MB                               |
| 15,000                 | 1011 MB                              |
| 20,000                 | 1274 MB                              |
| 25,000                 | 1536 MB                              |

### 5.3.2 ReportStore log sizing guidelines

Use this table to determine how to specify the size of the ReportStore log.

| Number of workstations | ReportStore log size guidelines |
|------------------------|---------------------------------|
| 1500                   | 150 MB                          |
| 3000                   | 206 MB                          |
| 5000                   | 281 MB                          |
| 7500                   | 374 MB                          |
| 10,000                 | 467 MB                          |
| 15,000                 | 653 MB                          |
| 20,000                 | 839 MB                          |
| 25,000                 | 1024 MB                         |

### 5.3.3 Change NAC database sizes – SQL Server 2005/2008

1. On the SQL Server **Start** menu, point to **Microsoft SQL Server 2005** or **Microsoft SQL Server 2008** as appropriate, and then click **SQL Server Management Studio**.
2. In SQL Server Management Studio, locate the ReportStore database in the Databases folder, right-click it, and click **Properties**.
3. In the **Properties** dialog box, select **Files**.
4. Locate the ReportStore\_Data file. In the **Initial Size (MB)** field, type an appropriate size for the database.
5. Locate the ReportStore\_Log file. In the **Initial Size (MB)** field, type an appropriate size for the log.

6. Click **OK**.
7. Close SQL Server Management Studio.

## 5.4 Install the SEC database

You install the database on the same server on which you installed the NAC databases.

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

If the server is in a *domain*, log on as a domain administrator.

If the server is in a *workgroup*, log on as a local administrator.

1. Locate the Enterprise Console installer that you downloaded earlier and double-click it.
2. Extract the installation files to the suggested destination folder or another one of your choice. The folder must be on this server.

An installation wizard starts.

3. In the **Sophos Enterprise Console** dialog box, click **Next**.

A wizard guides you through installation of Enterprise Console. Accept the default options, except as shown below.

On the **Setup Type** page, click **Custom**.

On the **Custom Setup** page, make sure that **Database** is selected and **Management console** and **Management server** are not selected.

On the **Database Connection User Account Details** page, enter the details of an account that can log onto both this server and the server on which you will install the Enterprise Console management server. If the servers are in a *domain*, you can use a domain account. If the servers are in a *workgroup*, use a local account that exists on both servers.

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

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

## 5.5 Install NAC Manager

Go to the server on which you want to install NAC Manager. Ensure that it is connected to the internet.

Log on using a domain account with local administrator privileges.

The NAC installation wizard guides you through the installation of the NAC system requirements. As part of the NAC installation, you must have the appropriate operating system CD available to

install certain system requirements. Other system requirements are installed automatically by the NAC installation wizard.

1. Locate the NAC installer that you downloaded earlier and double-click it.

An installation wizard starts.

2. Click **Install**.
3. On the **Welcome** page, click **Next**.
4. Do one of the following:
  - If a message is displayed that indicates that the NAC Application Server is the only NAC server that can be installed, click **OK**. On the **Select Features** page, click **Next**.
  - If the **Select Features** page is displayed straightaway, click **Advanced**. Clear all check boxes, and then select the **Sophos NAC Application Server** check box. Click **Next**.

If you want to change the folder where the NAC Manager files are installed, click **Browse**.

5. On the **Service Account Information** page, type the service account information in the appropriate fields. Click **Next**.

This is the standard domain account required by the NAC databases and NAC Manager. You created this service account in step 1 of the NAC databases installation.

6. On the **Sophos Database Server** page, type the NAC database server name. Click **Next**.

If, when you installed the NAC databases, you changed the SQL server instance that NAC will use, you must also type the instance name, in this format:

*server name\instance name*

7. On the **Server Proxy Settings** page, if you need to specify internet proxy settings for this server, click **Use Proxy**. The proxy can be the same as, or different to, the proxy specified in Enterprise Console. Click **Next**.

The username and password fields are required only when NAC Manager is using an authenticated proxy.

8. On the **Ready to Install** page, click **Install** to begin the installation.

NAC Manager is configured, and the installation progress is displayed. A portion of the installation takes several minutes, during which time the progress indicator may not move. Do not cancel the installation, and it will progress.

9. Click **Finish**.

**Note:** If installation errors occur, use the application event log to view additional information.

## 5.6 Install Compliance Dissolvable Agent on a web server

Sophos Compliance Dissolvable Agent is a client component of NAC that assesses a workstation for compliance. It is designed for users who do not, or cannot, have Sophos Compliance Agent

installed on their workstation, such as contractors or guests. To use it, you must first install Compliance Dissolvable Agent on a Windows web server that is accessible to users. Once installed, users download Compliance Dissolvable Agent using a browser.

**Note:** It does not matter if you install it on the same server as the one on which you installed NAC Manager or the NAC databases.

1. Locate the Compliance Dissolvable Agent installer that you downloaded earlier and double-click it.

An installation wizard starts.

2. On the **Welcome** page, click **Next**.
3. On the **Destination Folder** page, keep the default folder or click **Change** to select a different installation folder, as required. Click **Next**.
4. On the **Sophos Server** page, type the IP address or DNS name of the server on which you installed NAC Manager.

**Note:** If you change the NAC Manager server address later, you must re-install Compliance Dissolvable Agent on the web server and specify the new address during the installation.

5. If you are using HTTPS with NAC, select the **Secure Sophos Server (use HTTPS)** check box. The web certificate IP address or DNS name must be the same as the NAC Manager server.
6. Click **Next**.
7. On the **Ready to Install the Program** page, click **Install** to begin the installation.
8. Click **Finish**.

