SOPHOS

Security made simple.

Sophos Enterprise Console upgrade guide

Product version: 5.3.0

Document date: April 2015

Contents

1 About this guide

This guide tells you how to upgrade to Sophos Enterprise Console 5.3.0 and how to enable the new Malicious Traffic Detection feature.

2 Which versions can I upgrade from?

You can upgrade to Enterprise Console 5.3.0 directly from:

- Enterprise Console 5.2.2
- Enterprise Console 5.2.1 R2
- Enterprise Console 5.2.1
- Enterprise Console 5.2.0
- Enterprise Console 5.1
- Enterprise Console 5.0

If you are using Enterprise Console 4.x or Enterprise Manager 4.7, you will need to upgrade in two steps: first upgrade to Enterprise Console 5.1 and then upgrade to Enterprise Console 5.3.0.

If you are using Sophos Control Center 4.0.1 or 4.1, you will need to upgrade in two steps by following one of the supported upgrade paths:

- Upgrade to Enterprise Console 5.1 and then upgrade to Enterprise Console 5.3.0.
- Upgrade to Enterprise Console 5.2.2 and then upgrade to Enterprise Console 5.3.0.

Note: Alternatively, you could use Sophos Cloud to manage your computers. To find answers to frequently asked questions about Sophos Cloud, see knowledgebase article 119598.

See also knowledgebase article 119105 for more information about different upgrade paths.

The installers for earlier versions of Enterprise Console are available from the Sophos Enterprise Console Downloads page (http://www.sophos.com/en-us/support/downloads/console/sophos-enterprise-console.aspx).

Note: If you are upgrading from Enterprise Console 5.2.1, 5.2.1 R2, or 5.2.2, no changes to the database component are required. For more information, go to knowledgebase article 121956. If you are upgrading from an earlier version and want to upgrade the Sophos databases manually by running the database install scripts, see knowledgebase article 116768.

3 Sophos Disk Encryption

There is no upgrade for Sophos Disk Encryption 5.61—it will retire at the end of March 2016. If you use Sophos Disk Encryption and manage it via the **Full disk encryption** policy in Enterprise

Console, you can continue to do so after the upgrade to Enterprise Console 5.3.0 and until Sophos Disk Encryption retires.

For information about how to upgrade Sophos Disk Encryption 5.61 to SafeGuard Enterprise, see Appendix A: Upgrade Sophos Disk Encryption 5.61 to SafeGuard Enterprise (page 14).

If you didn't use Sophos Disk Encryption before the upgrade to Enterprise Console 5.3.0, you can add it after the upgrade, if you wish. Be aware, however, that Sophos Disk Encryption 5.61 is not supported on Windows 8 or later. If you want to use encryption on Windows 8 and later computers, you might want to consider using SafeGuard Encryption instead.

3.1 How do I add Sophos Disk Encryption?

If you use Sophos Disk Encryption and manage it from Enterprise Console, you do not need to do anything. Sophos Disk Encryption will continue to work as before the upgrade.

If you do not use Sophos encryption but would like to add it now:

- If you are upgrading from Enterprise Console 5.1 or later, you will have to upgrade to Enterprise Console 5.3.0 first, and then re-run the Enterprise Console 5.3.0 installer to add encryption.
- If you are upgrading from Enterprise Console 5.0, the installer will display the **Manage Encryption** page where you can choose to manage encryption (as described in Upgrade Enterprise Console (page 10)).

After you have added encryption, you need to set up encryption software on endpoint computers as described in Appendix B: Set up encryption software on endpoint computers (page 14).

4 What are the steps in upgrading?

Upgrading involves the following steps.

- Check the system requirements.
- Check the accounts you need.
- Check whether you need to change your software subscriptions.
- Download the installer.
- Upgrade Enterprise Console.

If your license includes encryption and if you haven't used it before the upgrade, you might also want to set up encryption software on endpoint computers after you upgrade Enterprise Console.

