

SOPHOS

simple + secure

Sophos Enterprise Manager startup guide

Product version: 4.7

Document date: August 2011



Contents

1 About this guide.....	3
2 What are the key steps?.....	3
3 Check the system requirements.....	4
4 Prepare for installation.....	5
5 Download the installer.....	5
6 Install Enterprise Manager	5
7 Download security software.....	6
8 Create computer groups.....	6
9 Set up security policies.....	7
10 Search for computers.....	8
11 Protect Windows computers.....	9
12 Protect Mac OS X computers.....	13
13 Protect Linux computers.....	13
14 Check the health of your network.....	16
15 Troubleshooting.....	16
16 Get help with common tasks.....	16
17 Appendix: Changing to Enterprise Manager from Enterprise Console.....	17
18 Technical support.....	20
19 Legal notices.....	20

1 About this guide

This guide tells you how to install Sophos Enterprise Manager, version 4.7, and protect your network with Sophos security software.

Sophos Enterprise Manager is a single, automated console that manages and updates Sophos security software on Windows, Mac and Linux computers. Enterprise Manager enables you to:

- Protect your network against viruses, Trojans, worms, spyware, malicious websites, and unknown threats, as well as adware and other potentially unwanted applications.
- Manage client firewall protection on endpoint computers.
- Prevent users from using unauthorized external storage devices and wireless connection technologies on endpoint computers.
- Prevent users from re-configuring, disabling, or uninstalling Sophos security software.

For the list of Enterprise Manager's features and information about how Enterprise Manager and associated licenses differ from other Sophos's products and licenses, see Sophos support knowledgebase article 113711 (<http://www.sophos.com/support/knowledgebase/article/113711.html>).

Changing from Enterprise Console

The guide also tells you about the additional steps you need to perform if you want to uninstall Enterprise Console and install Enterprise Manager.

Important: Downgrading from Enterprise Console to Enterprise Manager is not supported. You will need to uninstall Enterprise Console and then install Enterprise Manager as described in this guide and set it up.

You will lose all your Enterprise Console settings.

Before you uninstall Enterprise Console, make a note of your existing settings and back up the Enterprise Console database as described in [Appendix: Changing to Enterprise Manager from Enterprise Console](#) (page 17).

2 What are the key steps?

You carry out these key steps:

- Check the system requirements.
- Prepare for installation.
- Download the installer.
- Install Enterprise Manager.
- Download security software.

- Create computer groups.
- Set up security policies.
- Search for computers.
- Protect computers.
- Check the health of your network.

3 Check the system requirements

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

3.1 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>).

3.2 Microsoft system software

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

The Enterprise Manager 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 articles 65190 and 111220

(<http://www.sophos.com/support/knowledgebase/article/65190.html> and <http://www.sophos.com/support/knowledgebase/article/111220.html>).

4 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.

5 Download the installer

Download the Sophos installer and put it on the server where you want to install the management console:

1. Go to <http://www.sophos.com/support/updates/>.
2. Type your MySophos username and password.
3. On the **Downloads and updates** web page, download the Enterprise Manager installer.
4. If necessary, copy the downloaded installer to the server where you want to make the installation.

6 Install Enterprise Manager

To install Enterprise Manager:

1. At the computer where you want to install Enterprise 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 Enterprise Manager installer that you downloaded earlier.
3. Double-click the installer.
4. In the network installer dialog box, click **Install**.

The installation files are copied to the computer and an installation wizard starts.
5. On the Welcome page of the Sophos Enterprise Manager installation wizard, click **Next**.

6. A wizard guides you through installation. You should accept the defaults wherever possible.
7. When installation is complete, you may be prompted to restart. Click **Yes** or **Finish**.

7 Download security software

When you log back on (or restart) for the first time after installation, Enterprise Manager 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** check box.

2. On the **Platform selection** page, select the platforms that you want to protect.

When you click **Next**, Enterprise Manager 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 Manager 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 Manager.

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 Enterprise Manager is installed.

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

8 Create computer groups

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

Groups are useful because you can:

- Have computers in different groups updated from different sources or on different schedules.
- Use different anti-virus and HIPS, firewall, and other policies for different groups.
- Manage computers more easily.

If you have already set up your computer groups based on your Active Directory groups, using the **Download Security Software Wizard**, skip this section. Go to [Set up security policies](#) (page 7).

1. If Enterprise Manager 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

Default policies

Enterprise Manager 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. See [Set up a firewall policy](#) (page 8).
- You must edit the device control and tamper protection policies if you want to use these features. You can do this any time.

For information about enabling and configuring the device control and tamper protection policies, see *Configuring the device control policy* and *Configuring the tamper protection policy* in the *Enterprise Manager Help*.

Creating new policies

In Enterprise Manager, you can create up to four new policies of each type. Once you have reached this limit, the **Create Policy** and **Duplicate Policy** options will be disabled.

