

**SOPHOS**

simple + secure

# Sophos Endpoint Security and Control 9.7 quick startup guide

Document date: August 2011



# 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 Prepare for installation.....	5
6 Download the installers.....	5
7 Install Enterprise Console .....	5
8 Download security software.....	6
9 Install NAC Manager .....	6
10 Create computer groups.....	7
11 Set up security policies.....	7
12 Search for computers.....	8
13 Prepare to protect computers.....	8
14 Protect computers.....	11
15 Check the health of your network.....	13
16 Troubleshooting.....	13
17 Get help with common tasks.....	13
18 Technical support.....	14
19 Legal notices.....	15

## 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, go to the **Endpoint Security and Control Upgrade Center** at <http://www.sophos.com/support/upgrades/>

**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.
- Prepare for installation.
- Download the installers.
- Install Enterprise Console.
- Download security software.
- Install NAC Manager.
- Create computer groups.
- Set up security policies.

- Search for computers.
- Prepare to protect computers.
- Protect computers.
- Check the health of your network.

## 4 Check the system requirements

Check the hardware, operating system and system software requirements before you begin installation.

### 4.1 Hardware and operating system

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

### 4.2 Microsoft system software

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

The Enterprise Console installer attempts to install this system software if it is not already available on your server. However, in some cases, software is incompatible with your server or needs to be installed manually.

#### SQL Server installation

The installer attempts to install SQL Server 2008 Express, unless you already have SQL Server 2005 Express or later. Note that:

- We recommend that you do not install SQL Server on a domain controller.
- SQL Server 2008 Express is not compatible with Windows Server 2003 SP1 or Windows XP 64-bit 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>

#### .NET Framework installation

The installer attempts to install .NET Framework 3.5, unless it is already installed. Note that:

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

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

## 5 Prepare for installation

Select a server that meets the system requirements and prepare as follows:

- Ensure that you are connected to the internet.
- Ensure that you have the Windows operating system CD and Service Pack CDs. You may be prompted for them during installation.
- If the server is running Windows Server 2008 or later, turn off User Account Control (UAC) and restart the server.

**Note:** You can turn UAC on again after you have completed the installation and downloaded your security software.

## 6 Download the installers

Download the Sophos installers and put them on the server where you want to install the management tools:

1. Go to <http://www.sophos.com/support/updates/>.
2. Type your MySophos username and password.
3. On the web page for **Enterprise** downloads, you should:
  - Download the Enterprise Console installer.
  - If you want to use NAC Manager, download the Sophos NAC installer.
4. If necessary, copy the downloaded installers to the server where you want to make the installation.

If you intend to install NAC Manager on a different server from Enterprise Console, you should copy the installer to that server.

## 7 Install Enterprise Console

To install Enterprise Console:

1. At the computer where you want to install Enterprise Console, 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. Find the Enterprise Console installer that you downloaded earlier.

**Tip:** The installer file name includes "sec".

3. Double-click the installer.
4. In the **Sophos Endpoint Security and Control network installer** dialog box, click **Install**.

The installation files are copied to the computer and an installation wizard starts.

5. In the **Sophos Enterprise Console** dialog box, click **Next**.
6. A wizard guides you through installation. You should do as follows:
  - a) Accept the defaults wherever possible.
  - b) Select a **Complete** setup.
7. When installation is complete, you may be prompted to restart. Click **Yes** or **Finish**.

## 8 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 for installation, 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.

## 9 Install 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 a SQL Server 2005 or later database manually first.

1. At the computer where you want to install NAC Manager, 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. Find the Sophos NAC installer that you downloaded earlier.

**Tip:** The installer file name includes "nac".
3. Double-click the installer.
4. In the **Sophos NAC Manager** dialog box, click **Install**.
5. A wizard guides you through installation.

## 10 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.

## 11 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.

## 11.1 Set up a firewall policy

**Note:** During the installation of firewall, there will be a temporary disconnection of network adapters. The interruption may cause the disconnection of networked applications, such as Remote Desktop.

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

1. In the **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**.

## 12 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.

## 13 Prepare to protect computers

Before you protect computers, you must prepare them as follows:

- Prepare for removal of third-party security software.
- Check that you have an account that can be used to install software.
- Prepare for installation of anti-virus software.
- Prepare for installation of network access control.

## 13.1 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.

## 13.2 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. 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**.

## 13.3 Prepare for installation of anti-virus software

You must prepare computers for installation of anti-virus software. The steps depend on the operating system.

**Note:** If an operating system is not shown here, you do not have to prepare computers running that system.

### 13.3.1 Prepare Windows 7 computers

1. 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

2. Ensure that the Remote Registry service is started and that its startup type is set to Automatic.

3. Set User Account Control to **Never notify**. When installation is complete, you should reset this to **Default**.
4. Turn off Sharing Wizard.
5. Open Windows Firewall with Advanced Security, using the **Administrative Tools** item in Control Panel.
  - a) Ensure that **Inbound connections** are allowed.
  - b) 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

### 13.3.2 Prepare Windows Vista computers

1. 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
2. Ensure that the Remote Registry service is started and that its startup type is set to Automatic.
3. Turn off User Account Control. When installation is complete, you should turn this back on.
4. Turn off Sharing Wizard.
5. Open Windows Firewall with Advanced Security, using the **Administrative Tools** item in Control Panel.
  - a) Ensure that **Inbound connections** are allowed.
  - b) 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

### 13.3.3 Prepare Windows 2003/XP Pro/2000 computers

1. Ensure that the Remote Registry, Server, Computer Browser, and Task Scheduler services are started.
2. Ensure that the C\$ admin share is enabled.
3. Ensure that Simple File Sharing is turned off (XP Pro only).

### 13.3.4 Prepare Windows XP (SP2 or later) computers

**Note:** For Windows XP Pro computers, see [Prepare Windows 2003/XP Pro/2000 computers](#) (page 11).

1. Ensure that the Remote Registry, Server, Computer Browser, and Task Scheduler services are started.
2. Ensure that the C\$ admin share is enabled.
3. Ensure that Simple File Sharing is turned off.
4. Enable File and Printer Sharing for Microsoft Networks.
5. Ensure that TCP ports 8192, 8193, and 8194 are open.
6. Restart the computer to make the changes effective.

## 13.4 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**.

## 14 Protect computers

This section tells you how to:

- Protect Windows computers automatically.
- Protect Windows or Mac OS X computers manually.

## 14.1 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, you can install optional features. Select **Compliance Control** if you want network access control.
  - b) On the **Protection summary** page, check for any installation problems. For help, see [Troubleshooting](#) (page 13).
  - c) On the **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.

## 14.2 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.

## 15 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) Select **File > Open > NAC**.
- b) In NAC Manager, select **Report > Compliance**.

This shows you whether computers comply with NAC policy.

## 16 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 12). 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.

## 17 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 9.7 startup guide for Linux, NetWare and UNIX: "Protecting Linux computers"

Task	Document
Protect standalone computers	SESC 9.7 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"
Configure tamper protection	Enterprise Console Help: "Configuring the tamper protection policy"
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"

## 18 Technical support

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

- Visit the SophosTalk community 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.

## 19 Legal notices

Copyright © 2011 Sophos Limited. 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 license terms or you otherwise have the prior permission in writing of the copyright owner.

Sophos and Sophos Anti-Virus are registered trademarks of Sophos Limited. 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](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.