SafeGuard Enterprise
Installation guide

Product version: 6
Document date: February 2012
Contents

1 About SafeGuard Enterprise.................................................................3
2 Getting started.................................................................................6
3 Setting up SafeGuard Enterprise Server........................................12
4 Setting up SafeGuard Enterprise Database....................................21
5 Setting up SafeGuard Management Center....................................30
6 Testing communication.................................................................42
7 Securing transport connections with SSL.......................................45
8 Registering and configuring SafeGuard Enterprise Server.............47
9 Setting up SafeGuard Enterprise on endpoints.............................51
10 Setting up SafeGuard Configuration Protection............................71
11 Setting up SafeGuard Enterprise Runtime.....................................77
12 Replicating the SafeGuard Enterprise Database............................79
13 About upgrading............................................................................84
14 About migrating.............................................................................90
15 About uninstallation.......................................................................100
16 Technical support.........................................................................103
17 Legal notices.................................................................................104
1 About SafeGuard Enterprise

SafeGuard Enterprise is a comprehensive, modular data security solution that uses a policy-based encryption strategy to provide reliable protection for information and information sharing on servers, PCs and mobile end devices.

The central administration is carried out with the SafeGuard Management Center. Security policies, keys and certificates, smartcards and tokens can be managed using a clearly laid out, role-based administration strategy. Detailed logs and report functions ensure that users and administrators always have an overview of all events.

On the user side, data encryption and protection against unauthorized access are the main security functions of SafeGuard Enterprise. SafeGuard Enterprise can be seamlessly integrated into the user’s normal environment and it is easy and intuitive to use. The SafeGuard specific authentication system, Power-on Authentication (POA), provides the necessary access protection and offers user-friendly support if credentials have to be recovered.

1.1 SafeGuard Enterprise components

This section provides an overview of the SafeGuard Enterprise components and explains how they interact.

One or several Microsoft SQL databases store information about the endpoints on the company network. The administrator, known in SafeGuard Enterprise as the Master Security Officer (MSO), uses the SafeGuard Management Center to manage the database contents and to create new security instructions (policies).

The endpoints read the policies from the database and report successful execution to the database. The communication between the database and the endpoints is done by Internet Information Services (IIS) based web server which has the SafeGuard Enterprise Server installed on it.
The table below describes the individual components:

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SafeGuard Enterprise Database(s) based on Microsoft SQL Server Database</td>
<td>The SafeGuard Enterprise Database(s) hold all relevant data such as keys/certificates, information about users &amp; computers, events and policy settings. The database(s) need to be accessed by the SafeGuard Enterprise Server and by one security officer only through the SafeGuard Management Center, usually the Master Security Officer. The SafeGuard Enterprise Database(s) can be generated and configured using a wizard or scripts.</td>
</tr>
<tr>
<td>SafeGuard Enterprise Server on IIS based web server</td>
<td>Microsoft Internet Information Services (IIS), .NET Framework 4 and ASP.NET 4 are required. The web server used for SafeGuard Enterprise must be based on Internet Information Services (IIS). We recommend that you use a dedicated IIS for SafeGuard Enterprise Server. The IIS may be clustered. SafeGuard Enterprise Server interfaces between the SafeGuard Enterprise Database and the SafeGuard Enterprise endpoint. Upon request, the SafeGuard Enterprise Server sends policy settings to the endpoint computers. It requires access to the database. It runs as an application on a Microsoft Internet Information Services (IIS) based web server.</td>
</tr>
<tr>
<td>SafeGuard Management Center on administrator computer</td>
<td>Central management tool for SafeGuard Enterprise protected endpoints, managing keys and certificates, users &amp; computers, and for creating SafeGuard Enterprise policies. The SafeGuard Management Center</td>
</tr>
<tr>
<td>Component</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>communicates with the SafeGuard Enterprise Database. .NET Framework 4 is required.</td>
</tr>
<tr>
<td>Directory Services (optional)</td>
<td>Import of an active directory. It holds the company's organizational structure with users and computers.</td>
</tr>
<tr>
<td>SafeGuard Enterprise encryption software on endpoint computers</td>
<td>Encryption software for secure authentication and data encryption on endpoints. SafeGuard Enterprise protected endpoints can either be connected to the SafeGuard Enterprise Server (managed) or not connected to a SafeGuard Enterprise Server at all (unmanaged). Managed endpoints receive their policies directly from the SafeGuard Enterprise Server. Unmanaged endpoints receive their policies inside configuration packages that can be deployed using third-party distribution mechanisms.</td>
</tr>
</tbody>
</table>
2 Getting started

This section explains how to prepare for your SafeGuard Enterprise installation successfully.

- First-time installation: The SGN Install Advisor simplifies the first time installation of the management components including default policies. To launch the SGN Install Advisor for new SafeGuard Enterprise installations, start SGNInstallAdvisor.bat from your product delivery. A wizard guides you through installation.

- Update installation: Follow the steps described in this guide.

Note: Our video tutorials is an ideal way to learn about SafeGuard Enterprise. They show how SafeGuard Enterprise is installed and how to use the SafeGuard Management Center. For further information, visit our website at http://www.sophos.com.

2.1 What are the key steps?

To install SafeGuard Enterprise follow these installation steps.

Note:

SafeGuard Enterprise for Windows does not support Apple hardware and cannot be installed on a Boot Camp environment.

You find all SafeGuard Enterprise components (.msi packages) in the product delivery.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Package/Tool</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Download the installers.</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Install .NET Framework 4 with ASP.NET 4.</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Set up Internet Information Services (IIS) for SafeGuard Enterprise.</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Install SafeGuard Enterprise Server.</td>
<td>SGNServer.msi</td>
</tr>
<tr>
<td>5</td>
<td>Configure Microsoft SQL Server database authentication for the SafeGuard Enterprise Master Security Officer.</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Generate the SafeGuard Enterprise Database(s) with a script.</td>
<td>Database scripts in product delivery, in Tools directory</td>
</tr>
<tr>
<td>Step</td>
<td>Description</td>
<td>Package/Tool</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
<td>--------------</td>
</tr>
<tr>
<td>7</td>
<td>Install the management console SafeGuard Management Center for central management of users, computers, policies, keys and reports.</td>
<td>SGNManagementCenter.msi</td>
</tr>
<tr>
<td>8</td>
<td>Configure SafeGuard Management Center: database and database server connections, certificates, Master Security Officer credentials.</td>
<td>SafeGuard Management Center Configuration Wizard</td>
</tr>
<tr>
<td>9</td>
<td>Register and configure SafeGuard Enterprise Server: Create server configuration package and deploy it on the web server.</td>
<td>SafeGuard Management Center Configuration Package Tool</td>
</tr>
<tr>
<td>10</td>
<td>Create the organizational structure from Active Directory or manually.</td>
<td>SafeGuard Management Center</td>
</tr>
<tr>
<td>11</td>
<td>Prepare endpoints for encryption.</td>
<td>SGxClientPreinstall.msi</td>
</tr>
<tr>
<td>12</td>
<td>Create initial configuration package for endpoint configuration.</td>
<td>SafeGuard Management Center Configuration Package Tool</td>
</tr>
<tr>
<td>13</td>
<td>Install encryption software and initial configuration package on endpoints.</td>
<td>For available packages, see About managed and unmanaged endpoints (page 51).</td>
</tr>
</tbody>
</table>

### 2.2 What are the key steps for runtime systems?

A runtime system enables starting the computer from a secondary boot volume when multiple operating systems are installed and to access these volumes when they are encrypted by a SafeGuard Enterprise installation on the primary volume.

This solution is available for both managed and unmanaged endpoints protected by SafeGuard Enterprise.

**Note:**

SafeGuard Enterprise for Windows does not support Apple hardware and cannot be installed on a Boot Camp environment.