5 System requirements

.NET Framework 4.0

The Enterprise Console 5.3.0 installer installs .NET Framework 4.0, unless it is already installed.

Important: As part of the .NET Framework 4.0 installation some system services (such as IIS Admin Service) may restart.

After .NET Framework 4.0 is installed, you may receive a message asking you to restart your computer. If you do, we recommend that you restart the computer immediately or shortly after the installation.

For a full list of system requirements, see the system requirements page of the Sophos website http://www.sophos.com/en-us/products/all-system-requirements.aspx.

Tip: You can run the Enterprise Console installer to check if your system meets the requirements for the upgrade, even if you do not want to proceed with the upgrade immediately. You can view the results of the system check on the **System Property Checks** page of the installation wizard. After you have reviewed the results, click **Cancel** to close the wizard. For more information about the system check results, go to http://www.sophos.com/en-us/support/knowledgebase/113945.aspx.

5.1 Free disk space requirements

The amount of free disk space you need to upgrade Enterprise Console depends on the size of the Enterprise Console database files (.mdf files) and transaction log files (.ldf files) that are currently in use.

Tip: The file names begin with "SOPHOS" and usually contain Enterprise Console version number.

For information about the database file names for different console versions and how to locate the database files on disk, see Sophos support knowledgebase article 17323 (http://www.sophos.com/en-us/support/knowledgebase/17323.aspx).

To ensure that you have sufficient disk space to upgrade Enterprise Console, do the following:

- Check the disk drive on which the database files (.mdf files) are deployed and ensure that it has free capacity of at least three times the current size of the .mdf files.
- Check that the disk drive on which the transaction log files (.ldf files) are deployed and ensure that it has free capacity of at least eight times the current size of the database files (.mdf files).
- If both .mdf and .ldf files are deployed on the same disk, ensure that it has free capacity of at least 10 times the current size of the .mdf files.

If you have upgraded Enterprise Console in the past, you may still have old Enterprise Console databases that are no longer required. You may consider deleting those databases to free up disk space. For more information, see Sophos support knowledgebase article 17508 (http://www.sophos.com/en-us/support/knowledgebase/17508.aspx).

6 The accounts you need

Accounts required to perform the upgrade

Ensure that the user logged on to and running the upgrade on the management server has sufficient rights to all Sophos databases. The user running the management server upgrade should be a member of the "db_owner" role on each of the Sophos databases (members of the server role "sysadmin" would implicitly have sufficient rights to all databases). These rights are only required temporarily during the upgrade, to check that the new databases have been created and to migrate the data.

Note: For a list of database names per version of the console, see Sophos support knowledgebase article 17323 (http://www.sophos.com/en-us/support/knowledgebase/17323.aspx).

Sophos database account

When you upgrade your management 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 management console is installed. For distributed installations of Enterprise Console, the account must be able to log onto the computer where the Sophos Management Server component 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/en-us/support/knowledgebase/113954.aspx).

7 Will I get the same updates as before?

Since version 5.2.1, Enterprise Console supports new options for getting your automatic updates from Sophos and doesn't support some of the old ones. If you are upgrading from an earlier

version, depending on the software packages you selected when you installed Enterprise Console, you may need to change your software subscription settings before you upgrade.

To open an endpoint software subscription, on the **View** menu, click **Update Managers**. In the **Software Subscriptions** pane, double-click the subscription you want to check.

To open an update manager software subscription, in the **Update managers** view, double-click the update manager you want to check. In the **Configure update manager** dialog box, go to the **Advanced** tab.

The following matrix shows whether you can or cannot upgrade with your current settings.

