SOPHOS

Security made simple.

Sophos Enterprise Console quick startup guide

Product version: 5.2

Document date: September 2014

Contents

1 About this guide

This guide tells you how to protect your network with Sophos security software.

The guide is for you if:

- You are installing the software for the first time.
- You are installing the protection and encryption features (encryption is optional).

If you are upgrading, see the *Sophos Enterprise Console upgrade guide* instead.

Other documents you might need

If you have a very large network, you may want to consider the installation options in the *Sophos Enterprise Console advanced startup guide*.

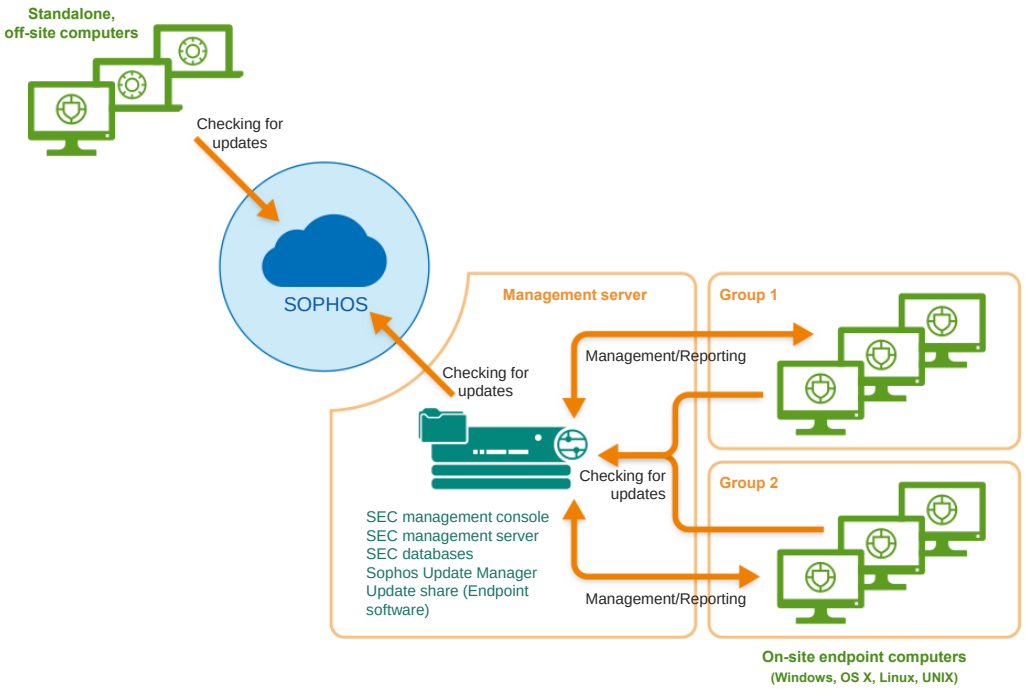
If you currently use Sophos encryption software that is not managed from Enterprise Console, see the upgrade advice in the *Sophos Disk Encryption License migration guide*.

Sophos documentation is published at http://www.sophos.com/en-us/support/documentation.aspx.

2 What do I install?

To protect your network, you install:

- **Sophos Enterprise Console** on your server. This enables you to install and manage Sophos security software.
- **Sophos protection software** on your endpoint computers. This protects the computers against threats and sends alerts to Enterprise Console.
- **Sophos encryption software** on your endpoint computers (if your license includes it).



3 What are the key steps?

You carry out these key steps:

- Download the Enterprise Console installer.
- Check the system requirements.
- Create the accounts you need.
- Prepare for installation.
- Install Enterprise Console.
- Download protection and encryption software.
- Create computer groups.
- Set up security policies.
- Search for computers.
- Prepare to protect computers.
- Protect computers.
- Set up encryption on computers, if your license includes it.
- Check the health of your network.

4 Download the Enterprise Console installer

- **If you have a Sophos license**

The following steps assume that you have a MySophos account and that you have associated your license credentials with it. If you need help, go to www.sophos.com/en-us/support/knowledgebase/111195.aspx.

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

   You see a webpage that shows your license or licenses.

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

- **If you want to evaluate Enterprise Console**

1. Go to http://www.sophos.com/en-us/products/free-trials/endpoint-protection.aspx.
2. Complete the registration form.

   After you submit the registration form, your evaluation credentials will be displayed. The credentials will also be sent to the email address you entered in the registration form. You will need them when setting up Enterprise Console.