To install SafeGuard Enterprise Client on multiple operating systems, follow these installation steps:
2.3 Check the system requirements

Before you deploy SafeGuard Enterprise, check the system requirements.

For hardware and software requirements, service packs and disk space required during installation as well as for effective operation, see the system requirements section of the current release notes version at http://www.sophos.com/support/knowledgebase/article/114138.html.

2.4 Download installers

1. Using the web address and download credentials provided by your system administrator, go to the Sophos website and download the installers.
2. Store them in a location where you can access them for installation.

2.5 Language settings

The language settings for the setup wizards and the different SafeGuard Enterprise components are as follows:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Package/Tool</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Download the installers.</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Set up the runtime system on the secondary boot volume of the endpoint.</td>
<td>SGNClientRuntime.msi, SGNClientRuntime_x64.msi</td>
</tr>
<tr>
<td>3</td>
<td>Provide endpoints with necessary requirements for successful installation of the current encryption software (mandatory).</td>
<td>SGxClientPreinstall.msi</td>
</tr>
<tr>
<td>4</td>
<td>Install the SafeGuard Device Protection package on the primary boot volume of the endpoint.</td>
<td>SGNClient.msi, SGNClient_x64.msi</td>
</tr>
<tr>
<td>5</td>
<td>Create the initial configuration package for endpoint configuration.</td>
<td>SafeGuard Management Center Configuration Package Tool</td>
</tr>
</tbody>
</table>
Wizards

The installation and configuration wizards of the different installation packages use the language setting of the operating system. If the operating system language is not available for these wizards, they default to English automatically.

SafeGuard Management Center

You can set the language of the SafeGuard Management Center as follows:

- In SafeGuard Management Center, click menu Tools > Options > General. Select Use user defined language and select an available language. English, German, French and Japanese are provided.
- Restart SafeGuard Management Center. It is displayed in the selected language.

Sophos SafeGuard on endpoints

You set the language of Sophos SafeGuard on endpoints in a policy of the type General in the SafeGuard Policy Editor, setting Customization > Language used on client:

- If the language of the operating system is selected, Sophos SafeGuard uses the language setting of the operating system. If the operating system language is not available in Sophos SafeGuard, the Sophos SafeGuard language defaults to English.
- If one of the available languages is selected, Sophos SafeGuard functions are displayed in the selected language on the endpoint.

2.6 Compatibility with other SafeGuard products

This section describes the compatibility of SafeGuard Enterprise 6 with other SafeGuard products.

2.6.1 Compatibility with SafeGuard LAN Crypt

- SafeGuard LAN Crypt 3.7x and the SafeGuard Enterprise 6 component File Share cannot coexist on the same computer. If SafeGuard LAN Crypt is already installed on the computer, the File Share component is not available for selection when the SafeGuard Enterprise encryption software is installed on the computer.

- Apart from the above exception, SafeGuard LAN Crypt 3.7x and SafeGuard Enterprise 6 can coexist on the same computer and are compatible.

Note: If SafeGuard Enterprise 6 is installed on-top of SafeGuard LAN Crypt, the installation program will complain that the component SGLC Profile Loader is already in use. This message is caused by the fact that SafeGuard LAN Crypt and SafeGuard Enterprise share common components and can therefore be ignored. The affected components will be updated upon restart.
SafeGuard LAN Crypt below 3.7x and SafeGuard Enterprise 6 cannot coexist on the same computer.

If you try to install SafeGuard Enterprise 6 on a computer where SafeGuard LAN Crypt 3.6x or below is already installed, the setup is cancelled and an error message is displayed.

SafeGuard LAN Crypt 3.7x and SafeGuard Enterprise below 5.40 cannot coexist on one computer.

If you try to install SafeGuard LAN Crypt 3.7x on a computer with an already installed SafeGuard Enterprise below 5.40, the setup is cancelled and a respective error message is displayed.

2.6.2 Compatibility with SafeGuard PrivateCrypto and SafeGuard PrivateDisk

SafeGuard Enterprise 6 and the standalone products SafeGuard PrivateCrypto (version 2.30 or above) and SafeGuard PrivateDisk (version 2.30 or above), can coexist on the same computer.

Both SafeGuard PrivateCrypto and SafeGuard PrivateDisk can then share the SafeGuard Enterprise key management.

2.6.3 Compatibility with SafeGuard RemovableMedia

The SafeGuard Data Exchange component and SafeGuard RemovableMedia cannot coexist on the same computer. Before you install SafeGuard Data Exchange on an endpoint computer, check if SafeGuard RemovableMedia is already installed. In this case, make sure that you uninstall SafeGuard RemovableMedia before you install SafeGuard Data Exchange.

Local keys created with SafeGuard RemovableMedia below version 1.20 before switching to SafeGuard Data Exchange can be used on the SafeGuard Enterprise protected computer. But they are not transferred to the SafeGuard Enterprise Database automatically.

2.6.4 Compatibility with SafeGuard Easy 4.x

SafeGuard Easy 4.x and SafeGuard Enterprise 6 can be installed on the same computer as long as the SafeGuard Enterprise Device Protection module is not installed. Since both products install their own GINA (graphical identification and authentication), SafeGuard Enterprise can only be operated successfully if its own GINA is used. To assure proper configuration, SafeGuard Easy 4.x has to be installed without GINA support (use the GINASYS=0 option) before the relevant SafeGuard Enterprise module is installed. If SafeGuard Easy 4.x has been installed with GINA support, it has to be removed before installing SafeGuard Enterprise.

Note: When SafeGuard Easy 4.x and SafeGuard file-based encryption module are installed on one computer, the SafeGuard Easy GINA mechanisms (especially Windows Secure Autologon - SAL) do no longer work. As a workaround, SafeGuard Easy 4.x must be installed first and both products should only be uninstalled together (without a restart) to avoid GINA conflicts.
2.7 General Restrictions

Note the following general restrictions for SafeGuard Enterprise on endpoints:

- SafeGuard Enterprise for Windows does not support Apple hardware and cannot be installed in a Boot Camp environment.

- If using Intel Advanced Host Controller Interface (AHCI) on the endpoint, the boot hard disk must be in Slot 0 or Slot 1. You can insert up to 32 hard disks. SafeGuard Enterprise only runs on the first two slot numbers.

- Volume-based encryption for volumes that are located on Dynamic disks and on GUID partition table disks, (GPT), are not supported. In such cases, installations are terminated. If such disks are found on the endpoint, they are not supported.

- The SafeGuard Device Protection module does not support systems that are equipped with hard drives attached through a SCSI bus.

- **Fast User switching** is not supported.

- Operating SafeGuard Enterprise in a terminal server environment is not supported.
3 Setting up SafeGuard Enterprise Server

The SafeGuard Enterprise Server acts as the interface to the SafeGuard Enterprise Clients. Like the SafeGuard Management Center, it accesses the database. It runs as an application on a web server based on Microsoft Internet Information Services (IIS).

SafeGuard Enterprise Server also includes the Task Scheduler to create and schedule periodic tasks that can be based on scripts. The tasks are automatically run on the SafeGuard Enterprise Server. You find the scripts in the SafeGuard Enterprise product delivery. For further information, see the SafeGuard Enterprise Administrator help.

We recommend that you install SafeGuard Enterprise Server on a dedicated IIS. This improves the performance. Moreover, it ensures that other applications cannot conflict with SafeGuard Enterprise, for instance concerning the version of ASP.NET to be used.

This chapter describes how to install SafeGuard Enterprise Server including Task Scheduler on IIS. You first have to install and configure Microsoft Internet Information Services (IIS).

3.1 Prerequisites

The following prerequisites must be met:

- You need Windows administrator rights.
- Microsoft Internet Information Services (IIS) must be available.
- If you use SSL transport encryption between SafeGuard Enterprise Server and SafeGuard Enterprise Client you have to set up the IIS for it in advance, see Securing transport connections with SSL (page 45).
- .NET Framework 4 and ASP.NET 4 must be installed. It is provided in the SafeGuard Enterprise product delivery.