**Note:** If installation errors occur, use the application event log to view additional information.

If you install Compliance Dissolvable Agent in the default folder, workstations can access it using the following address: `http(s)://IP address or DNS name/dissolvableagent`. The IP address or DNS name is the web server where you installed Compliance Dissolvable Agent. For example:

```
http://www.example.com/dissolvableagent  
https://192.0.2.0/dissolvableagent
```

## 5.7 Install SEC: management console, management server, update manager

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

To enable the management console to communicate with managed workstations, open ports 8192 and 8194 on the server. To enable the update manager to download security software from Sophos, open port 80 on the server.

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

If the server is running Windows Server 2008 or later, 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 in a *domain*, log on as a domain administrator.

If the server is in a *workgroup*, log on as a local administrator.

1. Locate the Enterprise Console installer that you downloaded earlier and double-click it.
2. Extract the installation files to the suggested destination folder or another one of your choice. The folder must be on this server.

An installation wizard starts.

3. In the **Sophos Enterprise Console** dialog box, click **Next**.

A wizard guides you through installation of Enterprise Console. Accept the default options, except as shown below.

On the **Setup Type** page, click **Custom**.

On the **Custom Setup** page, make sure that **Management console** and **Management server** are selected and **Database** is not selected.

On the **Database Details** page, enter the location and name of the Enterprise Console database that you created on the other server.

On the **Database Connection User Account Details** page, enter the details of an account that can log onto both this server and the server on which you installed the Enterprise Console database. If the servers are in a *domain*, you can use a domain account. If the servers are in a *workgroup*, use a local account that exists on both servers.

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

## 5.8 Install an additional SEC management console

You might want to install another instance of the SEC management console on another server, so that you can manage networked computers conveniently. If you do not want to, skip this section.

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

If the server is in a *domain*, log on as a domain administrator.

If the server is in a *workgroup*, log on as a local administrator.

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

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

An installation wizard starts.

3. In the **Sophos Enterprise Console** dialog box, click **Next**.

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

On the **Setup Type** page, click **Custom**.

On the **Custom Setup** page, make sure that **Management console** is selected and **Management server** and **Database** are not selected.

On the **Management Server** page, enter the name of the server on which you have installed the SEC management server.

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

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

To enable other users to use the additional management console:

- Add them to the Sophos Console Administrators group and the Distributed COM Users group on the server on which you have installed the management server.
- Assign them to at least one Enterprise Console role and sub-estate.

To enable other users to run reports, add them to the Sophos DB Users group on the server on which you have installed the Enterprise Console database.

## 5.9 Create a directory for Sophos Anti-Virus for NetWare

If you want to protect NetWare servers, you must create a directory into which the update manager can put the latest Sophos Anti-Virus for NetWare software, on each NetWare server that you want to protect.

To create a directory for Sophos Anti-Virus for NetWare:

1. At a Windows computer that is running NetWare administrator software, on one of the NetWare servers that you want to protect, create the directory \\*NetWare server*\SYS\SWEEP\NLMINST where *NetWare server* is the name of the NetWare server.
2. Share the directory so that it can be accessed by the servers on which you have installed an update manager.
3. Repeat this procedure for all the NetWare servers that you want to protect.

Installation of Sophos Anti-Virus on NetWare servers is explained in the *Sophos Endpoint Security and Control 9.5 startup guide for Linux, NetWare, and UNIX*.

## 5.10 Downloading security software

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

*Configure the update manager automatically* (page 22) explains how to run a wizard, which enables you to download:

- Only the latest version.
- Only to subfolders of the share \\server name\SophosUpdate, where *server name* is the name of the server on which the update manager is installed.

*Configure the update manager manually* (page 23) explains how to configure the update manager directly, to enable you to download:

- Earlier versions.
- To other shares, perhaps on other servers.

**Note:** To download Sophos Anti-Virus for NetWare, you must use this method.

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

### 5.10.1 Configure the update manager automatically

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

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

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

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

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

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

Now configure the update manager manually, if necessary. Then go to [Publish security software on a web server](#) (page 42).

## 5.10.2 Configure the update manager manually

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

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

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

**Important:** To subscribe to Sophos Anti-Virus for NetWare, you must add a new subscription exclusively for this. You must not include any other software in this subscription.

- b) In the **Software Subscription** dialog box, if you are adding a new subscription, type a name for it in the **Subscription name** box.
  - c) In the platform list, select the check box next to the software that you want and in the version box select the version that you want.  
Normally, you subscribe to the **Recommended** version to ensure that your software is kept up to date automatically. For information about what other types of version are available, see the Enterprise Console Help, in the section about configuring software subscriptions.
  - d) Click **OK** to close the **Software Subscription** dialog box.
  - e) Repeat these steps for each subscription that you want to change or add.
4. Configure the update manager to use these subscriptions:
- a) In the **Update managers** pane, select the update manager that is installed on this server. Right-click it and click **View/Edit configuration**.
  - b) In the **Configure update manager** dialog box, on the **Subscriptions** tab, make sure that the subscriptions are in the **Subscribed to** list. If not, select the subscriptions in the **Available** list and click the > button to move them to the **Subscribed to** list.
5. If you want to download to shares other than \\server name\SophosUpdate, for example the shares that you created on the NetWare servers:
- a) Click the **Distribution** tab.
  - b) Make sure that the subscription that you want to use is selected in the list at the top of the tab.
  - c) Click **Add**.
  - d) In the **Browse For Folder** dialog box, browse to one of the shares. Click **OK**.
  - e) Select the share in the **Available** list and click the > button to move it to the **Update to** list.
  - f) To enter a description for the share, or credentials to write to it, select the share and click **Configure**. In the **Share Manager** dialog box, enter the description and credentials.
  - g) Repeat these steps for each share.
6. Click **OK** to close the **Configure update manager** dialog box.
- The software that you have selected is downloaded to the shares that you have specified.

