

Sophos Enterprise Console upgrade guide

Product version: 5.0

Document date: December 2011



Contents

1 About this guide.....	3
2 What are the steps in upgrading?.....	3
3 System requirements.....	3
4 The accounts you need.....	3
5 Download the installers.....	4
6 Upgrade Enterprise Console	4
7 Check existing policies.....	5
8 Upgrade endpoint computers.....	6
9 Upgrade the Compliance Dissolvable Agent.....	15
10 Technical support.....	15
11 Legal notices.....	16

1 About this guide

This guide tells you how to upgrade to:

- Enterprise Console 5.0
- Endpoint Security and Control 10.0 for Windows
- NAC Manager 3.9 (Optional)
- Compliance Dissolvable Agent 3.9 (Optional)

You only need to upgrade NAC Manager and Compliance Dissolvable Agent if you use Sophos NAC.

Tip: The Enterprise Console installer has a built-in advisor. You can use it to check system requirements and get advice before you upgrade.

2 What are the steps in upgrading?

Upgrading involves the following steps.

- Check the system requirements.
- Check the accounts you need.
- Download the installers.
- Upgrade Enterprise Console (and optionally NAC Manager).
- Check your existing policies.
- Upgrade endpoint computers.
- Upgrade the Compliance Dissolvable Agent (optional).

3 System requirements

See the system requirements page of the Sophos website
<http://www.sophos.com/products/all-sysreqs.html>

4 The accounts you need

When you upgrade Enterprise Console, you might be asked for details of a database account. This happens if your existing account no longer meets the requirements.

Ensure you have an account that:

- Can log onto the computer where the Sophos Management Server is installed.
- Can read and write to the system temporary directory e.g. "\\windows\temp\". By default members of "Users" have this right.
- Has a UPN (User Principal Name) associated with the account if it is a domain account.

All other rights and group memberships that the account needs are granted automatically during the upgrade.

Sophos recommends that the account:

- Is not set to expire and does not have any other logon restriction.
- Is not an administrative account.
- Is not changed after the upgrade.

For more information, see Sophos support knowledgebase article 113954 (<http://www.sophos.com/support/knowledgebase/article/113954.html>)

5 Download the installers

Note: You can download the installers at any computer and then copy them to the computer where you will use them.

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 you are not at the computer where you want to install the software, copy the installers to that computer.
Alternatively, copy the installers to a CD or DVD and take them to the computer.

6 Upgrade Enterprise Console

Tip: The Enterprise Console installer has a built-in advisor. You can use it to check system requirements and get advice before you upgrade.

Note: If you have NAC Manager, the Enterprise Console installer will detect it and will advise you to upgrade NAC Manager first. It will also give you full instructions.

To upgrade Enterprise Console:

1. At the computer where you want to upgrade Enterprise Console, log on as an administrator:
 - If the server is in a domain, use a domain account that has local administrator rights.
 - If the server is in a workgroup, use a local account that has local administrator rights.
2. Find the Enterprise Console installer that you downloaded earlier.

Tip: The installer file name includes "sec".
3. Double-click the installer.
4. A wizard guides you through the upgrade.

If the wizard cannot handle all aspects of your upgrade, it will automatically run an advisor tool and display further instructions.

7 Check existing policies

7.1 Check policy settings

Note: If you use role-based administration, you must have the **Computer search, protection and groups** right to perform these tasks. For more information, see "About roles and sub-estates" in the section "Managing roles and sub-estates" in the *Sophos Enterprise Console Help*.

To check that your policy settings have been preserved after upgrading Enterprise Console:

1. Start Enterprise Console.
2. In the **Policies** pane, double-click a policy type (for example, **Anti-virus and HIPS**).
3. Double-click the policy you want to check.
4. In the dialog box that is displayed, review the policy settings.

7.2 Check policies applied to computer groups

Note: If you use role-based administration, you must have the **Computer search, protection and groups** right to perform these tasks. For more information, see "About roles and sub-estates" in the section "Managing roles and sub-estates" in the *Sophos Enterprise Console Help*.

To check that your groups have the correct policies applied to them after upgrading Enterprise Console:

1. Start Enterprise Console.
2. In the **Groups** pane, right-click a group, and then click **View/Edit Group Policy Details**.
3. In the **Group Details** dialog box, verify that the group is assigned the right policies. If not, for a policy type, select a different policy from the drop-down list.