IIS is available free of charge. You find the program on your Windows DVD, for example, or on the Microsoft web site.

A certificate must be issued and the IIS server configured to use SSL and point to the certificate.

The server name specified when configuring the SafeGuard Enterprise Server must be the same as the one specified in the SSL certificate. Otherwise client and server cannot communicate. For each SafeGuard Enterprise Server a separate certificate is needed.

If you use Network Load Balancer, make sure that the port range includes the SSL port.

If you use SSL transport encryption between SafeGuard Enterprise Server and SafeGuard Enterprise Client you have to set up the IIS for it in advance, see Securing transport connections with SSL (page 45).

A certificate must be issued and the IIS server configured to use SSL and point to the certificate.

The server name specified when configuring the SafeGuard Enterprise Server must be the same as the one specified in the SSL certificate. Otherwise client and server cannot communicate. For each SafeGuard Enterprise Server a separate certificate is needed.

If you use Network Load Balancer, make sure that the port range includes the SSL port.

...
3.2 Installing and configuring Microsoft Internet Information Services (IIS)

The section explains how to prepare Microsoft Internet Information Services (IIS) to run with SafeGuard Enterprise Server.

Settings vary depending on your version of IIS and operating system. Specific setup is mentioned for the following:

- IIS 6 on Microsoft Windows Server 2003
- IIS 7 on Microsoft Windows Server 2008
- IIS 7.5 on Microsoft Windows Server 2008 R2

3.2.1 Install and configure IIS 6 on Microsoft Windows Server 2003

IIS is available free of charge. You find the program on your Windows DVD, for example, or on the Microsoft web site.

1. On the Start menu, click Control Panel, and select Add/Remove Windows Components.
2. On the Components list box, click Application Server.
3. In Application Server, click Details and select Internet Information Services (IIS).
4. Additionally, select ASP.NET.
5. Click OK.
   
IIS 6 is installed with a default configuration for hosting ASP.NET.

6. Check that the web page is displayed properly using http://<server name>. For further information, see: [http://support.microsoft.com](http://support.microsoft.com).

3.2.1.1 Check .NET Framework installation and registration

.NET Framework 4 is required. You find the program in the SafeGuard Enterprise product delivery.

To check whether it is installed correctly on IIS 6 or IIS 7:

1. From the Start menu, select Run....
2. Enter the following command: Appwiz.cpl. All programs installed on the computer are displayed.
3. Check if .NET Framework Version 4 is displayed. If it is not displayed, install this version. Follow the steps in the installation wizard and confirm all defaults.
4. To test that the installation is correctly registered, go to C:\Windows\Microsoft.NET\Framework. Each installed version must be visible as a separate folder showing the version as folder name, for example "v 4.0".
3.2.1.2 Check ASP.NET registration on IIS 6

ASP.NET Version 4 is required.

To check that the correct version of ASP.NET is installed and registered on IIS 6:

1. Open Internet Information Services Manager on the IIS server.
2. On the navigation area on the right, under Internet Information Services, click SGNSRV (local computer), then click Web Sites.
3. Under Web Sites, right-click Default Web Sites, and click Properties. Select the ASP.NET tab. Version 4.0 should be displayed under ASP.NET Version.
   ■ If this version is displayed, select it. Click Apply, and then OK
   ■ If it is not displayed, enter the command aspnet_regiis.exe -i at the command prompt to ensure that ASP Services Version 4.0 is installed.
4. To check that the correct version is installed, enter aspnet_regiis.exe -lv at the command prompt.
   Version 4.0 should be displayed for ASP.NET.

3.2.1.3 Configure ASP.NET for IIS 6 on Windows Server 2003 64 bit

When you operate IIS 6 and want to install SafeGuard Enterprise Server on Windows Server 2003 64 bit, carry out the following additional steps:

1. Enter the following command: cscript %SYSTEMDRIVE%\inetpub\adminscripts\adsutil.vbs SET W3SVC/AppPools/Enable32bitAppOnWin64 1
2. Register the required ASP.NET version with the following command:
   %SYSTEMROOT%\Microsoft.NET\Framework\v4.0\aspnet_regiis.exe -i
3. To activate the 32 bit version of ASP.Net 4.0, open Internet Information Services Manager on the IIS server.
4. In IIS Manager, click Server (local computer), and then click Web Service Extensions.
5. Right-click ASP.NET v4.0 (32 bit), click Properties and set the status to Allowed.
6. Click Apply, and then OK.

3.2.1.4 Specific SafeGuard user account for IIS 6

During IIS 6 setup, a user is created to authenticate anonymously from the client to the SGNSRV site on the IIS.

When SafeGuard Enterprise Server is installed on the IIS server, a customized user IUSR_SafeGuard is created. With IUSR_SafeGuard, you are still able to use anonymous access to the SGNSRV site in case the IIS host name is changed.

With IIS 6, the standard user name is IUSR_MACHINENAME. If the IIS host name is renamed after installation, it will not match the standard user name anymore and anonymous access will fail. With IUSR_SafeGuard, you always have a valid logon name even if the IIS host name is renamed.
3.2.1.5 Enable memory recycling on IIS 6

When using IIS 6, we recommend that you enable Recycle worker processes.

1. Open Internet Information Services Manager on the IIS server.
2. On IIS Manager, click Server (local computer).
3. Right-click Application Pools, and then click Properties.
4. Under Memory recycling, set the values as follows:
   a) Maximum virtual memory = 500 MB
   b) Maximum used memory = 192 MB
5. Click Apply, and then click OK.

Memory recycling is now enabled on IIS 6.

Note: Only one worker process is allowed. Only when using SSL, more than one worker process is allowed.

3.2.2 Install and configure IIS 7/7.5 on Microsoft Windows Server 2008/2008 R2

The description applies to the following installations:
- IIS 7 on Microsoft Windows Server 2008
- IIS 7.5 on Microsoft Windows Server 2008 R2

IIS is available free of charge. You find the program on your Windows DVD, for example, or on the Microsoft web site.

1. On the Start menu, click All Programs, Administrative Tools and then Server Manager.
2. In the Server Manager, click Roles and then click Add Roles.
3. In the Add Roles Wizard, on the Before you Begin page, verify the following:
   - The administrator account has a strong password.
   - The network settings, for example IP addresses are configured.
   - The latest security updates from Windows Update are installed.
4. Select Select Roles on the right, and then select Web server (IIS). On the subsequent page, click Add Required Features. Web Server (IIS) is listed in the navigation area of the Add Roles Wizard.
5. Click Web Server (IIS), then click Roles Services. Keep the default roles services.
6. On the right, additionally select the following: ASP.NET, which also selects the necessary sub-role services.
7. Select IIS Management Scripts and Tools that is needed for correct IIS 7 configuration.
8. Click **Next**, then **Install** and then **Close**, 
IIS is installed with a default configuration for hosting ASP.NET.

9. Check that the web page is displayed properly using http://<server name>. For further information, see: http://support.microsoft.com.

### 3.2.2.1 Check .NET Framework registration on IIS 7

.NET Framework version 4 is required.

1. To check that .NET Framework is installed and registered with the correct version, see **Check .NET Framework installation and registration** (page 13).

### 3.2.2.2 Check ASP.NET registration on IIS 7

ASP.NET Version 4 is required.

1. To check that ASP.NET is installed and registered with the correct version, enter the command `aspnet_regiis.exe -lv` at the command prompt.

   Version 4.0 should be displayed for ASP.NET.

### 3.3 Hardening the IIS server

To enhance security in your company's intranet it is recommended that you protect each IIS server and the applications that run on it by specific security settings so that the IIS server is "hardened".

