

SOPHOS

Sophos Endpoint Security and Control 9 quick startup guide

Document date: September 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.....	4
6 Download security software.....	5
7 Install Sophos NAC Manager.....	6
8 Create computer groups.....	6
9 Set up security policies.....	7
10 Search for computers.....	7
11 Protect computers.....	7
12 Check the health of your network.....	9
13 Troubleshooting.....	10
14 Get help with common tasks.....	10
15 Technical support.....	11
16 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 quick upgrade guide*.

Note: If you have a very large network, you may want to consider the installation options in the *Sophos Endpoint Security and Control advanced startup guide*.

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 unauthorized computers or computers that do not comply with your security standards.

Installation of 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. However, if you have more than 1,000 computers, you should install the tools on different servers. The procedure is the same.

3 What are the key steps?

You carry out these key steps:

- Check the system requirements.
- Install Sophos Enterprise Console.
- Download security software.
- Install Sophos Network Access Control.
- Create computer groups.
- Set up security policies.
- Search for computers.
- Protect computers.
- Check the health of your network.

4 Check the system requirements

The system requirements depend on which tool(s) you install.

Requirements shown are the minimum except where stated. Database requirements assume up to 1,000 computers.

Internet access is required in all cases.

The requirements here list server operating systems only. If you need more detailed requirements, visit <http://www.sophos.com/products/all-sysreqs.html>

Enterprise Console only

Processor	Disk space	Memory	Operating system
2 GHz Pentium or equivalent	150 MB for installation Up to 2GB for database	512 MB	Windows Server 2008 (32 or 64 bit) Windows Server 2003 SP1+ (32 or 64 bit) Windows 2000 SP4 VMWAre ESX 3.0 VMWare Workstation 5.0

Enterprise Console and NAC Manager on the same server

Processor	Disk space	Memory	Operating system
2 GHz Pentium or equivalent	Up to 3 GB for database	1 GB	Windows Server 2008 (32 bit) Windows Server 2003 SP1+ (32 bit)

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:

- If you want to use SQL Server 2008 (rather than SQL Server 2005 Express, which comes with Enterprise Console), ensure it is 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 page.
 - b) Select a **Complete** setup.

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

6 Download security software

When you log back on (or restart) for the first time after installation, Enterprise Console opens automatically and a wizard runs.

Note: If you used Remote Desktop to install Enterprise Console, the console does not open automatically. Open it from the Start menu.

The wizard guides you through selecting and downloading security software. You should do as follows:

1. On the **Sophos Download Account Details** page, enter the username and password printed on your license schedule. If you access the internet via a proxy server, select the **Access Sophos via a proxy server** checkbox.
2. On the **Platform selection** page, select only the platforms you need to protect now.
When you click **Next**, Enterprise Console begins downloading your software.
3. On the **Downloading Software** page, downloading progress is displayed. Click **Next** at any time.
4. On the **Import computers from Active Directory** page, select **Set up groups for your computers** if you want Enterprise Console to use your existing Active Directory computer groups.

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 operating system CD and Service Pack CDs. You may be prompted for them during installation.

Note: If you install NAC Manager on a different server from Enterprise Console, you must install an SQL Server 2005 or later database manually first.

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 **Download Security Software Wizard** to set up your computer groups (based on your Active Directory groups), skip this section. Go to [Set up security policies](#) (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. In the **Groups** pane (on the left-hand side of the console), ensure that the server name shown at the top is selected.
3. On the toolbar, click the **Create group** icon.

A "New Group" is added to the list, with its name highlighted.

4. Type a name for the group.

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

9 Set up security policies

Enterprise Console applies “default” security policies to your computer groups. You do not have to change these policies unless you want to, with these exceptions:

- You must set up a firewall policy now.
- You must edit the network access control, application control, data control or device control policies if you want to use these features. You can do this any time.

9.1 Set up a firewall policy

By default, the firewall blocks all non-essential connections. Therefore you must configure the firewall before you protect your computers.

1. In the **Policy** pane, double-click **Firewall**.
2. Double-click the **Default** policy to edit it. A wizard is launched.
3. In the **Firewall Policy Wizard** we recommend that you make the following selections.
 - a) On the **Configure firewall** page, select **Single location** unless you want the firewall to use different settings according to the location where you use it.
 - b) On the **Operational Mode** page, select **Block inbound and allow outbound traffic**.
 - c) On the **File and print sharing** page, select **Allow file and print sharing**.

10 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 if necessary and specify where you want to search.

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

11 Protect computers

To protect computers you:

- Prepare computers.
- Protect Windows computers automatically.

- Protect Windows or Mac OS X computers manually.

11.1 Prepare to protect computers

Before you protect computers, do as follows:

Prepare for removal of third-party security 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 "Remove third-party security software" in the "Protecting computers" section of the Enterprise Console Help.

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 installation of network access control

Before you can install network access control on computers, you must:

- Specify the URL of the computer where you installed NAC Manager. In Enterprise Console, select **Tools > Configure NAC URL**.

11.2 Protect Windows computers automatically

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** group, simply drag them to your chosen groups.

3. A wizard guides you through the installation of Sophos security software. You should do as follows:
 - a) On the **Select features** page, select **Sophos Compliance Agent** if you want network access control.
 - b) On the **Protection summary** page, any problems with installation are shown. See [Troubleshooting](#) (page 10).
 - c) On the **Protect computer credentials** page, 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.

11.3 Protect Windows or Mac OS X computers manually

If you have computers that you cannot protect automatically, you protect them by running a setup program from a central directory.

To find out which directory the setup program is in, open Enterprise Console and select **View > Bootstrap locations**.

1. Go to each computer and log on with local administrator rights.
2. Locate the setup program in the central directory and double-click it.
 - For Windows, the program is called setup.exe.
 - For Mac OS X, the program is called Sophos Anti-Virus.mpkg
3. A wizard guides you through installation.

12 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.

13 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 [Protect Windows or Mac OS X computers manually](#) (page 9) . For other operating systems, see the *Sophos Endpoint Security and Control advanced startup guide*.
- 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.

14 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

Task	Document
Protect Linux computers	SESC advanced startup guide: "Protecting Linux computers"
Protect standalone computers	SESC advanced startup guide: "Protecting standalone computers"
Configure anti-virus and HIPS	Enterprise Console Help: "Configuring the anti-virus and HIPS policy"
Configure application control	Enterprise Console Help: "Configuring the application control policy"
Configure data control	Enterprise Console Help: "Configuring the data control policy"
Configure device control	Enterprise Console Help: "Configuring the device control policy"

Task	Document
Configure NAC	NAC Manager Help: "Manage overview"
Give network access to guest users	Sophos Compliance Agent configuration guide: "Dissolvable agent"
Deal with alerts	Enterprise Console Help: "Dealing with alerts and errors"
Clean up computers	Enterprise Console Help: "Cleaning up computers"
Generate SEC reports	Enterprise Console Help: "Generating reports"
Generate NAC reports	NAC Manager Help: "Report overview"

15 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

16 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.

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 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>