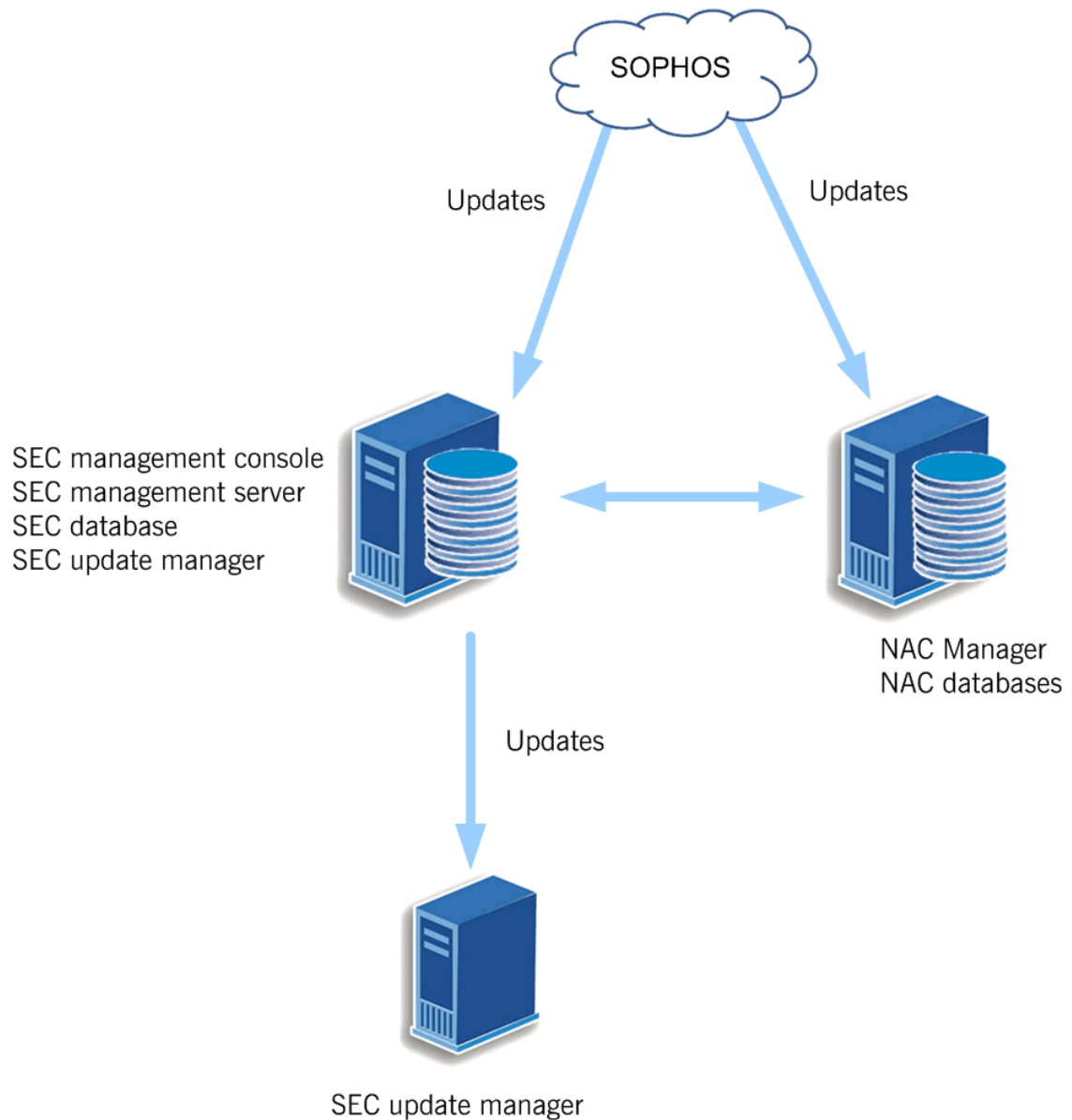
You have finished installing the management tools. Now go to [Publish security software on a web server](#) (page 42).