8 Upgrade endpoint computers

8.1 About upgrading endpoint computers

To upgrade your Windows endpoint computers and use the new features, you must change the version of the software that the computers are kept up to date with to Sophos Endpoint Security and Control 10.0.

The procedures described here upgrade all the security software components, including the Compliance Agent for NAC (if you use NAC Manager).

8.2 Can I upgrade computers gradually?

There are two ways that you can approach the upgrade of endpoint computers.

- If you want to begin using the latest versions of the security software **immediately**, you can upgrade your endpoint computers in one step.

See [Upgrade endpoint computers immediately](#) (page 6).

- If you want to try out the latest versions of the security software before upgrading all computers, you can upgrade your endpoint computers **gradually**.

See [Upgrade endpoint computers gradually](#) (page 7).

8.3 Which versions can I upgrade from?

The information in this section covers the following upgrade scenarios:

- Upgrade Sophos Endpoint Security and Control 9.0, 9.5 or 9.7 to version 10.0
- Upgrade Sophos Anti-Virus 7 and Sophos Client Firewall 1.5 to Sophos Endpoint Security and Control 10.0

8.4 Upgrade endpoint computers immediately

To upgrade your Windows computers immediately, you change your existing software subscriptions to download the new version of the endpoint security software.

To change your existing software subscriptions:

1. In Enterprise Console, on the **View** menu, click **Update Managers**.
2. In the **Software Subscriptions** pane, double-click the subscription you want to change.

The **Software Subscription** dialog box appears.

3. Next to **Windows 2000 and later**, click in the **Version** field, and then click again.
4. In the list of available versions, select **10.0 Recommended**.

The next time Enterprise Console downloads updates, it will download the new version of the endpoint software. Your Windows computers will then upgrade themselves to version 10.0 automatically.

You do not need to perform any other configuration steps:

- The update manager is already configured to maintain the subscription and distribute the software into update shares on the network.
- You already have updating policies that refer to that subscription and are applied to your Windows computers.

Notes

- To deploy the patch agent to your Windows computers, you must reprotect them using the **Protect computers** wizard. You must do this even if they have an earlier version of Sophos Endpoint Security and Control installed. For more information, see *Protect computers* in the Sophos Enterprise Console Help.
- During the Sophos Client Firewall installation, there will be a temporary disconnection of network adapters. The interruption may cause the disconnection of networked applications, such as Remote Desktop.
- When computers upgrade to Sophos Endpoint Security and Control 10.0, the computer details in Enterprise Console may show "Differs from policy" in the **Policy Compliance** column. To correct this, right-click the computers, click **Comply with**, and then click the relevant policy or policies.

8.5 Upgrade endpoint computers gradually

8.5.1 Subscribe to the new endpoint software

Creating new software subscriptions

If you want to test the new software on a small group of computers before releasing it to the network, you can create a new subscription.

After you have created a new subscription, you will need to perform the following steps:

- Configure the update manager to maintain the subscription: that is, download the software from Sophos and put it in network shares from which endpoint computers will update.
- Create new updating policies that will refer to the new subscription and point to the update shares set up for it in the update manager.
- Upgrade endpoint computers by applying the new updating policies to them.

Important: Do not upgrade to Sophos Endpoint Security and Control 10.0 on any Windows 2000 computers running SP3 or earlier. The minimum requirement for the software is Windows 2000 with SP4.

Continue using your existing versions

If you are subscribed to a fixed version of Sophos Endpoint Security and Control and Compliance Agent for NAC and want to continue using that version, you can do so. When Sophos stops supporting that version, your computers will be upgraded automatically, provided that you leave selected the check box **Automatically upgrade fixed version software when it is no longer supported by Sophos** in the **Software Subscription** dialog box.

If you want to evaluate new versions of the software before placing them on your main network, you may want to consider using fixed versions of the software on the main network while evaluating the new versions. Fixed versions are updated with new threat detection data, but not with the latest software version each month.

If you want to continue using your existing versions of Sophos endpoint security software you can do so. However, you will eventually be automatically upgraded to version 10.0. You will be warned about this well in advance.

8.5.2 Create a new software subscription

To create a new software subscription:

1. In Enterprise Console, on the **View** menu, click **Update Managers**.
2. In the **Software Subscriptions** pane, click the **Add** button at the top of the pane to create a new subscription.

The **Software Subscription** dialog box appears.