To create a new policy:

1. In the **Endpoints** view, in the **Policies** pane, right-click the type of policy you want to create, for example, “Updating,” and select **Create policy**.

A “New Policy” is added to the list, with its name highlighted.

2. Type a new name for the policy.
3. Double-click the new policy. Enter the settings you want.

For the instructions on how to choose the settings, see the section on configuring the relevant policy.

You have created a policy that can now be assigned to groups.

Assigning policies to groups

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

9.1 Set up a firewall policy

By default, the firewall is enabled and blocks all non-essential traffic. Therefore, you should configure it to allow the applications you want to use, and test it before installing it on all computers. See the *Sophos Enterprise Manager policy setup guide* for detailed advice.

You can set up the main configuration options for the firewall in the **Firewall Policy Wizard**.

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 printer sharing** page, select **Allow file and printer sharing**.

10 Search for computers

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

If you have already set up your computer groups based on your Active Directory groups, using the **Download Security Software Wizard**, skip this section. Go to [Protect Windows computers](#) (page 9).

1. Click the **Find new computers** icon in the toolbar.
2. Select the method you want to use to search for computers.
 - If you use the **Import from Active Directory** option, and then choose to import computers and containers, the computers are placed in their respective groups.
 - If you use one of the **Find** options, the computers are placed in the **Unassigned** group.
3. Enter account details if necessary and specify where you want to search.
4. If you used one of the **Find** options, click the **Unassigned** group to see the computers that have been found. To begin managing computers, select them and drag them to a group.

11 Protect Windows computers

This section tells you how to protect Windows computers automatically or manually, if computers cannot be protected automatically.

11.1 Prepare to protect Windows computers automatically

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.

11.1.1 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 Manager Help*.

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

When protecting computers automatically, in the **Protect computers wizard**, 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 Manager.
- Have read access to the location that computers will update from.

By default, computers update from a single primary source UNC share, \\<ComputerName>\SophosUpdate, where <ComputerName> is the name of the computer where Enterprise Manager is installed. To check this location, in the **Policies** pane, double-click **Updating**, and then double-click the policy you want to check.

11.1.3 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.

11.1.3.1 Prepare Windows 7 computers

To prepare Windows 7 computers for installation of anti-virus software, follow the steps below.

Alternatively, if you use Active Directory, you can prepare your Windows 7 computers using a Group Policy Object (GPO) in Windows 2008 and Windows 2008 R2. See Sophos support knowledgebase article 111180 (<http://www.sophos.com/support/knowledgebase/article/111180.html>).

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

11.1.3.2 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

11.1.3.3 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).

11.1.3.4 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.

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 any optional features you want.

The anti-virus feature is always installed.

Sophos Client Firewall is not supported on server operating systems.

Important: Make sure you have configured the firewall to allow the traffic, applications, and processes you want to use prior to installing and running it on computers. See [Set up a firewall policy](#) (page 8).

- b) On the **Protection summary** page, check for any installation problems. For help, see [Troubleshooting](#) (page 16).
- 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.

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.

To check the protection status of computers, select the group where you placed the computers, or select the server shown at the top to see all computers. When installation is complete, in the computer list, in the **On-access** column, the word **Active** indicates that the computer is running on-access virus scanning.

11.3 Protect Windows computers manually

If you have computers that you cannot protect automatically, protect them by running a setup program from a shared folder to which the endpoint security software has been downloaded. This folder is known as the bootstrap location.

1. To find out which directory the setup program is in, open Enterprise Manager. On the **View** menu, click **Bootstrap locations**.

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

2. Go to each computer and log on with local administrator rights.
3. Locate the setup program in the bootstrap location and double-click it.
For Windows, the program is called setup.exe.
4. A wizard guides you through installation.

12 Protect Mac OS X computers

Automatic installation is not possible on Mac computers. Protect them by running a setup program from a shared folder to which the endpoint security software has been downloaded. This folder is known as the bootstrap location.

1. To find out which directory the setup program is in, open Enterprise Manager. On the **View** menu, click **Bootstrap locations**.

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

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

13 Protect Linux computers

To protect Linux computers, you must:

- Create a deployment package.
- Install Sophos Anti-Virus on the Linux computers.

13.1 Create a deployment package

This section assumes that you have downloaded Sophos Anti-Virus for Linux, as explained in [Download security software](#) (page 6).

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

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

To create a deployment package:

1. To find out the path of the shared folder to which Sophos Anti-Virus has been downloaded, known as the bootstrap location:

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

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

- b) Make a note of the relevant path.

2. Log on to your Linux server as root.
3. Mount the bootstrap location.

To enable this folder to be mounted automatically on system boot, use distribution-specific tools for doing so, or edit `fstab`.