## **6 Installing the management tools with an additional update manager on a separate server**

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

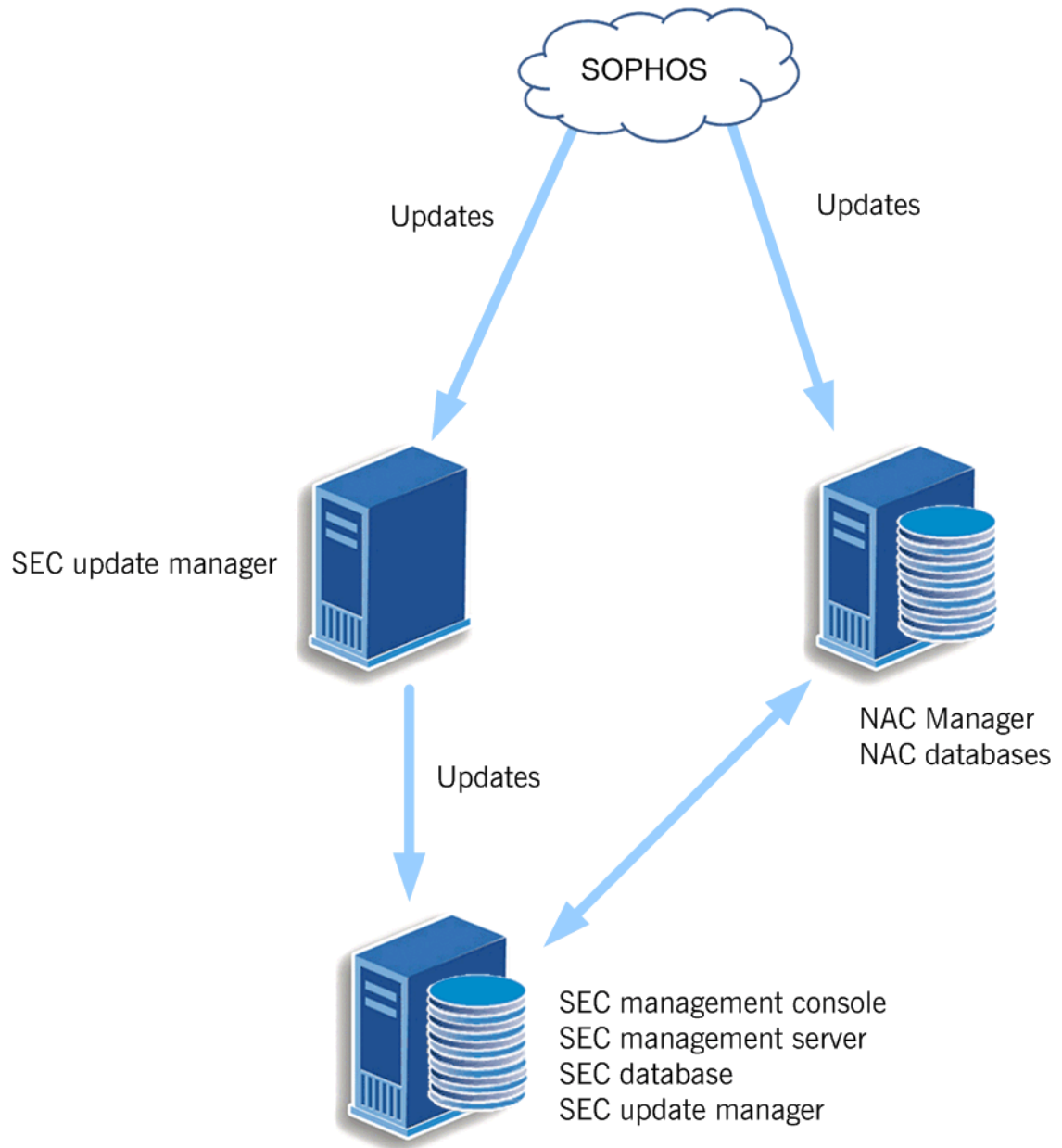
The first method is to:

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



The second method is to:

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



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

The method that you choose affects:

- Which servers need to be connected to the internet. In the following installation sections, you are told when the server that you are installing on needs an internet connection.
- Which method you choose to download security software to a central location, ready for deployment to workstations. Choose the appropriate section when you get to that point.

## 6.1 Download the installers

1. Go to <http://www.sophos.com/support/updates/>.
2. Type your MySophos username and password.
3. On the web page for Endpoint Security and Data Protection downloads, download the Enterprise Console installer.
4. Download the NAC Manager installer.
5. Download the Sophos Compliance Dissolvable Agent installer.
6. Ensure that the installers are in a location that can be accessed from the servers on which you want to install the software.  
Alternatively, copy them to a CD or DVD.

## 6.2 Install NAC Manager and the NAC databases

Go to the server on which you want to install NAC Manager and the NAC databases. Ensure that it is connected to the internet.

The NAC installation requires that you log on as follows:

- If the server is in a domain, log on as a domain administrator.
- If the server is in a workgroup, log on as a local administrator.

The NAC installation wizard guides you through the installation of the NAC system requirements. As part of the NAC installation, you must have the appropriate operating system CD available to install certain system requirements. Other system requirements are installed automatically by the NAC installation wizard.

1. Locate the NAC installer that you downloaded earlier and double-click it.

An installation wizard starts.

2. Click **Install**.
3. On the **Welcome** page, click **Next**.
4. On the **Select Features** page, click **Next**.
5. On the **Sophos Download Account Details** page, type your Sophos download account details in the appropriate fields. Click **Next**.

Sophos download account details are provided to you when you purchase Sophos NAC. The username and password are required to download the latest detection data for security applications. If you mistype the details, you can correct them later using NAC Manager. For more information, see the NAC Manager Help.

- On the **Server Proxy Settings** page, if you need to specify internet proxy settings for this server, click **Use Proxy**. The proxy can be the same as, or different to, the proxy specified in Enterprise Console. Click **Next**.

The username and password fields are required only when NAC Manager is using an authenticated proxy.

- On the **Ready to Install** page, click **Install** to begin the installation.

NAC is configured, and the installation progress is displayed. A portion of the installation takes several minutes, during which time the progress indicator may not move. Do not cancel the installation, and it will progress.

- Click **Finish**.

**Important:** If installation errors occur, use the application event log to view additional information. If the database installation fails, you must delete the following databases if they have been created: AlertStore, AuditStore, GeneralStore, PolicyStore, ReportStore, and SecurityStore. Once you have deleted the databases, you can attempt a re-installation.

## 6.3 Sizing the NAC databases

For installations up to 1500 workstations, the NAC installation process sizes the NAC databases appropriately. You can skip this section.

For larger installations, you must increase the sizes of the NAC databases: the ReportStore database and the ReportStore log, as explained in this section.