This chapter describes how to set up the IIS server for use with SafeGuard Enterprise Server to meet the hardening recommendations of Microsoft. If further settings are enabled which are not recommended by Microsoft or as explained in this chapter, this might lead to unwelcome results.

**Note:**


The explanations in this chapter are based on the following sample configuration:

- **Server 1:**
  - Microsoft Windows Server 2003 SP1
  - SafeGuard Enterprise Server latest version
  - SafeGuard Management Center latest version
  - Microsoft SQL Server 2005 Express
  - IIS with minimal components

- **Server 2:**
  - Microsoft Windows Server 2003 SP1
SafeGuard Enterprise Server latest version
Microsoft SQL Server 2005 Express
IIS with minimal components

Server 2 only runs the SafeGuard Enterprise Server (IIS server). If Server 2 is additionally in use, the services enabled for Server 1 are automatically disabled

■ Client:
  SafeGuard Enterprise Client
  SafeGuard Management Center latest version

### 3.3.1 Install only necessary IIS components

Make sure that only essential and necessary IIS components are installed as this reduces the chance that the IIS server might be attacked. Disable all unnecessary settings.

The minimum component set of the IIS server to run with SafeGuard Enterprise Server is:

■ Common Files
■ Internet Information Services (IIS) Manager
■ World Wide Web Services

### 3.3.2 Enable only essential Web Service Extensions

Make sure that only essential Web Service Extensions are enabled, as this reduces the chance that the IIS server might be attacked. Disable all unnecessary settings.

The required settings for the IIS server to run with SafeGuard Enterprise Server are:

Web Service Extension:

■ ASP.NET v.1.1.4322 and 2.0.50727 **Prohibited**
■ ASP.NET 4.0 **Allowed**

### 3.3.3 Place web site content on a dedicated disk volume

IIS stores the files for its default Web site in the following folder:

%systemroot%\inetpub\wwwroot

%systemroot% is the drive on which the Windows Server 2003 operating system is installed.

Move all files and folders that make up Web sites and applications on dedicated disk volumes that are separate from the operating system. This helps to prevent attacks in which an attacker sends requests for a file that is located outside the directory structure of an IIS server.
For the sample configuration these may be moved as follows:

- IIS web files to E:\inetpub
- SafeGuard Enterprise Server Web files to F:\mycompany.web

*Note:*
After moving the Web files you need to update the path information in the IIS Manager accordingly.

### 3.3.4 Set NTFS permissions

Computers that run Windows Server 2003 with SP1 examine NTFS file system permissions to determine the types of access a user or a process has on a specific file or folder. You should assign NTFS permissions to allow or deny Web site access to specific users on the IIS server.

For the sample configuration the minimal NTFS permissions are as follows:

<table>
<thead>
<tr>
<th>User/Folder</th>
<th>NTFS permissions for E:\inetpub</th>
<th>NTFS permissions for F:\mycompany.web</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrators</td>
<td>full control</td>
<td>full control</td>
</tr>
<tr>
<td>System</td>
<td>full control</td>
<td>full control</td>
</tr>
<tr>
<td>Users</td>
<td>execute</td>
<td>execute</td>
</tr>
</tbody>
</table>

You may set a different account or group for "Users" as long as this is provided on the IIS server. When doing so, you need to update the account IUSR_SERVERNAME on the IIS server accordingly.

The NTFS permissions for file types are as follows:

<table>
<thead>
<tr>
<th>File type</th>
<th>Recommended NTFS permissions</th>
</tr>
</thead>
</table>
| CGI files (.exe, .dll, .cmd, .pl) | Administrators (full control)  
System (full control)  
Everyone/User (execute) |
| Script files (.asp) | Administrators (full control)  
System (full control)  
Everyone/User (execute) |
| Include files (.inc, .shtm, .shtml) | Administrators (full control)  
System (full control)  
Everyone/User (execute) |
### 3.3.5 Disable Integrated Windows Authentication

We recommend that you disable Integrated Windows Authentication in IIS to avoid sending unnecessary authentication information.

1. In IIS Manager, double-click the local computer; right-click the **Web Sites** folder, and then click **Properties**.
2. Click the **Directory Security** tab, and then, in the **Authentication and access control** section, click **Edit**.
3. In the **Authenticated access** section, clear **Windows Integrated Authentication**.
4. Click **OK** twice.

### 3.3.6 Settings for Application Pool "DefaultAppPool"

Settings depend on where the IIS server resides:

- If the SQL server resides on the same computer as the IIS server, set the built-in Local Service user account for "DefaultAppPool". In the sample configuration this applies to Server 1.
- If the SQL server resides on a different computer than the IIS server, set the built-in Network Service user account for "DefaultAppPool". In the sample configuration this applies to Server 2. Otherwise synchronization with the client fails.

### 3.4 Install SafeGuard Enterprise Server

After the IIS is configured, you can install SafeGuard Enterprise Server on the IIS server. You find the install package **SGNServer.msi** in the product delivery.

1. On the server where you want to install SafeGuard Enterprise Server, double-click **SGNServer.msi**. A wizard guides you through the necessary steps.
2. Accept the defaults on all subsequent dialogs. Task Scheduler is automatically installed with an installation of type **Complete**.

SafeGuard Enterprise Server including Task Scheduler is installed.

**Note:**

<table>
<thead>
<tr>
<th>File type</th>
<th>Recommended NTFS permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Static content (.txt, .gif, .jpg, .htm, .html)</td>
<td>Administrators (full control)</td>
</tr>
<tr>
<td></td>
<td>System (full control)</td>
</tr>
<tr>
<td></td>
<td>Everyone/User (read-only)</td>
</tr>
</tbody>
</table>
To enhance performance, the connection of logged events is deactivated for the SafeGuard Enterprise Database by default after installation of SafeGuard Enterprise Server. However, without the connection of logged events no integrity protection is provided for logged events. The connection of logged events strings together all entries in the event table so that if an entry is removed this is evident and can be verified with an integrity check. To make use of integrity protection, you need to set the connection of logged events manually. For further information, see the SafeGuard Enterprise Administrator help, chapter Reports.
4 Setting up SafeGuard Enterprise Database

SafeGuard Enterprise stores all relevant data such as keys/certificates, information about users and computers, events and policy settings in a database. The SafeGuard Enterprise Database is based on Microsoft SQL Server.

Check the list of currently supported SQL Server types in the system requirements section of the current release notes version at http://www.sophos.com/support/knowledgebase/article/112776.html.

You can set up the database either automatically during first-time configuration in the SafeGuard Management Center or manually using the SQL scripts provided in your product delivery. Depending on your enterprise environment, check which method to choose. For further information, see Database access rights (page 22).

To enhance performance, the SafeGuard Enterprise Database may be replicated to several SQL servers. To set up database replication, see Replicating the SafeGuard Enterprise Database (page 79).

Multiple SafeGuard Enterprise Databases can be created and maintained for different tenants such as different company locations, organizational units or domains (multi-tenancy). To configure multi-tenancy, see Multi Tenancy configurations (page 32).

Note:

We recommend that you operate a permanent online backup for the database. Back up your database regularly to protect keys, company certificates and user-computer assignments. Recommended backup cycles are, for example: after the data is first imported, after major changes or at regular intervals, for example every week or every day.

4.1 Database authentication

To access the SafeGuard Enterprise Database, the SafeGuard Management Center’s first security officer must be authenticated at the SQL Server. This can be done in the following ways:

- Windows authentication: promote an existing Windows user to SQL user
- SQL authentication: create an SQL user account

Find out from your SQL administrator which authentication method is intended for you, as a security officer. You need this information before generating the database and before first-time configuration in the SafeGuard Management Center Configuration Wizard.