4. Change to the bootstrap location.
5. To create a deployment package in tar format, called `savinstpkg.tgz`, type:

```
./mkinstpkg.sh
```

To create a deployment package in RPM format, called `savinstpkg-0.0-1.i586.rpm`, type:

```
./mkinstpkg.sh -r
```

Note: The filename might differ depending on the RPM setup.

6. When prompted, choose to enable remote management.
7. When prompted for the location, enter the bootstrap location (as seen from the Linux computers).

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

13.2 Install Sophos Anti-Virus for Linux using the deployment package

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

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

Note: On Red Hat Enterprise Linux version 6 64 bit, the following packages must be installed so that the installation of Sophos Anti-Virus succeeds:

- `glibc-2.11.1-1.i686`
- `nss-softokn-freebl i686 3.12.4-10.fc12`

13.2.1 Install Sophos Anti-Virus for Linux manually

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

```
tar -zxvf savinstpkg.tgz  
./sophos-av/install.sh
```

To install from the RPM package, type:

```
rpm -i RPM package
```

The necessary files are copied from the server and Sophos Anti-Virus is installed. From now on, Sophos Anti-Virus will be updated automatically whenever the bootstrap location is updated.

13.2.2 Install Sophos Anti-Virus for Linux automatically

- To install Sophos Anti-Virus automatically from the deployment package, use one of the operating system administration tools that support remote deployment.

For more information, see the documentation for that tool.

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

14 Check the health of your network

To check the health of your network from Enterprise Manager, 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.

15 Troubleshooting

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

- Automatic installation using Enterprise Manager is not possible on Mac and Linux computers. For information about how to protect these operating systems, see [Protect Mac OS X computers](#) (page 13) and [Protect Linux computers](#) (page 13).
- 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.

16 Get help with common tasks

For information on how to carry out common tasks, see the following sections in the *Enterprise Manager Help*:

- *Configuring policies*
 - *Configuring the anti-virus and HIPS policy*
 - *Configuring the firewall policy*
 - *Configuring the device control policy*
 - *Configuring the tamper protection policy*
- *Protecting computers*
 - *Dealing with alerts and errors*
 - *Cleaning up computers*

■ *Generating reports*

For policy setup guidelines and best practice, see also the *Sophos Enterprise Manager policy setup guide*.

17 Appendix: Changing to Enterprise Manager from Enterprise Console

When you uninstall Enterprise Console and then install Enterprise Manager, all your Enterprise Console settings will be lost. Computers will be moved into the **Unassigned** group and the policies reset to default.

Make a note of your existing configuration. It will make it easier to re-create computer groups and configure policies in Enterprise Manager.

You can export firewall policy configuration settings from Enterprise Console version 4.5 or 4.7 and import them to Enterprise Manager. For instructions on how to do this, see the next section.

If you are currently using Sophos NAC (Network Access Control), you must remove it from your network. It is also recommended that if you are using the data control and application control features, you disable them before uninstalling Enterprise Console.

Important: Before you uninstall Enterprise Console, back up the Enterprise Console database as described in [Back up the Enterprise Console database](#) (page 19).

17.1 Export and import firewall configuration settings

To export firewall policy configuration settings from Enterprise Console and then import them to Enterprise Manager:

1. In Enterprise Console, in the **Policies** pane, double-click **Firewall**, and then double-click the policy you want to export.
2. On the **Welcome** page of the **Firewall Policy** wizard, click **Advanced firewall policy**.
3. In the **Firewall Policy** dialog box, on the **General** tab, under **Managing configuration**, click **Export** to export the firewall settings as a configuration file (*.conf).
4. Repeat steps 1-3 for every Enterprise Console firewall policy up to a maximum of 5 (Enterprise Manager supports a maximum of 5 policies).
5. To import the settings to Enterprise Manager, in Enterprise Manager, in the **Policies** pane, double-click **Firewall**, and then double-click the policy where you want to import the settings.
6. On the **Welcome** page of the **Firewall Policy** wizard, click **Advanced firewall policy**.
7. In the **Firewall Policy** dialog box, on the **General** tab, under **Managing configuration**, click **Import** to import the firewall configuration settings.
8. Repeat steps 5-7 for other Enterprise Manager firewall policies as required.

17.2 Remove Sophos NAC

If you are currently using Sophos NAC (Network Access Control), you must remove it from your network.

You must remove the Sophos NAC components as follows:

- Remove Sophos Compliance Agent from endpoint computers.
- Remove NAC Manager from the server.
- Remove the NAC databases from the server.

Note: If you do not remove the components in this order, errors may be displayed for users.

17.2.1 Remove Sophos Compliance Agent

To remove Sophos Compliance Agent, you must go to each endpoint computer and remove the agent manually.

Note: You may be prompted to close certain applications before removing the agent.

Note: You are required to restart the computer after removing the agent.