Alternatively, if you want to create a copy of an existing subscription, select the subscription, right-click and click **Duplicate Subscription**. Type a new name for the subscription and then double-click it to open the **Software Subscription** dialog box.

3. In the **Software Subscription** dialog box, edit the name of the subscription, if you wish.
4. Click in the **Version** field next to Windows 2000 and later and then click again.

A drop-down list of available versions appears.

5. Select the type of update you want to download for version 10.0 of Sophos Endpoint Security and Control.

Normally, you subscribe to the “Recommended” versions to ensure that your software is kept up to date automatically. To learn what other types of update are available, see [What types of update are available?](#) (page 9).

Important: If you select a fixed version, for example, 10.0.1, Sophos recommends that you leave the **Automatically upgrade fixed version software when it is no longer supported by Sophos** check box selected. Running unsupported software leaves you unprotected against new security threats.

After you have created a new software subscription, configure the update manager to maintain it as described in [Configure the update manager to maintain a new subscription](#) (page 10).

You can also set up subscription email alerts. For more information about subscription email alerts, see the topic “Set up software subscription alerts” in the “Setting up alerts and messages” section of the Sophos Enterprise Console Help.

8.5.3 What types of update are available?

There are several versions of the software associated with each major version of a solution (for example, Sophos Endpoint Security and Control 9) and platform (for example, Windows 2000 or later). You can choose which software version to download from Sophos for further deployment to endpoint computers by selecting an update type in the subscription. You can select among three labeled versions and three fixed versions of the software.

Labeled versions

There are three labeled versions:

Label	Description
Recommended	The version that we considers to be the most appropriate for those who want the most up-to-date version of the product. We normally recommend that the latest version of the endpoint software is deployed to endpoints as soon as it is released.
Previous	The previously-recommended version.
Oldest	The oldest version that Sophos is still supporting with updates.

Note: We may add new labels over time.

The **Download Security Software Wizard** sets up a subscription that specifies the recommended versions of any selected software.

When subscribed to a labeled version, the actual version(s) downloaded will usually change each month.

Fixed versions

Fixed versions are updated with new threat detection data, but not with the latest software version each month.

If you want to evaluate new versions of the software before placing them on your main network, you may want to consider using fixed versions of the software on the main network while evaluating the new versions.

Usually, there are three fixed versions for each operating system, representing the previous three monthly releases. An example of a fixed version is Sophos Endpoint Security and Control for Windows 2000 and later, version 9.4.3.

Fixed versions are downloaded for as long as they are available from Sophos. If a fixed version is due to retire, you will see an alert in the **Update managers** view next to any update managers that are subscribed to that version. If email alerting is active, the administrator will also receive an email alert.

By default, when a subscribed fixed version is retired, Enterprise Console will redefine the subscription to use the oldest fixed version that is still available.

Note: You can change this behavior in the subscription by clearing the check box **Automatically upgrade fixed version software when it is no longer supported by Sophos**. Be aware, however, that running unsupported software will leave you unprotected against new security threats. Therefore, we recommend that you upgrade any unsupported versions as soon as possible.

8.5.4 Configure the update manager to maintain a new subscription

If you created a new subscription for the new software version, now configure the update manager to maintain this subscription.

To configure the update manager to maintain a new subscription:

1. In the **Update managers** view, select the update manager, right-click and click **View/Edit Configuration**.
2. In the **Configure update manager** dialog box, on the **Subscriptions** tab, select the software subscription in the list of available subscriptions.
To view the details of the subscription, for example, what software is included in the subscription, click **View details**.
3. To move the selected subscription to the “Subscribed to” list, click the > button.

By default, the software is downloaded to the share \\<ComputerName>\SophosUpdate, where ComputerName is the name of the computer where the update manager is installed. You can specify additional shares as described in [Specify where the software is placed](#) (page 10).

If you want to download the new version immediately, select the update manager, right-click and click **Update Now**.

8.5.5 Specify where the software is placed

After you have selected which software to download, you can specify where it should be placed on the network. By default, the software is placed in a UNC share \\<ComputerName>\SophosUpdate, where ComputerName is the name of the computer where the update manager is installed.

You can distribute downloaded software to additional shares on your network. To do this, add an existing network share to the list of available shares and then move it to the list of update shares as described below.

