

SOPHOS

Sophos Endpoint Security and Control quick startup guide

Document date: January 2009



Contents

1 About this guide.....	3
2 What do I install?.....	3
3 What are the key steps?.....	3
4 Check the system requirements.....	4
5 Install Sophos Enterprise Console.....	5
6 Subscribe to Sophos updates.....	5
7 Install Sophos NAC Manager.....	6
8 Create computer groups.....	6
9 Search for computers.....	6
10 Protect computers.....	7
11 Set up a firewall policy.....	8
12 Set up a NAC policy.....	9
13 Check the health of your network.....	9
14 Troubleshooting.....	10
15 Get help with common tasks.....	10
16 Technical support.....	11
17 Copyright.....	11

1 About this guide

This guide tells you how to protect your network with Sophos security software.

If you are installing Sophos software for the first time, read this guide.

If you are upgrading, see the *Sophos Endpoint Security and Control network upgrade guide* for your version of the software.

2 What do I install?

You install two management tools:

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

Installation of Sophos NAC Manager is optional.

Note: You install the tools separately, using two different setup programs.

Note: You can install both tools on the same server, as long as it meets the system requirements for both. However, if you have more than 1,000 computers, you should install the tools on different servers.

3 What are the key steps?

You carry out these key steps:

- Check the system requirements.
- Install Sophos Enterprise Console.
- Subscribe to Sophos updates.
- Install Sophos NAC Manager.
- Create groups for computers.
- Search for computers.
- Protect computers.
- Set up a firewall policy.
- Set up a NAC policy.

- Check the health of your network.

4 Check the system requirements

The system requirements depend on which management tools you install. Internet access is required in all cases.

Sophos Enterprise Console and Sophos NAC Manager on a single server

Processor	Disk space	Memory	Operating systems	Database
Minimum 2.0 GHz Pentium or equivalent	3 GB on the C: drive	Minimum 1 GB	Windows 2003 Server SP0+	MSDE SQL Server 2000 SQL Server 2005 SQL Server 2005 Express

Sophos Enterprise Console only

Processor	Disk space	Memory	Operating systems	Database
Minimum 2.0 GHz Pentium or equivalent	Minimum 150 MB Plus up to 2 GB database space (MSDE)	Minimum 512 MB	Windows Server 2008 Windows 2003 Server SP0+ Windows 2003 Server 64-bit Windows 2000 SP3+ VMWare ESX 3.0 VMWare Workstation 5.0 VMWare Server 1.0	MSDE SQL Server 2000 SQL Server 2005 SQL Server 2005 Express

5 Install Sophos Enterprise Console

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

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

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

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

1. Log on as an administrator.
 - *If the computer is in a domain*, log on as a domain administrator.
 - *If the computer is in a workgroup*, log on as a local administrator.
2. Go to the Sophos website. On the web page for Endpoint Security and Control downloads, download the **Enterprise Console** installer.
3. Double-click the downloaded installer.
4. In the **Sophos Network Installer** dialog box, click **Install**.
5. A wizard guides you through installation. You should do as follows:
 - a) Accept the defaults on each dialog box.
 - b) Select a **Complete** setup.

When installation is complete, log off or restart the server (the final dialog in the wizard shows which).

6 Subscribe to Sophos updates

Note: If you installed Enterprise Console with Remote Desktop, this section doesn't apply. Select Start|Programs|Sophos|EM Library and follow the instructions on screen.

1. When you log back on (or restart), the **Welcome to Sophos Endpoint Security and Control** dialog box is displayed. Select **Quick setup**.
2. The **Subscribe to Sophos Updates** wizard guides you through selecting and downloading software. You should do as follows:
 - a) In the **Enter Sophos Download Account Details** dialog box, enter the username and password printed on your license schedule. If you access the internet via a proxy server, select the **Enter proxy information** checkbox.
 - b) In the **Download Software** dialog box, if you use Active Directory and want Enterprise Console to use your existing computer groups, select **Set up groups for your computers**.

Your chosen software is downloaded. This can take several minutes.

When downloading is complete, Sophos Enterprise Console is launched automatically. You will use it after you install Sophos NAC Manager.

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

7 Install Sophos NAC Manager

Ensure that you have the Windows 2003 Server operating system CD and Service Pack CDs. You may be prompted for them during installation.

1. Log on as an administrator.
 - *If the computer is in a domain*, log on as a domain administrator.
 - *If the computer is in a workgroup*, log on as a local administrator.
2. Go to the Sophos website. On the web page for Endpoint Security and Control downloads, download the **NAC Manager** installer.
3. Double-click the downloaded installer.
4. In the **Sophos NAC Manager** dialog box, click **Install**.
5. A wizard guides you through installation.

8 Create computer groups

If you used the **Subscribe to Sophos Updates** wizard to set up your computer groups (based on your Active Directory groups), skip this section and the next. Go to [Protect computers](#) on page 7.

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

1. If Enterprise Console is not already open, open it.
2. Click the **Create group** icon.
 - A **New Group** is added in the left-hand pane, with its name highlighted.
3. Enter the name you want to use for the group.

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

9 Search for computers

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

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

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

10 Protect computers

To protect computers you:

- Prepare computers.
- Run the **Protect computers** wizard.