1. Go to the endpoint computer.
2. From the **Start** menu, select **Control Panel > Add or Remove Programs**.
3. Select **Sophos Network Access Control**, and click **Remove**.
4. Click **Yes** to confirm removal.

17.2.2 Remove NAC Manager

To remove NAC Manager:

1. Go to the server where NAC Manager is installed. This is usually the same server where Enterprise Console is installed.
2. On the **Start** menu, click **Control Panel > Add or Remove Programs**.
3. Select **Sophos NAC Application Server** and click **Remove**.
4. Click **Yes** to confirm removal.

NAC Manager is removed.

17.2.3 Remove NAC databases

Note: This procedure removes only the server files that were used to create the databases and not the databases themselves.

At the server where the NAC database is installed:

1. On the **Start** menu, click **Control Panel > Add or Remove Programs** .
2. Select **Sophos NAC databases** and click **Remove**.
3. Click **Yes** to confirm removal.

17.3 Back up the Enterprise Console database

Before you uninstall Enterprise Console, make sure you have a valid, complete backup of your Enterprise Console installation. Make sure you can recover the system from the backup. If you later decide to reinstall Enterprise Console, this will enable you to restore its settings.

Note: The default installation folder for the database is C:\Program files\Microsoft SQL Server\MSSQL\$SOPHOS.

To back up the Enterprise Console database:

1. Go to the computer where the Enterprise Console management server is installed.
2. Stop the Sophos Message Router and Sophos Management Service services. To do this:
 - a) Click **Start, Run**, type **services.msc** and click **OK**.
 - b) In the **Services** window, right-click the service name and click **Stop**.
 - c) Close the **Services** window.

This ensures that no new information is written to the database while it is being backed up.

3. Create a folder for the database backup, for example, C:\SophosBackups.
4. Open a command window at the Enterprise Console installation database directory.

The default directory is C:\Program Files\Sophos\Enterprise Console\DB.

5. Backup the database by entering a command in this format:

BackupDB C:\SophosBackups\SOPHOS.bak

If the SQL Server instance is anything other than SOPHOS, add the name of the SQL Server instance, for example:

BackupDB C:\SophosBackups\SOPHOS.bak MySQLServerInstance

6. Export the following registry key:
 - For a 32-bit operating system: HKLM\SOFTWARE\Sophos\Certification Manager
 - For a 64-bit operating system:
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Sophos\Certification Manager

You are now ready to uninstall Enterprise Console.

For information about restoring Enterprise Console database, see *Troubleshooting* below.

17.4 Troubleshooting

Restoring Enterprise Console data

If you want to restore the Enterprise Console installation to its previous state, do the following:

1. Restore the database to the instance you use. The default SQL Server instance is SOPHOS.
2. Restore the following registry key:
 - For a 32-bit operating system: HKLM\SOFTWARE\Sophos\Certification Manager
 - For a 64-bit operating system:
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Sophos\Certification Manager

If you need more information or guidance, then please contact technical support.

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, 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.

ACE™, TAO™, CIAO™, and CoSMIC™

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

Since DOC software is open-source, 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 us¹⁰ know so we can promote your project in the DOC software success stories¹¹.

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 companies¹² 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 ACE¹³, TAO¹⁴, CIAO¹⁵, and CoSMIC¹⁶ web sites are maintained by the DOC Group¹⁷ at the Institute for Software Integrated Systems (ISIS)¹⁸ and the Center for Distributed Object Computing of Washington University, St. Louis¹⁹ for the development of open-source software as part of the open-source software community²⁰. 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 me²¹ know.

Douglas C. Schmidt²²

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. mailto:doc_group@cs.wustl.edu
11. <http://www.cs.wustl.edu/~schmidt/ACE-users.html>
12. <http://www.cs.wustl.edu/~schmidt/commercial-support.html>
13. <http://www.cs.wustl.edu/~schmidt/ACE.html>
14. <http://www.cs.wustl.edu/~schmidt/TAO.html>
15. <http://www.dre.vanderbilt.edu/CIAO/>
16. <http://www.dre.vanderbilt.edu/cosmic/>
17. <http://www.dre.vanderbilt.edu/>
18. <http://www.isis.vanderbilt.edu/>
19. <http://www.cs.wustl.edu/~schmidt/doc-center.html>
20. <http://www.opensource.org/>
21. <mailto:d.schmidt@vanderbilt.edu>
22. <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 referenced 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>

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.

OpenSSL license

Copyright © 1998–2011 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

“This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)”
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

“This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)”

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (ey@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay license

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

This package is an SSL implementation written by Eric Young (ey@cryptsoft.com). The implementation was written so as to conform with Netscape’s SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young’s, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

“This product includes cryptographic software written by Eric Young (ey@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 license 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 license [including the GNU Public License.]