Software package	Upgrade possible	Advice, if applicable
Endpoint		
Recommended (default)	Yes	
Previous	Yes	
Oldest	No	Resubscribe to a different package, for example, "Previous".
Extended Maintenance Recommended	Yes	
Extended Maintenance Previous	Yes	
Extended Maintenance Oldest	No	Resubscribe to a different package, for example, "Extended Maintenance Previous".
Fixed (e.g. *10.3.11.2 VE3.53.0*)	Yes	You do not need to do anything immediately, but you should read About fixed version software (page 8).
Update Manager		
1 Recommended (default)	Yes	
Preview	Yes	
Extended	Yes	
1 Previous	No	Resubscribe to "1 Recommended". For more information, read About Sophos Update Manager upgrade (page 8).
1 Oldest	No	
Fixed (e.g. *1.5.4.11*)	No	

If your software package is no longer supported and you don't change your subscription before upgrading, the installer will warn you about the unsupported subscriptions and you won't be able to proceed with the upgrade. For more information about software packages, see http://www.sophos.com/en-us/support/knowledgebase/112580.aspx.

7.1 About fixed version software

Since Enterprise Console 5.2.1, fixed versions are no longer displayed by default in the **Software Subscription** dialog box. If you are subscribed to a fixed software version and don't change your software subscription before upgrading, you will still be subscribed to the same fixed version after the upgrade and it will continue to be downloaded. However, you will not be able to subscribe to a different fixed version, and once you unsubscribe from a fixed version, it will be permanently removed from the list of available packages in the **Software Subscription** dialog box. For more information, see http://www.sophos.com/en-us/support/knowledgebase/119240.aspx.

Note: The option **Automatically upgrade fixed version software when it is no longer supported by Sophos** is always enabled since Enterprise Console 5.2.1 and you cannot disable it. If in an earlier version of Enterprise Console you disabled this option in your software subscription, the option will be automatically enabled during the upgrade and the check box in the **Software Subscription** dialog box will disappear.

7.2 About Sophos Update Manager upgrade

Since version 5.2.1, Enterprise Console supports only one, recommended Sophos Update Manager software package. If you are upgrading from a version earlier that 5.2.1, Update Manager (and any additional Update Managers, if you use them) must be subscribed to the "1 Recommended" package. Otherwise, you won't be able to upgrade.

If you are not subscribed to the "1 Recommended" package, you will need to subscribe to it and ensure that Update Manager has been updated to the latest recommended version before upgrading Enterprise Console.

If the Update Manager installer in the share `\\Servername\SUMInstallSet` on the computer where Enterprise Console management server is installed is earlier than the latest recommended version, the installer will be updated during the upgrade.

8 Download the installer

This section assumes that you have a MySophos account and that you have associated your license credentials with it. If you need help, see www.sophos.com/en-us/support/knowledgebase/111195.aspx.

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

1. Go to www.sophos.com/en-us/support/downloads.aspx.
2. Type your MySophos username and password.

   You see a web page that shows your licenses.

3. Under your license name, find the **Console** downloads and download the Enterprise Console installer.

9 Upgrade Enterprise Console

9.1 Back up Enterprise Console data and configuration

Before you upgrade Enterprise Console, use the DataBackupRestore.exe tool to back up:

- Databases: Enterprise Console (core) - SOPHOS5x, Patch - SOPHOSPATCH or SOPHOSPATCH5x, Encryption - SOPHOSENC5x, and Auditing - SophosSecurity.
- Registry settings
- Account information
- Configuration files

Important: The DataBackupRestore.exe tool will back up the Sophos management server's configuration only from a default installation location. Backing up or restoring the configuration files will fail if you have installed Enterprise Console to a non-default location. The default location is:

- Windows 64-bit: %programfiles(x86)%\Sophos\Enterprise Console\
- Windows 32 **and** 64-bit: %programfiles%\Sophos\Enterprise Console\

If you use a non-default installation location, see knowledgebase article 114299 (http://www.sophos.com/en-us/support/knowledgebase/114299.aspx#knownissues) for advice.