3. Click **Download now** and download the Enterprise Console installer.

5 Check the system requirements

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

Tip: You can run the Enterprise Console installer to check if the server meets the requirements for the installation, even if you do not want to proceed with the installation 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 Hardware and operating system

For hardware and operating system requirements, see the system requirements page of the Sophos website (http://www.sophos.com/en-us/products/all-system-requirements.aspx).

5.2 Microsoft system software

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

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

Whichever installer you use, read the advice below.

Note: After you install the required system software, you may need to restart your computers. For more information, go to www.sophos.com/en-us/support/knowledgebase/65190.aspx.

SQL Server installation

The installer attempts to install SQL Server 2008 R2 Express Edition with Service Pack 1 (SP1), unless you choose to use an existing instance of SQL Server 2005 Express or later. Note that:

- We recommend that you do not install SQL Server on a domain controller.
- SQL Server 2008 R2 Express is not compatible with Windows Server 2003 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 4.0, unless it is already installed. Note that:

- 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.

Microsoft Message Queuing installation

The installer attempts to install Microsoft Message Queuing (MSMQ), unless it is already installed. Note that:

- During MSMQ installation, the following services are stopped: MSDTC, MSSQLServer, SQLSERVERAGENT. This interrupts access to the default SQL Server database.

You should ensure that the services can safely be stopped during installation. You should also check that they have restarted afterwards.

5.3 Port requirements

Enterprise Console requires certain ports to be open. For more information, go to http://www.sophos.com/en-us/support/knowledgebase/38385.aspx.

6 The accounts you need

Before you install Sophos software, you should create the user accounts you need:

- **Database account.** This is a Windows user account that enables Enterprise Console's management service to connect to the database. It is also used by other Sophos services.

  We recommend that you name the database account **SophosManagement**.

- **Update Manager account.** This is a Windows user account that enables your endpoint computers to access the folders where Enterprise Console puts software updates.

  We recommend that that you name the Update Manager account **SophosUpdateMgr**.

6.1 Database account

The database account should:

- Be able to log onto the computer where you are going to install the Sophos Management Server (a component of Enterprise Console).
- Be able to read and write to the system temporary directory e.g. "\windows\temp\". By default members of "Users" have this right.
- Have a UPN (User Principal Name) associated with the account if it is a domain account.

All other rights and group memberships that it needs are granted automatically during installation.

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 installation.
- Is named **SophosManagement**.

For recommendations and step-by-step instructions, go to www.sophos.com/en-us/support/knowledgebase/113954.aspx.

6.2 Update Manager account

The Update Manager account should have Read access to the folder where Enterprise Console puts software updates. By default this is: \\[servername]\SophosUpdate

Sophos recommends that the account:

- Is not set to expire and does not have any other logon restriction.
- Is not an administrative account.
- Has a UPN (User Principal Name) associated with the account if it is a domain account.

- Is named **SophosUpdateMgr**.

For recommendations and step-by-step instructions, go to www.sophos.com/en-us/support/knowledgebase/113954.aspx.

7 Prepare for installation

Prepare for installation 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 User Account Control (UAC) is enabled on the server, turn off UAC and restart the server.

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

8 Install Enterprise Console

To install Enterprise Console:

1. At the computer where you want to install Enterprise Console, log on as an administrator:
   - If the 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.
3. Double-click the installer.
4. When you are prompted, click **Install**.

   The installation files are copied to the computer and a wizard starts.
5. The wizard guides you through installation. You should do as follows:
   a) Accept the defaults wherever possible.
   b) On the **Components Selection** page, ensure that all the components are selected.
   c) On the **System Property Checks** page, review the system check results and take action if necessary. For more information about the system check results, go to http://www.sophos.com/en-us/support/knowledgebase/113945.aspx.
   d) On the **Database Details** page, enter the details of the database account you created in Database account (page 10).
   e) On the **Sophos Update Manager Credentials** page, enter the details of the Update Manager account you created in Update Manager account (page 10).
   f) On the **Manage Encryption** page, click **Manage Encryption**, if you want to use Enterprise Console to manage encryption.

      Note: If you click **Do not manage encryption** or if you have SafeGuard Enterprise installed on this computer, there are no further installation options. Go straight to step 6.

   g) On the **Sophos Encryption** page, click **New installations** if you do not have an earlier version of Sophos Disk Encryption installed on the network. You are prompted for the password for the certificates backup store. Make a note of the password.
6. When installation is complete, you may be prompted to restart. Click **Yes** or **Finish**.

Important: The 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 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.

10 Download protection and encryption software

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

Note: If you used Remote Desktop for installation, the console does not open automatically. Open it from the Start menu.