### 6.3.1 ReportStore database sizing guidelines

Use this table to determine how to specify the size of the ReportStore database.

| Number of workstations | ReportStore database size guidelines |
|------------------------|--------------------------------------|
| 1500                   | 300 MB                               |
| 3000                   | 379 MB                               |
| 5000                   | 485 MB                               |
| 7500                   | 616 MB                               |
| 10,000                 | 748 MB                               |
| 15,000                 | 1011 MB                              |
| 20,000                 | 1274 MB                              |

| Number of workstations | ReportStore database size guidelines |
|------------------------|--------------------------------------|
| 25,000                 | 1536 MB                              |

### 6.3.2 ReportStore log sizing guidelines

Use this table to determine how to specify the size of the ReportStore log.

| Number of workstations | ReportStore log size guidelines |
|------------------------|---------------------------------|
| 1500                   | 150 MB                          |
| 3000                   | 206 MB                          |
| 5000                   | 281 MB                          |
| 7500                   | 374 MB                          |
| 10,000                 | 467 MB                          |
| 15,000                 | 653 MB                          |
| 20,000                 | 839 MB                          |
| 25,000                 | 1024 MB                         |

### 6.3.3 Change NAC database sizes – SQL Server 2005/2008

1. On the SQL Server **Start** menu, point to **Microsoft SQL Server 2005** or **Microsoft SQL Server 2008** as appropriate, and then click **SQL Server Management Studio**.
2. In SQL Server Management Studio, locate the ReportStore database in the Databases folder, right-click it, and click **Properties**.
3. In the **Properties** dialog box, select **Files**.
4. Locate the ReportStore\_Data file. In the **Initial Size (MB)** field, type an appropriate size for the database.
5. Locate the ReportStore\_Log file. In the **Initial Size (MB)** field, type an appropriate size for the log.
6. Click **OK**.
7. Close SQL Server Management Studio.

## 6.4 Install Compliance Dissolvable Agent on a web server

Sophos Compliance Dissolvable Agent is a client component of NAC that assesses a workstation for compliance. It is designed for users who do not, or cannot, have Sophos Compliance Agent installed on their workstation, such as contractors or guests. To use it, you must first install Compliance Dissolvable Agent on a Windows web server that is accessible to users. Once installed, users download Compliance Dissolvable Agent using a browser.

**Note:** It does not matter if you install it on the same server as the one on which you installed NAC Manager or the NAC databases.

1. Locate the Compliance Dissolvable Agent installer that you downloaded earlier and double-click it.

An installation wizard starts.

2. On the **Welcome** page, click **Next**.
3. On the **Destination Folder** page, keep the default folder or click **Change** to select a different installation folder, as required. Click **Next**.
4. On the **Sophos Server** page, type the IP address or DNS name of the server on which you installed NAC Manager.

**Note:** If you change the NAC Manager server address later, you must re-install Compliance Dissolvable Agent on the web server and specify the new address during the installation.

5. If you are using HTTPS with NAC, select the **Secure Sophos Server (use HTTPS)** check box. The web certificate IP address or DNS name must be the same as the NAC Manager server.
6. Click **Next**.
7. On the **Ready to Install the Program** page, click **Install** to begin the installation.
8. Click **Finish**.

**Note:** If installation errors occur, use the application event log to view additional information.

If you install Compliance Dissolvable Agent in the default folder, workstations can access it using the following address: `http(s)://IP address or DNS name/dissolvableagent`. The IP address or DNS name is the web server where you installed Compliance Dissolvable Agent. For example:

```
http://www.example.com/dissolvableagent  
https://192.0.2.0/dissolvableagent
```

## 6.5 Install SEC: all components

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

To enable the management console to communicate with managed workstations, open ports 8192 and 8194 on the server. To enable the update manager to download security software from Sophos or another update manager via HTTP, open port 80 on the server. To enable the update manager to download security software from another update manager via a UNC path, open ports 137, 138, 139, and 445 on the server.

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

If the server is running Windows Server 2008 or later, 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 in a *domain*, log on as a domain administrator.

If the server is in a *workgroup*, log on as a local administrator.

1. Locate the Enterprise Console installer that you downloaded earlier and double-click it.
2. Extract the installation files to the suggested destination folder or another one of your choice. The folder must be on this server.

An installation wizard starts.

3. In the **Sophos Enterprise Console** dialog box, click **Next**.

A wizard guides you through installation. Accept the default options, and make sure that you select a **Complete** setup.

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

## 6.6 Install an additional SEC management console

You might want to install another instance of the SEC management console on another server, so that you can manage networked computers conveniently. If you do not want to, skip this section.

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

If the server is in a *domain*, log on as a domain administrator.

If the server is in a *workgroup*, log on as a local administrator.

1. Locate the Enterprise Console installer that you downloaded earlier and double-click it.
2. Extract the installation files to the suggested destination folder or another one of your choice. The folder must be on this server.

An installation wizard starts.

3. In the **Sophos Enterprise Console** dialog box, click **Next**.

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

On the **Setup Type** page, click **Custom**.

On the **Custom Setup** page, make sure that **Management console** is selected and **Management server** and **Database** are not selected.

On the **Management Server** page, enter the name of the server on which you have installed the SEC management server.

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

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

To enable other users to use the additional management console:

- Add them to the Sophos Console Administrators group and the Distributed COM Users group on the server on which you have installed the management server.
- Assign them to at least one Enterprise Console role and sub-estate.

To enable other users to run reports, add them to the Sophos DB Users group on the server on which you have installed the Enterprise Console database.

## 6.7 Install an additional update manager

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

To enable the update manager to download security software from Sophos or another update manager via HTTP, open port 80 on the server. To enable the update manager to download security software from another update manager via a UNC path, open ports 137, 138, 139, and 445 on the server.

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

If the server is running a version of Windows that includes the Network Discovery feature, and the feature is turned off, turn it on and restart the server.

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

If the server is in a *domain*, log on as a domain administrator.

If the server is in a *workgroup*, log on as a local administrator.

1. Find the SUMInstallSet shared folder on the server on which you installed Enterprise Console.
2. Double-click Setup.exe to run the installer.
3. In the **Sophos Update Manager** dialog box, click **Next**.

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

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

## 6.8 Create a directory for Sophos Anti-Virus for NetWare

If you want to protect NetWare servers, you must create a directory into which the update manager can put the latest Sophos Anti-Virus for NetWare software, on each NetWare server that you want to protect.