If Enterprise Console databases are on a remote server, you can use Sophos tools BackupDB.bat and RestoreDB.bat to back up and restore the databases. For more information, see knowledgebase article 110380 (http://www.sophos.com/en-us/support/knowledgebase/110380.aspx).

To back up the Enterprise Console data and configuration:

1. Log on as the Administrator to the computer where the Enterprise Console management server is installed.
2. Open Command Prompt (click **Start**, **Run**, type **cmd**, and then press Enter).
3. Browse to the folder containing the tool.
   - In Windows 64-bit, type:

     ```
     cd "C:\Program Files (x86)\Sophos\Enterprise Console\"
     ```

   - In Windows 32-bit, type:

     ```
     cd "C:\Program Files\Sophos\Enterprise Console\"
     ```

4. To back up everything, type:

   `DataBackupRestore.exe -action=backup`

   To display the usage options, type:

   `DataBackupRestore.exe -?`

   For more information about using the tool, see also knowledgebase article 114299 (http://www.sophos.com/en-us/support/knowledgebase/114299.aspx).

You are now ready to upgrade Enterprise Console.

9.2 Upgrade Enterprise Console

Important:

If you have the Sophos Management Database component installed on a separate server, you must upgrade the database component first before upgrading the management server.

You must not make any changes in Enterprise Console (for example, change policy settings) between upgrading the database and upgrading the management server.

For more information about upgrading the database on a remote server, including upgrading on a secure server using a script and upgrading in a clustered SQL Server environment, see Sophos support knowledgebase article 33980 (http://www.sophos.com/en-us/support/knowledgebase/33980.aspx).

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.
5. If you are upgrading from Enterprise Console 5.0 and want to add Sophos Disk Encryption:
   a) On the **Manage Encryption** page of the wizard, select **Manage encryption**.
   b) On the **Sophos Encryption** page, click **New installations**. You are prompted to create a password for the certificates backup store. Make a note of the password.
6. Complete the wizard.

If you have upgraded from Enterprise Console 5.1 and want to add Sophos Disk Encryption, re-run the Enterprise Console 5.3.0 installer. The installer will now display the options for managing encryption, as described in step 5 above.

After you have added encryption, you need to set up encryption software on endpoint computers as described in Appendix B: Set up encryption software on endpoint computers (page 14).

Important: The new Sophos Auditing database, **SophosSecurity**, must be present and running side by side with the other Enterprise Console databases, even if you don't intend to use the

Sophos Auditing feature. This is because the database is used for enhanced access control as well as for logging audit events.

9.3 Enhance database security

Audit the database

In addition to the protection built into the Enterprise Console databases, we recommend setting additional protection at the SQL Server instance level (if not already in place) to audit user activities and changes on your SQL Server.

For example, if you are using an Enterprise edition of SQL Server 2008, you can use the SQL Server Audit feature. Earlier versions of SQL Server support login auditing, trigger-based auditing, and event auditing by using a built-in trace facility.

For more information about features that you can use for auditing activities and changes on your SQL Server system, see the documentation for your version of SQL Server. For example:

- SQL Server Audit (Database Engine)
- Auditing (Database Engine), SQL Server 2008 R2
- Auditing in SQL Server 2008
- Auditing (Database Engine), SQL Server 2008

Encrypt connections to the database

We strongly recommend that you encrypt connections between any clients and the Enterprise Console databases. For more information, see the SQL Server documentation:

- Enable Encrypted Connections to the Database Engine (SQL Server Configuration Manager)
- Encrypting Connections to SQL Server 2008 R2
- How to enable SSL encryption for an instance of SQL Server by using Microsoft Management Console

Control access to the database backups

Ensure proper, restrictive access control to any database backups or copies. This will ensure that unauthorized users cannot access the files, tamper with them, or accidentally delete them.

Note: The links in this section lead to information maintained by third parties and are provided for your convenience. Although we try to review the accuracy of the links periodically, the links may change without our knowledge.