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

1. On the **Sophos download account details** page, enter the username and password printed on your license schedule or your evaluation credentials. If you access the internet via a proxy server, select the **Access Sophos via a proxy server** check box and enter the proxy details.
2. On the **Platform selection** page, select only the platforms you need to protect now.
3. If your license includes encryption, on the **Software type** page, select **Encryption** if you want to download it now.

   When you click **Next**, Enterprise Console begins downloading your software.
4. On the **Downloading software** page, downloading progress is displayed. Click **Next** at any time.
5. On the **Import computers from Active Directory** page, select **Set up groups for your computers** if you want Enterprise Console to use your existing Active Directory computer groups.

Note: For information about protecting Windows 8 computers, go to http://www.sophos.com/en-us/support/knowledgebase/118261.aspx.

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

11 Create computer groups

If you used the **Download Security Software Wizard** to set up your computer groups (based on your Active Directory groups), skip this section. Go to Set up security policies (page 17).

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

1. If Enterprise Console is not already open, open it.
2. In the **Groups** pane (on the left-hand side of the console), ensure that the server name shown at the top is selected.
3. On the toolbar, click the **Create group** icon.

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

4. Type a name for the group.

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

12 Set up security policies

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

- If you want to use Sophos Client Firewall, we recommend that you set up the firewall policy before deploying the firewall to computers.
- You must edit the application control, device control, patch or web control policies if you want to use these features. You can do this any time.
- By default, full disk encryption is not enabled after installation on computers. You must edit the full disk encryption policy to encrypt drives on computers. You can edit this any time. By default, Power-on Authentication is enabled.

  You must edit this policy to give administrators access to computers for further installation or verification tasks. You must configure this before installing full disk encryption, see Give administrators access to computers after installation (page 23).

  Note: We recommend that for a first-time installation, you configure encryption by enabling and testing each setting step-by-step.

12.1 Set up a firewall policy

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

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

1. In the **Policies** pane, right-click **Firewall**, and click **Create Policy**.

   A **New Policy** is added to the list, with its name highlighted. Type the name that you want to use for the policy.

2. Double-click the policy to edit it.

   A wizard is launched.

3. In the **Firewall Policy Wizard** we recommend that you make the following selections.

   a) On the **Configure firewall** page, select **Single location** unless you want the firewall to use different settings according to the location where you use it.

   b) On the **Operational Mode** page, select **Block inbound and allow outbound traffic**.

   c) On the **File and print sharing** page, select **Allow file and print sharing**.

13 Search for computers

If you used the **Download Security Software Wizard** to set up your computer groups (based on your Active Directory groups), skip this section. Go to Prepare to protect computers (page 19).

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

1. Click the **Discover computers** icon in the toolbar.
2. Select the method you want to use to search for computers.
3. Enter account details if necessary and specify where you want to search.

If you use one of the **Discover** options, the computers are placed in the **Unassigned** group.

14 Prepare to protect computers

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

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

14.1 Prepare for removal of third-party security software

If you want the Sophos installer to remove any previously installed security software, do the following:

- If computers are running another vendor's anti-virus software, ensure that its user interface is closed.
- If computers are running another vendor's firewall or HIPS product, ensure that it is turned off or configured to allow the Sophos installer to run.

If computers are running another vendor's update tool, you may want to remove it. See "Remove third-party security software" in the "Protecting computers" section of the Enterprise Console Help.

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

You will be prompted to enter details of a Windows user account that can be used to install security software. This is typically a domain administrator account. It must:

- Have local administrator rights on computers you want to protect.
- Be able to log on to the computer where you installed Enterprise Console.
- Have read access to the location that computers will update from. To check this location, in the **Policies** pane, double-click **Updating**, and then double-click **Default**.

14.3 Prepare for installation of anti-virus software

You may need to prepare computers prior to installation of anti-virus software. Check the following knowledgebase articles for advice:

- If you use Active Directory, see www.sophos.com/en-us/support/knowledgebase/116754.aspx.
- If you use workgroups, see www.sophos.com/en-us/support/knowledgebase/116755.aspx.

15 Protect computers

This section tells you how to:

- Protect Windows computers automatically.
- Protect Windows computers or Macs manually.
- Protect Linux computers (if your license includes this).

You can also use your own tools or scripts for installing protection on Windows computers. For details, go to www.sophos.com/en-us/support/knowledgebase/114191.aspx.

15.1 Protect Windows computers automatically

To protect computers:

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 **Welcome** page, click **Next**.

   b) On the **Installation Type** page, leave the option **Protection software** selected.

   c) On the **Select features** page, you can choose to install optional features.