Use SQL authentication for computers that are not part of a domain, otherwise use Windows authentication. If you use SQL authentication, we highly recommend that you secure the connection to and from the database server with SSL. For further information, see Set up SSL (page 45).
4.1.1 Database access rights

SafeGuard Enterprise is set up in such a way that, to work with the SQL database, it only needs a single user account with minimum access rights for the database. This user account is used by the SafeGuard Management Center and is only issued to the first SafeGuard Management Center security officer. This guarantees the connection to the SafeGuard Enterprise Database. While SafeGuard Enterprise is running, a single SafeGuard Management Center security officer only needs read/write permission for the SafeGuard Management Center Database.

The SafeGuard Enterprise Database can either be created manually or automatically during first-time configuration in the SafeGuard Management Center. If it is created automatically, extended access rights for the SQL database (db_creator) are needed for the first SafeGuard Management Security officer. However, these rights can be revoked afterwards by the SQL administrator until the next install/update.

If extending permissions during SafeGuard Management Center configuration is undesirable, the SQL administrator can generate the SafeGuard Enterprise Database with a script. The two scripts included in the product delivery, CreateDatabase.sql and CreateTables.sql, can be run for this purpose.

The following table shows the necessary SQL permissions for Microsoft SQL Server.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Create database</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server</td>
<td>db_creator</td>
<td>db_creator</td>
</tr>
<tr>
<td>Master database</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>SafeGuard Enterprise Database</td>
<td>db_ownerpublic (default)</td>
<td>db_ownerpublic (default)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Master database</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>SafeGuard Enterprise Database</td>
<td>db_datareaderdd</td>
<td>db_datareader</td>
</tr>
<tr>
<td></td>
<td>b_datawriter</td>
<td>db_datawriter</td>
</tr>
<tr>
<td></td>
<td>public (default)</td>
<td>public (default)</td>
</tr>
</tbody>
</table>

4.1.2 Configure a Windows account for SQL server logon

The description of the individual configuration steps below is aimed at SQL administrators and relates to Microsoft Windows Server 2008 and Microsoft SQL Server 2008 Standard or Express

As an SQL administrator, you need the right to create user accounts.

1. Open SQL Server Management Studio. Log on to the SQL Server with your credentials.
2. Open the **Object Explorer**, right-click **Security**, point to **New** and then click **Logins**.
3. In **Login - New** on the **General** page, select **Windows authentication**.
4. Click **Search**. Find the respective Windows user name and click **OK**. The user name is displayed as **Login name**.
5. In **Default Database**, if a script has not been used to create a SafeGuard Enterprise database yet, select **Master**.
6. Click **OK**.
7. To create the database automatically during SafeGuard Management Center first-time configuration, you have to change the access rights as follows: In **Login - New** on the **General** page, assign the access rights/roles by clicking **Server Roles** on the left. Select **dbcreator**. Once SafeGuard Enterprise has been installed, the database role can be reset to **dbowner**.

### 4.1.3 Create an SQL account for SQL server logon

As an SQL administrator, you need the right to create an SQL user account.

1. Open SQL Server Management Studio. Log on to the SQL Server with your credentials.
2. Open the **Object Explorer**, right-click **Security**, point to **New** and then click **Logins**.
3. In **Login - New** on the **General** page, select **SQL Server authentication**.
4. On the **General** page, in **Login name**, do the following:
   a) Enter the name of the new user, for example SGN SQLSERVICE.
   b) Enter and confirm a password for the account.
   c) Clear **Enforce password policy**.
   d) In **Default Database**, if a script has not been used to create a SafeGuard Enterprise database yet, select **Master**. Click **OK**.

Take a note of the authentication method and the credentials. You have to inform the SafeGuard Management Center security officer about them.
5. To create the database automatically during SafeGuard Management Center first-time configuration, you have to change the access rights as follows: In **Login - New** on the **General** page, assign the access rights/roles by clicking **Server Roles** on the left. Select **dbcreator**. Once SafeGuard Enterprise has been installed, the database role can be reset to **dbowner**.

![Server Roles](image)

The SQL user account and the access rights are now set up for the SafeGuard Enterprise security officer.

### 4.2 Generating the SafeGuard Enterprise Database

After setting up the user account for the SQL server logon you need to generate the SafeGuard Enterprise Database. There are two ways to do so:

- **Using SafeGuard Management Center Configuration Wizard**

  As a security officer, you can easily create the SafeGuard Enterprise Database during first-time configuration in the SafeGuard Management Center. The SafeGuard Management Center Configuration Wizard takes you through the basic configuration which also includes database creation. To do so, carry on with installing and configuring SafeGuard Management Center, see **Setting up SafeGuard Management Center** (page 30), and then continue with changing the relevant access rights, see **Change access rights for the SafeGuard Enterprise Database** (page 27).

- **Using SQL scripts provided in the product delivery**

  This procedure is often preferred if extended SQL permissions during SafeGuard Management Center Configuration is not desirable.

  It depends on your enterprise environment which method should be applied. It is best to be clarified between SQL administrator and SafeGuard Enterprise security officer.
4.2.1 Prerequisites

The following prerequisites must be met:

- Microsoft SQL Server must already be installed and configured. Microsoft SQL Express Edition is suitable for use in smaller companies, as there are no license fees.
- For performance reasons Microsoft SQL Server should not be installed on the computer on which SafeGuard Enterprise Server is installed.
- Database authentication methods and database access rights should be clarified.

4.2.2 Generate SafeGuard Enterprise Database with a script

If you want to create the SafeGuard Enterprise Database automatically during SafeGuard Management Center configuration, you can skip this step. If extended SQL permissions during SafeGuard Management Center configuration is not desirable, carry out this step. Two database scripts are provided in the product delivery (Tools folder) for this purpose:

- CreateDatabase.sql
- CreateTables.sql

The description of the steps below is aimed at SQL administrators and relates to Microsoft SQL Server 2008 Standard Edition.

As SQL administrator, you need to have the right to create a database.

1. Copy the scripts CreateDatabase.sql and CreateTables.sql from the SafeGuard Enterprise product delivery to the SQL server.
2. Double-click CreateDatabase.sql script. Microsoft SQL Server Management Studio is launched.
3. Log on to the SQL Server with your credentials.
4. Check that the two target paths at the beginning of the script, under FILENAME (MDF, LDF), exist on the local hard drive. Correct them if necessary.
5. Click Execute from the Toolbar to generate the database. You have created the database SafeGuard. Next use the CreateTables.sql script in the product delivery to generate the tables.
6. Double-click CreateTables.sql. A further pane is opened in Microsoft SQL Server Management Studio.
7. At the top of the script, enter use SafeGuard to select the SafeGuard Enterprise Database in which the tables are to be created.
8. Click Execute from the Toolbar to generate the table.

The SafeGuard Enterprise Database and the associated tables have been created.
4.3 Change access rights for the SafeGuard Enterprise Database

When the SafeGuard Enterprise Database has been created, either by script or in SafeGuard Management Center, access permissions can be changed back. Since it is possible to assign different roles and permissions to a user on a database, only the minimum rights are required for connecting to the SafeGuard Enterprise Database.

1. Open the SQL Server Management Studio. Log on to the SQL Server with your credentials.
2. Open the Object Explorer, right-click Security, and then click Logins.
3. Right-click the respective user name and click Properties.
4. Select User Mapping on the left. Under Users mapped to this login, select the database SafeGuard.
5. Under Database role membership for set the minimum access rights to use the SafeGuard Enterprise Database: select db_datareader, db_datawriter and public.
6. Click OK.

4.4 Check SQL Services, named pipes and TCP/IP settings

The description relates to Microsoft Windows Server 2008 (R2) and Microsoft SQL Server 2008 Standard or Express Edition.