To create a directory for Sophos Anti-Virus for NetWare:

1. At a Windows computer that is running NetWare administrator software, on one of the NetWare servers that you want to protect, create the directory `\\NetWare server\SYS\SWEEP\NLMINST` where *NetWare server* is the name of the NetWare server.
2. Share the directory so that it can be accessed by the servers on which you have installed an update manager.
3. Repeat this procedure for all the NetWare servers that you want to protect.

Installation of Sophos Anti-Virus on NetWare servers is explained in the *Sophos Endpoint Security and Control 9.5 startup guide for Linux, NetWare, and UNIX*.

## 6.9 Downloading security software

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

- [Main update manager updating from Sophos](#) (page 34)
- [Additional update manager updating from Sophos](#) (page 38)

### 6.9.1 Main update manager updating from Sophos

#### Configuring the main update manager to update from Sophos

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

[Configure the main update manager automatically](#) (page 35) explains how to run a wizard, which enables you to download:

- Only the latest version.
- Only to subfolders of the share \\server name\SophosUpdate, where *server name* is the name of the server on which the main update manager is installed.

[Configure the main update manager manually](#) (page 36) explains how to configure the main update manager directly, to enable you to download:

- Earlier versions.
- To other shares, perhaps on other servers.

**Note:** To download Sophos Anti-Virus for NetWare, you must use this method.

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

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

[Configure the additional update manager](#) (page 37) explains how to configure the additional update manager to update from the main update manager.

#### **6.9.1.1 Configure the main update manager automatically**

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

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

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

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

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

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

Now configure the update manager manually, if necessary. Then go to [Configure the additional update manager](#) (page 37).

### 6.9.1.2 Configure the main update manager manually

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

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

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

**Important:** To subscribe to Sophos Anti-Virus for NetWare, you must add a new subscription exclusively for this. You must not include any other software in this subscription.
  - b) In the **Software Subscription** dialog box, if you are adding a new subscription, type a name for it in the **Subscription name** box.
  - c) In the platform list, select the check box next to the software that you want and in the version box select the version that you want.

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

- d) Click **OK** to close the **Software Subscription** dialog box.
  - e) Repeat these steps for each subscription that you want to change or add.
4. Configure the update manager to use these subscriptions:
    - a) In the **Update managers** pane, select the update manager that is installed on this server. Right-click it and click **View/Edit configuration**.
    - b) In the **Configure update manager** dialog box, on the **Subscriptions** tab, make sure that the subscriptions are in the **Subscribed to** list. If not, select the subscriptions in the **Available** list and click the > button to move them to the **Subscribed to** list.
  5. Click **OK** to close the **Configure update manager** dialog box.

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

### **6.9.1.3 Configure the additional update manager**

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

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

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

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

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

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

You have finished installing the management tools. Now go to [Publish security software on a web server](#) (page 42).

## 6.9.2 Additional update manager updating from Sophos

[Configure the additional update manager](#) (page 38) explains how to configure the additional update manager to update from Sophos directly.

[Configure the main update manager](#) (page 40) explains how to configure the main update manager that you installed alongside the SEC management console to update from the additional update manager.

### 6.9.2.1 Configure the additional update manager

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

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

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

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

**Important:** To subscribe to Sophos Anti-Virus for NetWare, you must add a new subscription exclusively for this. You must not include any other software in this subscription.
  - b) In the **Software Subscription** dialog box, if you are adding a new subscription, type a name for it in the **Subscription name** box.
  - c) In the platform list, select the check box next to the software that you want and in the version box select the version that you want.

Normally, you subscribe to the **Recommended** version to ensure that your software is kept up to date automatically. For information about what other types of version are available, see the Enterprise Console Help, in the section about configuring software subscriptions.
  - d) Click **OK** to close the **Software Subscription** dialog box.
  - e) Repeat these steps for each subscription that you want to change or add.

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

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

### 6.9.2.2 Configure the main update manager

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

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

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

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

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

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

You have finished installing the management tools. Now go to [Publish security software on a web server](#) (page 42).

## 7 Publish security software on a web server

You might want to publish Sophos security software on a web server for computers to access via HTTP.

To publish security software on a web server:

1. To find out the path of the shared folder to which the security software has been downloaded, known as the bootstrap location:
  - a) In Enterprise Console, on the **View** menu, click **Bootstrap Locations**.  
In the **Bootstrap Locations** dialog box, the **Location** column displays the bootstrap location for each platform.
  - b) Make a note of the path up to but not including the CIDs folder. For example:  
`\\server name\SophosUpdate`
2. Make the bootstrap location, including subfolders, available on the web server.
3. Specify usernames and passwords to prevent unauthorized access to this folder on the web server.

**Note:** The documentation for your web server should describe how to share a folder over the web and how to set up usernames and passwords for it. For more information about how to do this, contact your web server vendor.

## 8 Create computer groups

If you used the Download Security Software Wizard to set up your computer groups (based on your Active Directory groups), skip this section. Go to [Setting up security policies](#) (page 44).

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

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

A **New Group** is added in the left-hand pane, with its name highlighted.

4. Enter the name that you want to use for the group.
5. To create another top-level group, select the server shown at the top of the **Groups** pane, and repeat steps 3 and 4.

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

## 9 Setting up security policies

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

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

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

### 9.1 Default policies

This section tells you about the default policies and any changes that you should make. For recommended policy settings, see the *Sophos Endpoint Security and Control 9.5 policy setup guide*.

#### 9.1.1 Updating policy

By default, workstations update from the default share that was created on the server on which the relevant update manager is installed.

You might want to:

- Specify an alternative update source for computers that are not always connected to the company network, for example laptops.
- Specify the address of software that you have published on a web server.

You must edit the updating policy if you want to change how the workstation software updates. You can do this any time.

#### 9.1.2 Anti-virus and HIPS policy

By default, Sophos Endpoint Security and Control:

- Denies access to any file that contains viruses/spyware.
- Detects suspicious behavior that is exhibited by programs that are running.
- Blocks access to malicious websites.
- Uses Sophos Live Protection to improve detection of new threats.
- Sends an alert to Enterprise Console when it detects a threat.