10.1 Prepare computers

Before you protect computers, do as follows.

Prepare for removal of third-party software

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

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

If computers are running another vendor's update tool, you may want to remove it. See *Sophos Endpoint Security and Control network startup guide*, section 10.1.

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. It must:

- Have local administrator rights on computers you want to protect.
- Be able to log on to the computer where you installed Enterprise Console.
- Have read 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**.

Prepare for firewall or NAC installation

If you want to use Sophos Client Firewall, install it on only a few sample computers first. The firewall initially prevents network access and must be configured before you install it on all computers. See [Set up a firewall policy](#) on page 8.

If you want to use Sophos NAC, install it on sample computers first and decide on policy settings before you install in on all computers. See [Set up a NAC policy](#) on page 9.

Otherwise, you do not have to edit any security policies before you protect your network, as safe default policies are used.

10.2 Run the Protect computers wizard

To protect computers, do as follows.

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

Note: If computers are in the **Unassigned** folder, simply drag and drop them into your chosen groups.

3. A wizard guides you through the installation of Sophos security software. You should do as follows:
 - a) In the **Select security software** dialog box, if you want to select **Install Sophos NAC**, you must click the link to set up the NAC server URL. Enter or confirm the URL.
 - b) In the **Protection summary** dialog box, any problems with installation are shown. See [Troubleshooting](#) on page 10.
 - c) In the **Protect computers credentials** dialog box, enter details of an account that can be used to install software on computers.

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

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

11 Set up a firewall policy

By default, the firewall blocks all non-essential connections. Therefore, you must create your own firewall policy.

You should install the firewall on sample computers, customize it and use these settings as your policy.

1. Go to each computer and restart it to activate the firewall.
2. Right-click the firewall icon (brick wall) in the system tray and select **Configure**.
3. In the **SCF Configuration Editor** dialog box, click the **General** tabbed page.
4. Select **Interactive**. The firewall prompts you to allow or block each application as it is used. **Alternatively**, click the **Applications** tab. Click **Add** and browse to each application you want. The application is then "trusted".
5. After the firewall is configured, on the **General** tabbed page, click **Export** to export the configuration.

6. Go to Enterprise Console. In the **Policies** pane, double-click **Firewall** and then double-click the policy you want to edit.
7. In the **Firewall policy** dialog box, on the **General** tabbed page, click **Import** and import the firewall configuration.

12 Set up a NAC policy

When you first install NAC, the "Default" NAC policy is applied to all computers. NAC runs in report-only mode and does not block network access.

If you want to use a different policy, you need to use Sophos NAC Manager to edit a policy and Enterprise Console to apply that policy to computers.

Sophos NAC Manager is browser-based, so you should take these steps before you start:

- If you use Internet Explorer 6.x, add Sophos NAC Manager as a trusted website.
- Turn off pop-up blocking.

Then do as follows:

1. In Enterprise Console, in the **Policies** pane, double-click **NAC**.

You see three policies:

- **Default:** Used if no other policy has been assigned.
- **Managed:** Can be used for computers managed with Sophos Enterprise Console.
- **Unmanaged:** Can be used for computers from outside the company. This policy can't be edited.

See "Using predefined policies" in the Sophos NAC Manager help files or guide.

2. Double-click a policy. This launches Sophos NAC Manager.
3. When you use NAC Manager for the first time, use "Admin" as the account name and a password of your choice.
4. Edit the policy settings. See the Sophos NAC Manager help files or guide.
5. In Enterprise Console, drag and drop the policy onto the appropriate computer group(s).

13 Check the health of your network

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

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

The Dashboard shows you how many computers:

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

2. If you are using NAC, you can also:

- a) Click the **NAC** icon on the menu bar.
- b) In NAC Manager, select **Report** and then **Compliance**.

This shows you whether computers comply with NAC policy.

14 Troubleshooting

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

- Automatic installation is not possible on that operating system. Perform a manual installation. See *Sophos Endpoint Security and Control network startup guide*, sections 21-25.
- Operating system could not be determined. This may be because you did not enter your username in the format domain\username when finding computers.
- The computers are running a firewall (usually this is the case on Windows XP SP2 computers).

15 Get help with common tasks

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

SESC = Sophos Endpoint Security and Control

SEC = Sophos Enterprise Console

SCF = Sophos Client Firewall

Task	Document
Protect Windows computers manually	SESC network startup guide, section 20
Protect Mac OS X computers	SESC network startup guide, section 22
Protect Linux computers	SESC network startup guide, section 23
Protect standalone computers	SESC network startup guide, section 26

Task	Document
Set anti-virus and HIPS policy	SEC help files, "How do I change anti-virus and HIPS settings?"
Set application control policy	SEC help files, "How do I control applications on the network?"
Set firewall policy	SCF help files, "How do I configure the firewall?"
Set NAC policy	Sophos NAC Manager guide, "Manage overview" section
Manage alerts	SEC help files, "How do I deal with alerts?"
Clean up threats	SEC help files, "How do I clean up computers?"
Generate reports	SEC help files, "How do I generate reports?"
Generate NAC reports	Sophos NAC Manager, "Report overview" section

16 Technical support

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

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

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

17 Copyright

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

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