9.4 Check existing policies

9.4.1 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.

9.4.2 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, do the following.

Note: Features not included in your license, which were displayed in previous versions of Enterprise Console, may no longer be displayed.

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.

You have finished upgrading Enterprise Console.

If you want to set up encryption software on endpoint computers, go to Appendix B: Set up encryption software on endpoint computers (page 14).

10 Enable Malicious Traffic Detection

Enterprise Console 5.3.0 introduces support for Malicious Traffic Detection, which detects communications between endpoint computers and command and control servers involved in botnet or other malware attacks. To benefit from this new feature, you need to enable it after the upgrade.

Note: Malicious traffic detection is currently supported only on Windows 7 and later non-server operating systems and is first available in Endpoint Security and Control 10.6.0.

1. Check which anti-virus and HIPS policy is used by the group or groups of computers for which you want to enable the new feature.

   In the **Groups** pane, right-click the group. Select **View/Edit Group Policy Details**. In the group details dialog box, you can see the policies currently used.

2. In the **Policies** pane, double-click **Anti-virus and HIPS**.
3. Double-click the policy you want to change.

   The **Anti-Virus and HIPS policy** dialog box is displayed.

4. In the **On-access scanning** panel, make sure the **Enable behavior monitoring** check box is selected.
5. Beside **Enable behavior monitoring**, click **Configure**.
6. In the **Configure Behavior Monitoring** dialog box, make sure the **Detect malicious behavior** check box is selected.
7. To enable malicious traffic detection, select the **Detect malicious traffic** check box.

   Note: Malicious traffic detection uses the same set of exclusions as the Sophos Anti-Virus on-access scanner.

11 Appendices

11.1 Appendix A: Upgrade Sophos Disk Encryption 5.61 to SafeGuard Enterprise

Migration from Sophos Disk Encryption 5.61 to SafeGuard Enterprise involves the following steps:

- Export the SEC company certificate: In Enterprise Console on the **Tools** menu, click **Manage Encryption** and select **Backup Company Certificate**. Select a destination directory and file name and enter a password for the .P12 file when prompted.
- Install SafeGuard Management Center and SafeGuard Enterprise Server.

  Note: If you have the SEC management server with encryption installed on this server, install SafeGuard Enterprise on a different server.

- In the SafeGuard Management Center configuration wizard, select a new database to be created and import the company certificate exported before.
- In SafeGuard Management Center, create the endpoint configuration package: On the **Tools** menu, click **Configuration Packages Tool**. Select **Managed client packages**, make your edits and create the configuration package.
- Deploy the configuration package to the endpoints. After the endpoints have received it, they are able to connect to SafeGuard Enterprise Server. From that time on, the endpoint can be managed by SafeGuard Management Center.
- In SafeGuard Management Center, create and assign policies as desired.

The migrated endpoints remain visible in Enterprise Console as "managed by SafeGuard Enterprise". All non-encryption related tasks can still be performed on them.

For detailed information on SafeGuard Enterprise installation, see the *SafeGuard Enterprise installation guide*.

11.2 Appendix B: Set up encryption software on endpoint computers

Read this section if:

- Your license includes encryption.
- You are not currently using Sophos encryption.
- You have installed Enterprise Console to manage encryption.

Warning: When you are installing the Sophos encryption software for the first time, we strongly recommend that you enable and test each setting step by step.

To set up full disk encryption on computers you:

- Subscribe to encryption software.
- Prepare to install encryption software.
- Install encryption software automatically.
- Install encryption software manually.

Note: Full disk encryption can be installed on Windows XP, Windows Vista and Windows 7 computers but not on Windows 8 or later computers or Macs.

Warning: Before you install full disk encryption on computers, you must:

- Make sure that drives encrypted with third-party encryption software have been decrypted and that the third-party encryption software is uninstalled.
- Create a full backup of the data on computers.