To specify where the software is placed:

1. In the **Configure update manager** dialog box, on the **Distribution** tab, select a software subscription from the list.
2. Select a share from the “Available” shares list and move it to the “Update to” list by clicking the > button.

The default share \\<ComputerName>\SophosUpdate is always present in the “Update to” list. You cannot remove this share from the list.

The “Available” shares list includes all the shares that Enterprise Console knows about and that are not already being used by another update manager.

You can add an existing share to or remove a share from the “Available” shares list, using the **Add** or **Remove** button.

3. If you want to enter a description for a share or credentials needed to write to the share, select the share and click **Configure**.
4. In the **Share manager** dialog box, enter the description and credentials.

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

If you want to edit the default update schedule, see [Edit an update schedule](#) (page 11).

If you want to download the software immediately, select the update manager, right-click and click **Update Now**.

8.5.6 Edit an update schedule

By default, an update manager will check for threat detection data updates every 10 minutes. You can change this update interval. The minimum is 5 minutes. The maximum is 1440 minutes (24 hours). Sophos recommends an update interval of 10 minutes for threat detection data, so that you receive protection from new threats promptly after the detection data is published by Sophos.

By default, an update manager will check for software updates every 60 minutes. You can change this update interval. The minimum is 10 minutes. The maximum is 1440 minutes (24 hours).

For software updates, you can either specify an update interval that is used every hour of every day, or you can create more sophisticated schedules, in which each day can be specified independently and each day can be divided into periods with different update intervals.

Note: You can create a different schedule for each day of the week. Only a single schedule can be associated with a day of the week.

If you want to change the default schedule:

- In the **Configure update manager** dialog box, on the **Schedule** tab, enter new update intervals or create a more sophisticated schedule, or different schedules for different days of the week.

You can also change the default settings for the update manager log and self-updating, if you wish. You do this by editing the settings on the **Logging** and **Advanced** tabs, respectively.

8.5.7 Configure your updating policies

If you created a new software subscription, and then configured the update manager to maintain this subscription, now configure your updating policies to update the computers with the software specified in the subscription.

You can choose either of the following options.

- **Change your existing updating policies to refer to the new subscription**

For information on how to do this, see [Select a subscription](#) (page 12).

If you choose this option, your endpoint computers will be upgraded to the new version next time they check for updates.

- **Create new updating policies**

For information on how to do this, see [Create new updating policies](#) (page 12).

If you choose this option, you will then need to apply the new policies to endpoint computers to upgrade them and keep up to date with the new version.

8.5.8 Select a subscription

If you created a new software subscription, and then configured the update manager to maintain this subscription, now change your existing updating policies to refer to the new subscription.

1. In the **Endpoints** view, **Policies** pane, right-click the policy you want to configure, and then click **View/Edit Policy**.
2. In the **Updating policy** dialog box, click the **Subscription** tab, and then select the subscription for the software you want to keep up to date.

8.5.9 Create new updating policies

1. In the **Endpoints** view, **Policies** pane, right-click **Updating**, and then click **Create policy**.
2. Type the name for the new policy.
3. Right-click the new policy, and then click **View/Edit Policy**.
4. In the **Updating policy** dialog box, click the **Subscription** tab, and then select the subscription for the software you want to keep up to date.

5. On the **Primary server** tab, in the **Address** field, accept the default or specify a different share (UNC path or web address) from which endpoint computers will usually download updates.

By default, computers update from a UNC share \\<ComputerName>\SophosUpdate, where ComputerName is the name of the computer where the update manager is installed.

Important: If you choose to use an HTTP location (for example, a web update share) or a share that is not maintained by a managed update manager, Enterprise Console will not be able to check that the software specified in the subscription policy is available at that address. You must manually ensure that the share contains the software that is specified in the subscription policy. Otherwise, computers will not be updated.

6. If you have Macs that you want to manage from Enterprise Console and you specified a UNC path in the **Address** field, under **Mac OS-specific options**, select a protocol that Macs will use to access the update share.
7. If necessary, in the **Username** field, enter the username for the account that will be used to access the server, and then enter and confirm the password. This account should have read rights to the share you entered in the address field above.

Note: If the username needs to be qualified to indicate the domain, use the form domain\username.

8. If you access the update source via a proxy server, click **Proxy details**. In the **Proxy details** dialog box, select **Access the server via a proxy**. Then enter the proxy server **Address** and **Port** number. Enter a **Username** and **Password** that give access to the proxy server. If the username needs to be qualified to indicate the domain, use the form domain\username.