You might want to:

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

- Block suspicious behavior.
- Detect suspicious files.
- Detect adware and potentially unwanted applications.
- Detect threats in downloaded web pages.
- Turn on sending of file samples to Sophos to take full advantage of Live Protection.

You must edit the anti-virus and HIPS policy if you want to change how the endpoint software behaves. You can do this any time.

### **9.1.3 Application control policy**

By default, application control is disabled. You must edit the application control policy if you want to use this feature. You can do this any time.

### **9.1.4 Firewall policy**

By default, Sophos Client Firewall blocks all non-essential connections. Therefore, you must edit the firewall policy before you protect your computers, so that their network connectivity is not adversely affected.

### **9.1.5 NAC policy**

By default, computers are allowed to access the network. You must edit and apply one of the NAC policies if you want to use this feature. You can do this any time.

### **9.1.6 Data control policy**

By default, data control is turned off and no rules are specified to monitor or restrict the transfer of files to the internet or storage devices. You must edit the data control policy if you want to use this feature. You can do this any time.

### **9.1.7 Device control policy**

By default, device control is turned off and all devices are allowed. You must edit the device control policy if you want to use this feature. You can do this any time.

### **9.1.8 Tamper protection policy**

By default, tamper protection is turned off and no password is needed to reconfigure, disable, or uninstall Endpoint Security and Control. You must edit the tamper protection policy if you want to use this feature. You can do this any time.

## 9.2 Create or edit any policy except NAC

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

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

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

## 9.3 Edit a NAC policy

1. If you have not used NAC Manager yet:
  - a) Open your default web browser.

Sophos officially supports only Internet Explorer versions 7 and 8 and Firefox versions 3 and 3.5.
  - b) Add the address of the server on which you installed NAC Manager as a trusted website in your browser.

**Note:** If you are using Internet Explorer 7, you do not need to do this.
  - c) Allow pop-ups from the address of the server on which you installed NAC Manager.
2. In Enterprise Console, if the **Policies** pane (bottom left-hand side of the window) is not displayed, on the **View** menu, click **Endpoints**.
3. In the **Policies** pane, double-click NAC. Then double-click the policy that you want to edit.

NAC Manager is displayed in your default browser.

4. Log in using the default account or another that you have created.

The first time that you use NAC Manager, you must use the following account name and password:

- Account Name = admin
- Password = a password of your choice

**Note:** Keep a record of this password because it is the only access to NAC Manager that you have until you create other user accounts.

5. In the NAC Manager page for the policy that you want to edit, enter the settings that you want.

You need to make sure that your policy is applied to a computer group.

## **9.4 Apply a policy to a group**

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

## 10 Search for computers

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

1. If the **Groups** pane (left-hand side of the window) is not displayed, on the **View** menu, click **Endpoints**.
2. On the **Actions** menu, click **Find New Computers**.
3. Select the method that you want to use to search for computers.
4. Enter account details if necessary and specify where you want to search.

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

## 11 Protecting Windows computers and Macs

To protect Windows computers and Macs, you:

- Prepare to protect computers.
- Protect Windows computers automatically.
- Protect Windows computers or Macs manually.

### 11.1 Preparing to protect computers

#### 11.1.1 Prepare for removal of third-party software

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

1. On computers that are running another vendor's anti-virus software, ensure that the anti-virus software user interface is closed.
2. On computers that are running another vendor's firewall or HIPS product, ensure that the firewall or HIPS product is turned off or configured to allow the Sophos installer to run.

If computers are running another vendor's update tool, you may want to remove it. For more information, see the Enterprise Console Help.

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

You will be prompted to enter details of an account that can be used to install security software. This is typically a domain administrator account.

Check that you have an account that:

- Has local administrator rights on computers that you want to protect.
- Can log on to the computer where you installed Enterprise Console.
- Has read access to the location that computers will update from. To check this location, in the **Policies** pane, double-click **Updating**, and then double-click **Default**.

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

#### 11.1.3 Prepare for installation of anti-virus software

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

To prepare for installation of anti-virus software:

1. On Windows 7/Vista computers:

- a) On Windows 7, in Control Panel, open Network and Sharing Center. For the **Work network** location, ensure that the options are configured as below:

Network discovery: On

File and printer sharing: On

File sharing connections: Enable file sharing for devices that use 40- or 56-bit encryption

Password protected sharing: Off

- b) On Windows Vista, in Control Panel, open Network and Sharing Center. Ensure that the options are configured as below:

Network discovery: On

File sharing: On

Printer sharing: On

Password protected sharing: Off

- c) 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 7/Vista.

- d) On Windows 7, set User Account Control to **Never notify**. When installation is complete, you should reset this to **Default**.

- e) On Windows Vista, turn off User Account Control. When installation is complete, you should turn this back on.

- f) Turn off Sharing Wizard.

- g) Open Windows Firewall with Advanced Security, using the **Administrative Tools** item in Control Panel. Ensure that **Inbound connections** are allowed.

- h) 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

2. On Windows 2003/XP Pro/2000 computers:
  - a) Ensure that the Remote Registry, Server, Computer Browser, and Task Scheduler services are started.
  - b) Ensure that the C\$ admin share is enabled.
  - c) Ensure that Simple File Sharing is turned off (XP only).
3. On Windows XP SP2 or later computers:
  - a) Ensure that the Remote Registry, Server, Computer Browser, and Task Scheduler services are started.
  - b) Ensure that the C\$ admin share is enabled.
  - c) Ensure that Simple File Sharing is turned off.
  - d) Enable File and Printer Sharing for Microsoft Networks.
  - e) Ensure that TCP ports 8192, 8193, and 8194 are open.
  - f) Restart the computer to make the changes effective.