For a complete list of preparations, see Prepare computers for installation (page 17).

11.2.1 Subscribe to encryption software

Note: We recommend that you create a new subscription for encryption.

To subscribe to the encryption software:

1. In Enterprise Console, on the **View** menu, click **Update Managers**.
2. To create a new subscription, in the **Software Subscriptions** pane, click **Add** at the top of the pane. In the **Software Subscription** dialog box, type a name for the subscription in the **Subscription name** box. Under **Encryption Products**, next to **Windows XP and above**, click in the **Version** box, and select the latest "Recommended" version (version 5.61 at the time of this release). Click **OK**.
3. To add the subscription to the **Update Managers**, in the **Update managers** pane, right-click the update manager and select **View/Edit configuration**. In the **Configure update manager** dialog box, on the **Subscriptions** tab, select the subscription in the **Available** list and click the > button to move it to the **Subscribed to** list. Click **OK**.

The encryption software is downloaded to the default share \\<server_name>\SophosUpdate\CIDs\<subscription>\ENCRYPTION.

To download to shares other than the default share, see Specify where the software is placed (page 15).

To change the default update schedule, see Edit an update schedule (page 16).

Note: You cannot have the encryption software installed by applying update polices to a group of computers. You need to trigger the installation of the encryption software yourself.

For further information on the full disk encryption policy, see the *Enterprise Console policy setup guide*.

11.2.2 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 16).

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

11.2.3 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.

11.2.4 Preparing to install encryption software

Preparing to install encryption software on computers involves the following tasks:

- Give administrators access on computers after installation.
- Prepare computers for installation.

11.2.4.1 Give administrators access to computers after installation

Administrators might need to access and pre-configure computers after you have installed encryption software, for example to install other software. However, the first user who logs on after installation activates the Power-on Authentication.

To avoid this, add the respective administrators to a list of exceptions, as follows:

1. In Enterprise Console, in the **Policies** pane, double-click **Full disk encryption**. Double-click the **Default** policy to edit it.
2. Under **Power-on Authentication (POA)** click **Exceptions** next to **Enable Power-on Authentication**.
3. In **Exceptions**, click **Add**, enter the **User name** and the **Computer or domain name** of the relevant Windows account(s) and click **OK**.

   You can use wildcards as the first or last character. In the **User name** field, the ? character is not allowed. In the **Computer or Domain Name** field, the characters / \ [ ] : ; | = , + ? < > " are not allowed.
4. In the **Default** policy dialog, click **OK**.
5. In the **Policies** pane, select the policy and drag it onto the group to which you want to apply the policy. When prompted, confirm that you want to continue.

11.2.4.2 Prepare computers for installation

If your license includes full disk encryption, you must do the following before you install encryption software on computers:

- Make sure that drives encrypted with third-party encryption software have been decrypted and that the third-party encryption software is uninstalled.
- Create a full backup of the data.
- Check if a Windows user account with credentials is set up and active for the user on the endpoint computer.
- Make sure that the computer has already been protected with Sophos anti-virus software version 10 before you deploy full disk encryption.
- Uninstall third-party boot managers, such as PROnetworks Boot Pro and Boot-US.
- Create a full backup of the data.

- Check the hard disk(s) for errors with this command:

  `chkdsk %drive% /F /V /X`

  You might be prompted to restart the computer and run **`chkdsk`** again. For further information, see: http://www.sophos.com/en-us/support/knowledgebase/107799.aspx.

  You can check the results (log file) in the Windows Event Viewer:

  Windows XP: Select **Application**, **Winlogon**.
  Windows 7, Windows Vista: Select **Windows Logs**, **Application**, **Wininit**.

- Use the Windows built-in **`defrag`** tool to locate and consolidate fragmented boot files, data files, and folders on local drives:

  `defrag %drive%`

  For further information, see: http://www.sophos.com/en-us/support/knowledgebase/109226.aspx.