You can now apply this policy to a group or groups of computers to keep them up to date with your chosen security software.

You can also limit the bandwidth used, set up an alternative source for updates, or change the default schedule, logging, and initial install source details, if you wish. For more information about configuring updating policies, see the section “Configuring the updating policy” in the Sophos Enterprise Console Help.

Continue the migration as described in [Configure the update manager on the Enterprise Console computer](#) (page 13).

8.5.10 Configure the update manager on the Enterprise Console computer

Enterprise Console cannot protect the network fully until the update manager is installed on the same computer as the Enterprise Console management server is configured with an update source. This will enable Enterprise Console to receive necessary updates (for example, information about the versions of security software that endpoint computers should be running, new and updated Content Control Lists for data control, or the list of new controlled devices and applications).

To configure the update manager:

1. In the **Update managers** view, select the computer where Enterprise Console is installed. Right-click and click **View/Edit Configuration**.
2. In the **Configure update manager** dialog box, on the **Sources** tab, click **Add**.
3. In the **Source Details** dialog box, click the drop-down arrow in the **Address** field and select the default update share created by the update manager that updates from Sophos.
Alternatively, type in the address or click **Browse** to browse to the share.
The default update share is a UNC share \\<ComputerName>\SophosUpdate, where ComputerName is the name of the computer where the update manager that updates from Sophos is installed.
4. Enter the username, password, and proxy settings, as appropriate.

This will enable the update manager to download updates for Enterprise Console.

If you want to configure the update manager on the Enterprise Console computer to distribute endpoint software updates across the network, configure the software subscription, distribution, and schedule settings similarly to how you configured such settings for the update manager that updates from Sophos.

If you wish, you can change the default settings for the update manager log and self-updating. You do this on the **Logging** and **Advanced** tabs, respectively.

8.5.11 Apply a new updating policy to a group of Windows computers

Important: Do not upgrade Sophos endpoint security software to Sophos Endpoint Security and Control 10.0 on Windows 2000 computers running SP3 or earlier. The minimum requirement for the software is Windows 2000 with SP4.

To apply a new updating policy to a group of computers:

1. In the **Policies** pane, highlight the updating 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.
Alternatively, you can right-click a group and select **View group policy details**. You can then select policies for that group from drop-down menus.

During the next update, computers will be upgraded to the new version of the security software, Sophos Endpoint Security and Control 10.0.

Notes

- To deploy the patch agent to your Windows computers, you must reprotect them using the **Protect computers** wizard. You must do this even if they have an earlier version of Sophos Endpoint Security and Control installed. For more information, see *Protect computers* in the Sophos Enterprise Console Help.

- During the Sophos Client Firewall installation, there will be a temporary disconnection of network adapters. The interruption may cause the disconnection of networked applications, such as Remote Desktop.
- When computers upgrade to Sophos Endpoint Security and Control 10.0, the computer details in Enterprise Console may show "Differs from policy" in the **Policy Compliance** column. To correct this, right-click the computers, click **Comply with**, and then click the relevant policy or policies.

9 Upgrade the Compliance Dissolvable Agent

If you use NAC Manager, you can upgrade the Sophos Compliance Dissolvable Agent from version 3.7 or 3.5 to version 3.9.

To upgrade the Compliance Dissolvable Agent:

1. Go to <http://www.sophos.com/support/updates/>.
2. Type your MySophos username and password.
3. Download the Sophos NAC Compliance Dissolvable Agent version 3.9 installer.
4. Start the Sophos NAC Compliance Dissolvable Agent version 3.9 installer.
5. A wizard guides you through installation. Accept the default options, except as shown below.
6. On the **Sophos Server** page, type the IP address or DNS name of the server on which you installed NAC Manager.
 - If Sophos NAC was installed on more than one server, the server address is the IP address or DNS name of the NAC Manager Server and not the NAC Database Server.
 - If you change the NAC Manager server address later, you must reinstall Compliance Dissolvable Agent on the web server and specify the new address during the installation.
7. If you are using HTTPS with NAC, select the **Secure Sophos Server (use HTTPS)** check box. The web certificate IP address or DNS name must be the same as the NAC Manager server.

10 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.

11 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, Sophos Anti-Virus and SafeGuard are registered trademarks of Sophos Limited, Sophos Group and Utimaco Safeware AG, as applicable. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

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.