1. Open SQL Server Configuration Manager.
2. From the navigation tree on the left, select SQL Server Services.
3. Check that the State of SQL Server and SQL Server Browser is Running and the Start mode is set to Automatic.
4. From the navigation tree on the left, select SQL Server Network Configuration and select the current instance.
5. Right-click the protocol Named Pipes and click Enabled.
6. Right-click the protocol TCP/IP and click Enabled.
7. Additionally, right-click the protocol TCP/IP and click Properties. In the IP Addresses tab, under IPAll, leave TCP Dynamic Ports blank. Set TCP Port to 1433.
8. Restart the SQL Services.

4.5 Create Windows Firewall rule on Windows Server 2008 (R2)

The description relates to Microsoft Windows Server 2008 (R2) with Microsoft SQL Server 2008 Standard or Express Edition. When you use this configuration, carry out the steps below to ensure that a connection between SafeGuard Enterprise Database and SafeGuard Management Center can be established.

1. On the computer hosting the SQL Server instance, click Start, select Administrative Tools and then click Windows Firewall with Advanced Security.
2. From the navigation tree on the left, select Inbound Rules.
3. Click Action from the menu bar, and then click New Rule. The New Inbound Rule Wizard is launched.
4. On the Rule Type page, select Custom and click Next.
5. On the Program page, select the program and services this rule should apply to, and then click Next.
7. On the Scope page, you can specify that the rule applies only to network traffic to or from the IP addresses entered on this page. Configure as appropriate, and then click Next.
8. On the Action page, select Allow the connection, and click Next.
9. On the Profile page, select where to apply the rule, and click Next.
10. On the Name page, type a name and description for your rule, and click Finish.

4.6 Configure Windows authentication for SQL server logon


To enable communication between SafeGuard Enterprise Server and SafeGuard Enterprise Database when using Windows authentication, the user must be made a member of Active Directory groups. Local file permissions must be adjusted, and the SQL user account must be populated to the Application Pool of the IIS.

1. Select Start and then Run. Enter dsa.msc. Open the Active Directory Users and Computers snap-in.
2. In the navigation tree on the left, expand the domain tree and select BuiltIn.
3. Add the respective Windows user to the following groups: IIS_IUSRS, Performance Log Users, Performance Monitor Users.
4. Exit the snap-in.
5. On the local file system, in Windows Explorer, right-click the C:\Windows\Temp folder and select Security.
6. In Security, click Add, and under Object name, enter the respective Windows user name. Click OK.
7. In Security, under Permissions, select Special permissions and then set the following permissions in the Object dialog to Allow: List folders / read data, Create files / write data, Delete.
8. Click OK and exit Windows Explorer.
9. Open Internet Information Services Manager.
10. In the Connections pane on the left, select Application Pools of the relevant server node.
11. From the Application Pools list on the right, select SGNSRV-Pool.
12. In the Actions pane on the left, select Advanced Settings.
13. In Advanced Settings, under Process Model, for the Identity property, click the ... button.
15. In Set Credentials, type the relevant Windows user name in the following form:
   Domain\<Windows user name>. Type and confirm the respective Windows password
   and then click OK.
16. In the Connections pane on the left, select the relevant server node and click Restart from the
    Actions pane.
17. In the Connections pane on the left, under the relevant server node, under Sites, Default Web
    Sites, select SGNSRV.
18. From the Actions pane on the right, select Authentication.
20. For Anonymous user identity, select Specific user and check that the user name is IUSR.
    Correct it, if necessary.
21. Click OK.

Additional configuration when using a Windows account for SQL server logon is now completed.
5 Setting up SafeGuard Management Center

This section describes how to install and configure SafeGuard Management Center.

SafeGuard Management Center is the central administrative tool for SafeGuard Enterprise. You install it on the administrator computers that you intend to use for managing SafeGuard Enterprise. SafeGuard Management Center can be installed on any computer on the network from which the SafeGuard Enterprise Databases can be accessed.

SafeGuard Management Center provides for serving multiple databases by way of tenant-specific database configurations (Multi Tenancy). You are able to set up and maintain different SafeGuard Enterprise Databases for different tenants such as company locations, organizational units or domains. To ease management efforts, these database configurations can also be exported to and imported from files.

The SafeGuard Management Center does not need to be necessarily installed on one computer only. It can be installed on any computer on the network from which the databases can be accessed.

5.1 Prerequisites

The following prerequisites must be met:

- Make sure that you have Windows administrator rights.
- .NET Framework 4 must be installed. It is provided in the SafeGuard Enterprise product delivery.
- If you want to create a new SafeGuard Enterprise Database during SafeGuard Management Center configuration, you need the necessary SQL access rights and credentials, see Database access rights (page 22).

5.2 Install SafeGuard Management Center

1. Start SGNManagementCenter.msi from the install folder of your product delivery. A wizard guides you through the necessary steps.
2. Accept the defaults in the subsequent dialogs except as follows: On the Installation type page, do one of the following:
   - For SafeGuard Management Center to support one database only, select Typical.
   - For SafeGuard Management Center to support multiple databases (Multi Tenancy), select Complete. For further information, see Multi Tenancy configurations (page 32).

SafeGuard Management Center is installed. If necessary, restart your computer. Next you carry out initial configuration in SafeGuard Management Center.
5.3 Displaying SafeGuard Management Center help system

The SafeGuard Management Center help system is displayed in your browser. It provides comprehensive features such as context-specific help as well as a full-text search. It is configured for full functionality of the help system content pages enabling JavaScript in your browser.

With Microsoft Internet Explorer, the behaviour is as follows:

■ Windows XP/Windows Vista/Windows 7 - Internet Explorer 6/7/8 - Default security:
  You do not see a Security Bar informing you that Internet Explorer has blocked scripting from running.
  JavaScript is running.

  An information box is displayed informing you that the Enhanced Security Configuration is enabled and the page is running scripting. You can disable this message.
  JavaScript is running.

Note:
Even with JavaScript disabled, you can still display and navigate the SafeGuard Management Center help system. However, certain functionality such as the Search cannot be displayed.

5.4 Configuring SafeGuard Management Center

After installation, you need to configure the SafeGuard Management Center. The SafeGuard Management Center Configuration Wizard provides comfortable assistance for initial configuration by helping to specify the basic SafeGuard Management Center settings and the connection to the database. This wizard opens automatically when you start the SafeGuard Management Center for the first time after installation.

You may configure the SafeGuard Management Center for use with a single database or with multiple databases (Multi Tenancy).

Note:
You need to carry out initial configuration using the Configuration Wizard for Single Tenancy as well as for Multi Tenancy configurations.

5.4.1 Prerequisites

The following prerequisites must be met:

■ Make sure that you have Windows administrator rights.
Have the following information at hand. Where necessary, you can obtain this information from your SQL administrator.

- SQL credentials
  The name of the SQL Server which the SafeGuard Enterprise Database is to run on.
  The name of the SafeGuard Enterprise Database, if it has already been created.

### 5.4.2 Multi Tenancy configurations

You are able to configure different SafeGuard Enterprise Databases and maintain them for one instance of the SafeGuard Management Center. This is particularly useful when you want to have different database configurations for different domains, organizational units or company locations.

**Note:**

You need to set up a separate SafeGuard Enterprise Server instance for each database (tenant).

To ease configuration, previously created configurations can also be imported from files or newly created database configurations can be exported to be reused later.

To configure SafeGuard Management Center for Multi Tenancy, first carry out initial configuration and then proceed with further specific configuration steps for Multi Tenancy.

### 5.4.3 Start initial SafeGuard Management Center configuration

After installation of the SafeGuard Management Center, you need to carry out initial configuration. You need to do so in Single Tenancy as well as in Multi Tenancy mode.

To start the SafeGuard Management Center Configuration Wizard:

1. Select **SafeGuard Management Center** from the **Start** menu. The Configuration Wizard is launched and guides you through the necessary steps.
2. On the **Welcome** page, click **Next**.