- If you have used an imaging/cloning tool on the computer, clean the master boot record (MBR). Start the computer from a Windows DVD and use the command **`FIXMBR`** within the Windows Recovery Console. For further information, see: http://www.sophos.com/en-us/support/knowledgebase/108088.aspx.

- If the boot partition on the computer has been converted from FAT to NTFS, and the computer has not been restarted since then, restart the computer. If you do not do this, the installation may not complete successfully.

- Open Windows Firewall with Advanced Security, using the **Administrative Tools** item in Control Panel. Ensure that **Inbound connections** are allowed. Change the **Inbound rules** to enable the processes below:

  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

  When installation is complete and you want to continue using Windows Firewall, you may disable the processes again.

11.2.5 Install encryption software automatically

Warning: If you are installing the Sophos encryption software for the first time, we strongly recommend that you enable and test each setting step-by-step.

Make sure that the endpoints have been prepared for full disk encryption installation, in particular that third-party encryption software has been uninstalled, all data has been backed up and that Sophos anti-virus software version 10 has been installed.

To install encryption software automatically:

1. In Enterprise Console, select the computers on which you want to install full disk encryption.

2. Right-click the computer, and then click **Protect computers**. The **Protect Computers Wizard** is launched.
3. On the **Welcome** page, click **Next**.
4. On the **Installation Type** page, select **Encryption software**.
5. If there is more than one encryption subscription and installer location (bootstrap location) available, the **Encryption location** page is displayed. Select the **Encryption subscription** and **Address** to install from.
6. On the **Encryption summary** page, check for any installation problems.
7. On the **Credentials** page, enter details of an account that can be used to install software on computers.

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

The installation of encryption will cause computers to restart automatically within about 30 minutes after installation of the encryption software. If encryption is enabled by policy, it will only take place after the computer's restart.

For further information on the start behaviour of the computer and first logon after installation and activation of encryption, see First logon after installation (page 20).

11.2.6 Install encryption software manually

Warning: If you are installing the Sophos encryption software for the first time, we strongly recommend that you enable and test each setting step-by-step.

If you have computers that you cannot protect automatically, protect them by running an installer from the shared folder to which the encryption software has been downloaded. This shared folder is known as the *bootstrap location*.

Make sure that the endpoints have been prepared for full disk encryption installation, in particular that third-party encryption software has been uninstalled, all data has been backed up and that Sophos anti-virus software version 10 has been installed.

During the installation of full disk encryption, make sure that only one user session is active on the endpoint. If you do not do this, the installation will fail.

You must log on to the computers that you want to protect as a Windows administrator.

To install encryption software on computers manually:

1. To find out which directory the installer is in, open Enterprise Console and select **Bootstrap locations** from the **View** menu.

   In the **Bootstrap Locations** dialog box, the **Location** column displays the bootstrap location for each platform. Make a note of the relevant paths.

2. At the computer that hosts the bootstrap location, create a read-only user account.
3. Go to each computer and log on with local administrator rights.
4. Locate the encryption setup program setup.exe in the bootstrap location and double-click it.

   The encryption setup program can be found in the following location:
   \\<ServerName>\SophosUpdate\CIDs\<Subscription>\ENCRYPTION
5. A wizard guides you through installation of the encryption software.

For further information on the start behaviour of the computer and first logon after installation and activation of encryption, see First logon after installation (page 20).

11.2.7 First logon after installation

After encryption is installed, the computer restarts and the user is prompted to log on. The computer's behavior depends on the kind of account the user logs on with:

- log on as end user with normal Windows account.
- log on for administrative tasks with Windows account that has been put on the list of exceptions.

Log on as end user with normal Windows account

The logon procedure only corresponds to the one described here if Power-on-Authentication and encryption have been enabled in the full disk encryption policy.

When the computer restarts, a number of messages (for example, the autologon screen) are displayed. Then the Windows operating system starts. The user logs on to Windows with their Windows credentials. The user is registered as a Sophos SafeGuard user on the computer.