   The current version of the firewall (included with Endpoint Security and Control 10.2 or earlier) cannot be installed on Windows 8 computers.

   d) On the **Protection summary** page, check for any installation problems. For help, see Troubleshooting (page 28).

   e) On the **Credentials** page, enter details of a Windows user account that can be used to install software on computers.

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

When installation is complete, look at the list of computers again. In the **On-access** column, the word **Active** indicates that the computer is running on-access virus scanning.

15.2 Protect Windows computers or Macs manually

15.2.1 Locate the installers

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

To locate the installers:

1. In Enterprise Console, on the **View** menu, click **Bootstrap Locations**.

   A list of locations is displayed.

2. Make a note of the location for each operating system you want to protect.

15.2.2 Protect Windows computers manually

You must use an administrator account on the computers that you want to protect.

1. At each computer that you want to protect, browse to the bootstrap location, find `setup.exe` and double-click it.
2. In the **Sophos Setup** dialog box, in the **User account details**, enter details of the Update Manager account, **SophosUpdateMgr**, that you created to access the share where Enterprise Console puts software updates. You did this in Update Manager account (page 10).

   Tip: You can also use any low-privilege account that can access the bootstrap location. Enterprise Console will apply an updating policy that includes the right user account details later.

Note: For information about command line parameters for the `setup.exe` file, see http://www.sophos.com/en-us/support/knowledgebase/12570.aspx.

15.2.3 Protect Macs

You must use an administrator account on the Macs that you want to protect.

1. At each Mac that you want to protect, browse to the bootstrap location, copy `Sophos Anti-Virus.mpkg` to the Mac OS X desktop and double-click it.

   A wizard guides you through installation.

2. Accept the default options. When prompted, enter the details of a user account that can install software on the Mac.

15.3 Protect Linux computers

For details of how to protect Linux computers (if your license permits this), see the *Enterprise Console startup guide for Linux, NetWare and UNIX*.

16 Set up encryption software on computers

Read this section if your license includes encryption and if you have installed Enterprise Console to manage encryption.

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.

To set up full disk encryption on computers you:

- Subscribe to encryption software.
- Prepare to install encryption software.
- Install encryption software automatically or, if necessary, manually.

Note: Full disk encryption can currently be installed only on Windows XP (32-bit), Windows Vista and Windows 7 computers.

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 to install encryption software (page 22).

16.1 Subscribe to encryption software

If you haven't already subscribed to and downloaded the encryption software using the **Download Security Software Wizard**, add the encryption software to your software subscription.

1. In Enterprise Console, on the **View** menu, click **Update Managers**.
2. In the **Software Subscriptions** pane, double-click the subscription you want to edit (for example, "Recommended").
3. Under **Encryption Products**, select the **Windows XP and above** check box, click in the **Version** box, and select the latest "Recommended" version (version 5.61 at the time of this release). Click **OK**.

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

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.

16.2 Prepare to install encryption software

Preparing computers for encryption involves the following tasks:

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

16.2.1 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 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.

16.2.2 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.
- 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/107081.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 disables the process again.

16.3 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 computers, 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 25).

16.4 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. In Enterprise Console, on the **View** menu, click **Bootstrap locations**.

   A list of locations is displayed. Make a note of the location for each operating system you want to protect.

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 25).

16.5 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.

17 Check the health of your network

To check the health of your network from Enterprise Console, do as follows.

1. On the menu bar, click the **Dashboard** icon (if the Dashboard is not already displayed).

   The Dashboard shows you how many computers:

   - Have detected threats.
   - Are out of date.
   - Do not comply with policies.

18 Troubleshooting

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

- Automatic installation is not possible on that operating system. Perform a manual installation. See Protect Macs (page 21). For other operating systems (if your license permits you to protect them), see the *Sophos Enterprise Console startup guide for Linux, NetWare and UNIX*.
- 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.
- You have tried to install full disk encryption on computers where the required software such as anti-virus has not yet been installed.

19 Get help with common tasks

This section tells you where you can find information on how to carry out common tasks.

SEC = Sophos Enterprise Console

Task	Document
Protect standalone computers	SEC 5.1 advanced startup guide: "Protecting standalone computers"
Configure Enterprise Console policies	Enterprise Console Help: "Configuring policies"
Deal with alerts	Enterprise Console Help: "Dealing with alerts and errors"
Clean up computers	Enterprise Console Help: "Cleaning up computers"
Generate SEC reports	Enterprise Console Help: "Generating reports"

20 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/.
- Open a ticket with our support team at https://secure2.sophos.com/support/contact-support/support-query.aspx.

21 Legal notices

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

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

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

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.]