### 5.4.4 Configure the database server connection

A database is used to store all SafeGuard Enterprise specific encryption policies and settings. For the SafeGuard Management Center and the SafeGuard Enterprise Server to be able to communicate with this database, you must specify an authentication method for the database access, either Windows NT authentication or SQL authentication. If you want to connect to the database server...
with SQL authentication, make sure that you have the respective SQL credentials at hand. Where necessary, you may obtain this information from your SQL administrator.

1. On the **Database Server Connection** page, do the following:

   - Under **Connection settings**, select the SQL database server from the **Database Server** list. All computers on a network on which a Microsoft SQL Server is installed are listed. If you cannot select the server, enter the server name or IP address with the SQL instance name manually.
   
   - Select **Use SSL** to secure the connection between SafeGuard Management Center and SQL database server. We strongly recommend that you do so when you have selected **SQL Server Authentication** because this setting will encrypt the transport of the SQL credentials. SSL encryption requires a working SSL environment on the SQL database server which you have to set up in advance, see **Securing transport connections with SSL** (page 45).

2. Under **Authentication**, activate the type of authentication to be used to access the database server instance. This is needed so that the SafeGuard Management Center is able to communicate with the database:

   - Select **Use Windows NT Authentication** to use your Windows credentials.
     
     **Note:**
     
     Use this type when your computer is part of a domain. However, additional mandatory configuration is required as the user needs to be authorized to connect to the database, see **Configure a Windows account for SQL server logon** (page 22) and **Configure Windows authentication for SQL server logon** (page 28).

   - Select **Use SQL Server Authentication** to access the database with the respective SQL credentials. Enter the credentials for the SQL user account that your SQL administrator has created. Where necessary, you may obtain this information from your SQL administrator.
     
     **Note:**
     
     Use this type when your computer is not part of a domain. Make sure that you have selected **Use SSL** to secure the connection to and from the database server.

3. Click **Next**.

   The connection to the database server has been established.
5.4.5 Create or select a database

On the Database Settings page, determine whether an existing or a new database is used to store administration data.

1. Do one of the following:
   - If a database does not yet exist, select Create a new database named. Enter a name for the new database. To do this, you need the relevant SQL access rights, see Database access rights (page 22). SafeGuard Enterprise Database names should only consist of the following characters to prevent localization issues: characters (A-Z, a-z), numbers (0-9), underscores (_).
   - If a database has already been created or if you have already installed the SafeGuard Management Center on a different computer, select Select an available database and select the respective database from the list.

2. Click Next.

5.4.6 Create the Master Security Officer (MSO)

As security officer, you access the SafeGuard Management Center to create SafeGuard Enterprise policies and configure the encryption software for the end users.

The Master Security Officer (MSO) is the top-level administrator with all the rights and a certificate that does not expire.

1. On the Security Officer Data page under Master Security Officer ID, enter a name for the Master Security Officer.
2. Under Token logon, specify if you want to use or not use a token/smartcard for logon.
   - Initially, we recommend that you do not activate token logon as Mandatory. Logon with token or smartcard requires separate configuration which must be carried out within the SafeGuard Management Center.
3. Under Certificate for MSO, do one of the following:
   - Click Create to create a new MSO certificate. You are prompted to enter and confirm a password each for the certificate store and for the file the certificate are to be exported to (private key file P12). The certificate is created and displayed under Certificate for MSO.
   - Click Import to use a certificate for the MSO that is already available on the network. In Import Authentication Certificate browse for the backed up key file. Under Key file password enter and confirm the password specified for this file. Select Store key file in certificate store and enter the password for the store. Click OK. The certificate is imported and displayed under Certificate for MSO.

The MSO needs the certificate store password to log on to the SafeGuard Management Center. Make a note of this password and keep it in a safe place! If you lose it, the MSO will not be able to log on to the SafeGuard Management Center.
The MSO needs the private key file password for restoring a broken SafeGuard Management Center installation.

4. Click **Next**.

The Master Security officer is created.

### 5.4.6.1 Create the MSO certificate

In **Create MSO Certificate**, do the following:

1. Under **Master Security Officer ID**, confirm the Master Security Officer name.
2. Enter the password for the certificate store twice and click **OK**.

The MSO certificate is created and saved locally as a backup (\(<\text{mso\_name}\>\).cer).

**Note:**
Make a note of the password and keep it in a safe place. You need it to authenticate at SafeGuard Management Center.

### 5.4.6.2 Export the MSO certificate

The MSO certificate is exported to a file - the so-called private key file (P12) which is secured by a password. Thus, the MSO certificate has additional protection. The private key file is needed to restore a broken SafeGuard Management Center installation.

To export an MSO certificate:

1. In **Export certificate**, enter and confirm the password for the private key (P12 file). The password must consist of 8 alphanumeric characters.
2. Click **OK**.
3. Enter a storage location for the private key file.

The private key is created and the file is stored in the defined location (\(<\text{mso\_name}\>\).p12).

**Note:**
Create a backup of the private key (p12 file) and store it in a safe place right after initial configuration. In case of PC failure the key is otherwise lost and SafeGuard Enterprise has to be reinstalled. This applies to all SafeGuard generated security officer certificates. For further information, see the Administrator Help, chapter *Exporting company and Master Security Officer certificate*.

### 5.4.6.3 Import the MSO certificate

If an MSO certificate is already available, you need to import it into the certificate store.
Note: A certificate cannot be imported from a Microsoft PKI. An imported certificate must have a minimum of 1024 bits and a maximum of 4096 bits.

1. In Import Authentication Key file, click [...] and select the key file. Enter the password for key file. Enter the password for the certificate store previously defined in Cert. store password or token PIN. Select Import to certificate store, or select Copy to token to store the certificate on a token.

2. Enter the password once more to initialize the certificate store.

Certificates and private keys are now contained in the certificate store. Logging on to SafeGuard Management Center then requires the password to the certificate store.

5.4.7 Create the company certificate

The company certificate is used to differentiate between SafeGuard Management installations. In combination with the MSO certificate it allows for restoring a broken SafeGuard Enterprise Database configuration.

2. Enter a name of your choice.
3. Click Next.

The newly created company certificate is stored in the database.

Create a backup of the company certificate and store it in a safe place right after initial configuration.

To restore a broken database configuration, see Restore a corrupt database configuration (page 41).

5.4.8 Complete initial SafeGuard Management Center configuration

1. Click Finish to complete the initial configuration of SafeGuard Management Center.

A configuration file is created.

You have created the following:

- A connection to the SafeGuard Enterprise Server.
- A SafeGuard Enterprise Database.
- A Master Security Officer account to log on to SafeGuard Management Center.
- All necessary certificates to restore a corrupt database configuration or SafeGuard Management Center installation.

SafeGuard Management Center is launched once the configuration wizard has closed.
5.5 Create further database configurations (Multi Tenancy)

**Prerequisite:** The feature Multi Tenancy must have been installed with an installation of type **Complete**. SafeGuard Management initial configuration must have been carried out, see *Start initial SafeGuard Management Center configuration* (page 32).

**Note:**
You need to set up a separate SafeGuard Enterprise Server instance per database.

To create a further SafeGuard Enterprise Database configuration after initial configuration:

1. Start the SafeGuard Management Center. The **Select Configuration** dialog is displayed.
2. Click **New**. The SafeGuard Management Center Configuration Wizard starts automatically.
3. The Wizard guides you through the necessary steps of creating a new database configuration. Make your settings as required. The new database configuration is generated.
4. To authenticate at the SafeGuard Management Center you are prompted to select the Security Officer name for this configuration and to enter their certificate store password. Click **OK**.

The SafeGuard Management Center is launched and connected to the new database configuration. When the SafeGuard Management Center is started for the next time, the new database configuration can be selected from the list.