#### **11.1.4 Prepare for installation of Compliance Agent**

Sophos Compliance Agent is a client component of NAC that assesses a workstation for compliance. It is installed when you protect your Windows computers.

To prepare for installation of Compliance Agent:

- Specify the URL of the computer on which you installed NAC Manager. In Enterprise Console, on the **Tools** menu, click **Configure NAC URL**.

### **11.2 Protect Windows computers automatically**

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

1. In Enterprise Console, select the computers that you want to protect.

2. Right-click the selection and click **Protect computers**.

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

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

On the **Select features** page, select the **Compliance Control** check box if you want to install NAC.

On the **Protection summary** page, check the details of any installation problems. For help, see [Troubleshooting](#) (page 52).

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

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

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

### 11.2.1 Troubleshooting

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

- Automatic installation is not possible on that operating system. Perform a manual installation. See [Protect Windows computers or Macs manually](#) (page 52). For other operating systems, see the later sections of this guide.
- The operating system could not be determined. This may be because you did not enter your username in the format domain\username when finding computers.
- The computers are running a firewall.
- On Windows XP computers, Simple File Sharing has not been turned off.
- On Windows Vista computers, Sharing Wizard has not been turned off.
- You selected to install a feature that is not supported on that operating system.

If installation of Compliance Agent fails or there is an error during installation, you can view the Compliance Agent installation log. The log is in the %tmp% folder.

## 11.3 Protect Windows computers or Macs manually

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

To perform this procedure, you must use an administrator account on the computers that you want to protect.

To protect Windows computers or Macs manually:

1. To find out the bootstrap location:

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

In the **Bootstrap Locations** dialog box, the **Location** column displays the bootstrap location for each platform.

b) Make a note of the relevant paths.

2. At the computer that hosts the bootstrap location, create a read-only user account.

3. At each computer that you want to protect, locate the installer in the bootstrap location and double-click it.

■ For Windows computers, the installer is called setup.exe.

■ For Macs, the installer is called Sophos Anti-Virus.mpkg.

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

On the **User account details** page, enter the details of the account that you created in step 2.

4. When installation has finished, run an update:

■ For Windows computers, right-click the Sophos system tray icon and click **Update now**.

■ For Macs, click the Sophos Anti-Virus icon on the right-hand side of the menu bar, and then choose **Update Now** from the shortcut menu.

## 12 Check the health of your network

To check the health of your network from Enterprise Console:

1. View the Enterprise Console Dashboard.

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

The Dashboard shows you how many computers:

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

2. If you are using NAC, you can also check whether computers comply with NAC policy:

- a) On the **Tools** menu, click **Manage NAC**.

- b) In NAC Manager, on the **Report** menu, click **Compliance**.

## 13 Protecting standalone computers

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

- The user can download the software from Sophos. Thereafter it is updated automatically from the same location. See Sophos support knowledgebase article 41141 (<http://www.sophos.com/support/knowledgebase/article/41141.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 Sophos 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 that you prefer. See Sophos support knowledgebase article 13093 (<http://www.sophos.com/support/knowledgebase/article/13093.html>).

### 13.1 Send standalone users the information they need

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

- The location from which they can download the security software (unless you are providing it on CD).
- The *Sophos Endpoint Security and Control 9.5 standalone startup guide*.
- The username and password that they need (whether they are downloading from Sophos directly or from your own website).

When you send the username and password:

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

## 14 Technical support

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

- Visit the SophosTalk forum at <http://community.sophos.com/> and search for other users who are experiencing the same problem.
- Visit the Sophos support knowledgebase at <http://www.sophos.com/support/>
- Download the product documentation at <http://www.sophos.com/support/docs/>
- Send an email to [support@sophos.com](mailto:support@sophos.com), including your Sophos software version number(s), operating system(s) and patch level(s), and the text of any error messages.

## 15 Legal notices

Copyright © 2009–2010 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.

### **ACE™, TAO™, CIAO™, and CoSMIC™**

ACE<sup>1</sup>, TAO<sup>2</sup>, CIAO<sup>3</sup>, and CoSMIC<sup>4</sup> (henceforth referred to as “DOC software”) are copyrighted by Douglas C. Schmidt<sup>5</sup> and his research group<sup>6</sup> at Washington University<sup>7</sup>, University of California<sup>8</sup>, Irvine, and Vanderbilt University<sup>9</sup>, Copyright © 1993–2005, all rights reserved.

Since DOC software is open-source<sup>10</sup>, 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 us<sup>11</sup> know so we can promote your project in the DOC software success stories<sup>12</sup>.

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 companies<sup>13</sup> 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 ACE<sup>14</sup>, TAO<sup>15</sup>, CIAO<sup>16</sup>, and CoSMIC<sup>17</sup> web sites are maintained by the DOC Group<sup>18</sup> at the Institute for Software Integrated Systems (ISIS)<sup>19</sup> and the Center for Distributed Object Computing of Washington University, St. Louis<sup>20</sup> for the development of open-source software as part of the

open-source software community<sup>21</sup>. 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 me<sup>22</sup> know.

Douglas C. Schmidt<sup>23</sup>

## **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](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/>

### **Apache**

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

### **Common Public License**

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

### **ConvertUTF**

Copyright 2001–2004 Unicode, Inc.

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

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

### **iMatix SFL**

This product uses parts of the iMatix SFL, Copyright © 1991-2000 iMatix Corporation  
<http://www.imatix.com>.

### **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](mailto: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](mailto: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](mailto:eay@cryptsoft.com)). This product includes software written by Tim Hudson ([tjh@cryptsoft.com](mailto:tjh@cryptsoft.com)).

#### **Original SSLeay license**

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

This package is an SSL implementation written by Eric Young ([eay@cryptsoft.com](mailto: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](mailto: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.]