Note: After successful registration, a tool tip confirming this is shown on the endpoint computer.

If enabled by policy, encryption starts on the selected drives. Encryption and decryption are performed in the background without any user interaction. The user may continue working or shut down the computer during the encryption process. No restart is required after encryption is completed.

The next time the user starts the computer, Power-on Authentication is activated. From now on, the user only has to enter their Windows credentials at the Power-on Authentication and is automatically logged on to Windows.

Note: When starting the computer from hibernation, the user needs to enter their Windows credentials at Power-on Authentication and at Windows.

For further information, see the *Sophos Disk Encryption user help*.

Log on for administrative tasks with Windows account that has been put on the list of exceptions

The logon procedure only corresponds to the one described here if the user logs on with a Windows account that has been put on a list of exceptions and Power-on-Authentication has been enabled in the full disk encryption policy.

When the computer restarts, the Windows operating system starts. The Windows logon is displayed. The user logs on with their credentials as previously defined in the full disk encryption policy. The user is logged on to Windows as a guest user. Power-on Authentication is not activated. The encryption process does not start. The user can carry out post-installation tasks as required.

12 Technical support

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

- Visit the SophosTalk community at community.sophos.com/ and search for other users who are experiencing the same problem.
- Visit the Sophos support knowledgebase at www.sophos.com/en-us/support.aspx.
- Download the product documentation at www.sophos.com/en-us/support/documentation.aspx.
- Open a ticket with our support team at https://secure2.sophos.com/support/contact-support/support-query.aspx.

13 Legal notices

ACE™, TAO™, CIAO™, DAnCE™, and CoSMIC™

of Washington University, St. Louis for the development of open-source software as part of the open-source software community. Submissions are provided by the submitter "as is" with no warranties whatsoever, including any warranty of merchantability, noninfringement of third party intellectual property, or fitness for any particular purpose. In no event shall the submitter be liable for any direct, indirect, special, exemplary, punitive, or consequential damages, including without limitation, lost profits, even if advised of the possibility of such damages. Likewise, 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. 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.

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 companies 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. Likewise, DOC software is compliant with the new US daylight savings rule passed by Congress as "The Energy Policy Act of 2005," which established new daylight savings times (DST) rules for the United States that expand DST as of March 2007. Since DOC software obtains time/date and calendaring information from operating systems users will not be affected by the new DST rules as long as they upgrade their operating systems accordingly.

The names ACE™, TAO™, CIAO™, DAnCE™, 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. This license grants no permission to call products or services derived from this source ACE™, TAO™, CIAO™, DAnCE™, or CoSMIC™, nor does it grant permission for the name Washington University, UC Irvine, or Vanderbilt University to appear in their names.

If you have any suggestions, additions, comments, or questions, please let me know.

Douglas C. 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

Boost

Version 1.0, 17 August 2003

Permission is hereby granted, free of charge, to any person or organization obtaining a copy of the software and accompanying documentation covered by this license (the “Software”) to use, reproduce, display, distribute, execute, and transmit the Software, and to prepare derivative works of the Software, and to permit third-parties to whom the Software is furnished to do so, all subject to the following:

The copyright notices in the Software and this entire statement, including the above license grant, this restriction and the following disclaimer, must be included in all copies of the Software, in whole or in part, and all derivative works of the Software, unless such copies or derivative works are solely in the form of machine-executable object code generated by a source language processor.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

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/en-us/support/contact-support/contact-information.aspx. 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.

Loki

The MIT License (MIT)

Copyright © 2001 by Andrei Alexandrescu

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

OpenSSL Cryptography and SSL/TLS 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 (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay license

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

This package is an SSL implementation written by Eric Young (eay@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 (eay@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.]

WilsonORMapper

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

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- 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.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "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 COPYRIGHT HOLDER 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.