**Note:**
For further tasks concerning Multi Tenancy see the Administrator Help, chapter *Working with multiple database configurations*.

5.6 Configure additional instances of the SafeGuard Management Center

You can configure additional instances of the SafeGuard Management Center to give security officers access for carrying out administrative tasks on different computers. SafeGuard Management Center can be installed on any computer on the network from which the databases can be accessed.

SafeGuard Enterprise manages the access rights to the SafeGuard Management Center in its own certificate directory. This directory must contain all certificates for all security officers authorized to log on to the SafeGuard Management Center. Logging on to the SafeGuard Management Center then requires only the password to the certificate store.

1. Install SGNManagementCenter.msi on a further computer with the required features.
2. Start SafeGuard Management Center on the computer with the newly installed SafeGuard Management Center. The Configuration Wizard is launched and guides you through the necessary steps.
3. On the **Welcome** page, click **Next**.
4. On the **Database Server Connection** page, under **Database Server**, select the required SQL database instance from the list. All database servers available on your computer or network are displayed. Under **Authentication**, activate the type of authentication to be used to access this database server instance. If you select **Use SQL Server Authentication**, enter the SQL user account credentials that your SQL administrator has created. Click **Next**.

5. On the **Database Settings** page, click **Select an available database** and select the respective database from the list. Click **Next**.

6. In **SafeGuard Management Center Authentication**, select an authorized person from the list. If Multi Tenancy is enabled, the dialog shows to which configuration the user is going to log on. Enter and confirm the password for the certificate store.

   A certificate store is created for the current user account and is protected by this password. You only need this password for any subsequent logon.

7. Click **OK**.

   You see a message that the certificate and private key have not been found or cannot be accessed.

8. To import the data, click **Yes**, and then click **OK**. This starts the import process.

9. In **Import Authentication Key file**, click [...] and select the key file. Enter the **password for key file**. Enter the password for the certificate store previously defined in **Cert. store password or token PIN**. Select **Import to certificate store**, or select **Copy to token** to store the certificate on a token.

10. Enter the password once more to initialize the certificate store.

   Certificates and private keys are now contained in the certificate store. Logging on to the SafeGuard Management Center then requires the password to the certificate store.

### 5.7 Logon to SafeGuard Management Center

Logon to SafeGuard Management Center depends on whether you run it in Single Tenancy or in Multi Tenancy mode.

For first steps in the SafeGuard Management Center refer to the SafeGuard Enterprise Administrator help.

#### 5.7.1 Log on in Single Tenancy mode

1. Start SafeGuard Management Center from the **Start** menu. A logon dialog is displayed.
2. Log on as an MSO (Master Security Officer) and enter the certificate store password specified during initial configuration. Click **OK**.

   SafeGuard Management Center is launched.
Note: If you enter an incorrect password, an error message is displayed and a delay is imposed for the next logon attempt. The delay period is increased with each failed logon attempt. Failed attempts are logged.

5.7.2 Log on in Multi Tenancy mode

The logon process to SafeGuard Management Center is extended when you have configured several databases (Multi Tenancy).

1. Start SafeGuard Management Center from the product folder of the Start menu. The Select Configurations dialog is displayed.
2. Select the database configuration you want to use and click OK. The selected database configuration is connected to SafeGuard Management Center and becomes active.
3. You are prompted to select the Security Officer name for this configuration and to enter their certificate store password. Click OK.

SafeGuard Management Center is launched and connected to the selected database configuration.

Note:

If you enter an incorrect password, an error message is displayed and a delay is imposed for the next logon attempt. The delay period is increased with each failed logon attempt. Failed attempts are logged.

5.8 Setting up the organizational structure in the SafeGuard Management Center

There are two ways of mapping your organization in SafeGuard Enterprise:

- Importing a directory service, for example an Active Directory.

  During the synchronization with the Active Directory objects such as computers, users and groups are imported into the SafeGuard Management Center and stored in the SafeGuard Enterprise Database.

- Creating the company structure manually.

  If if there is no directory service available or if there are only few organizational units so that a directory service is not needed, you can create new domains/workgroups which the user/computer can log on to.

You can use either one of these two options or combine them. For example, you can import an Active Directory (AD) either partially or entirely, and create other organizational units (OUs) manually. No matter, if the organizational structure is imported or created manually, policy assignment is provided either way.

Note:
Note that when combining the two methods, the organizational units created manually are not mapped in the AD. If organizational units created in SafeGuard Enterprise are to be mapped in the AD, you must add these to the AD separately.

Note:
For information on how to import or create an organization structure, see the Administrator Help, chapter Setting up the organizational structure.

5.9 Importing the license file

SafeGuard Enterprise has an integrated license counter. By default, a fixed number of 5 licenses for every available SafeGuard Enterprise component is part of the installation. This enables the evaluation of other SafeGuard Enterprise components easily without any side effects. When purchasing SafeGuard Enterprise every customer receives a personalized license file for their company which needs to be imported into the SafeGuard Management Center.

For further information, see the Administrator Help, chapter Licenses.

5.10 Restore a corrupt SafeGuard Management Center installation

If a SafeGuard Management Center installation is corrupted but the database is still intact, the installation can be easily restored by installing the SafeGuard Management Center afresh and by using the existing database as well as the backed up Security Officer certificate.

■ The Master Security Officer certificate of the relevant database configuration must have been exported to .p12 file and must be available and valid.

■ The passwords for the .p12 file as well as for the certificate store must be known to you.

To restore a corrupt SafeGuard Management Center installation:

1. Install the SafeGuard Management Center installation package afresh. Open the SafeGuard Management Center. The Configuration Wizard is started automatically.

2. On the Database Connection page, select the relevant database server and configure the connection to the database if required. Click Next.

3. On the Database Settings page, click Select an available database and select the relevant database from the list.

4. On the Security Officer Data page, do one of the following:

■ If the backed up certificate file can be found on the computer, it is displayed. Enter the password you use for authenticating at SafeGuard Management Center.

■ If the backed up certificate file cannot be found on the computer, select Import. Browse for the backed up certificate file and click Open. Enter the password for the selected certificate file. Click Yes. Enter and confirm the password for authenticating at the SafeGuard Management Center.

5. Click Next, and then Finish to complete SafeGuard Management Center configuration.
The corrupt SafeGuard Management Center installation is restored.

5.11 Restore a corrupt database configuration

A corrupt database configuration can be restored by installing SafeGuard Management Center afresh to create a new instance of the database based upon the backed up certificate files. This guarantees that all existing SafeGuard Enterprise endpoint computers still accept policies from the new installation.

- The company and Master Security Officer certificates of the relevant database configuration must have been exported to .p12 files and must be available and valid. You backup the certificates in the SafeGuard Management Center.

- The passwords for the two .p12 files as well as for the certificate store must be known to you.

Note: We only recommend this type of restore if there is no valid database backup available. All computers that are connecting to a backend that was restored in this way will lose their user-machine assignment, resulting in a temporarily switched off Power-On-Authentication. Challenge/Response mechanisms will not be available until the corresponding endpoint computer has successfully sent its key information again.

To restore a corrupt database:

1. Install the SafeGuard Management Center installation package afresh. Open the SafeGuard Management Center. The Configuration Wizard is started automatically.

2. On the Database Connection page, select Create a new database. Under Database settings, configure the connection to the database. Click Next.

3. On the Security Officer Data page, select the relevant MSO and click Import.

4. In Import Authentication Certificate, browse for the backed up key file. Under Key file password enter and confirm the password specified for this file. Select Store key file in certificate store and enter the password for the store. Click OK.

5. The MSO certificate is imported. Click Next.

6. On the Company Certificate page, select Restore using an existing company certificate. Click Import to browse for the backed up certificate file that contains the valid company certificate. You are prompted to enter the password specified for the certificate store. Enter the password and click OK. Confirm the message with Yes. The company certificate is imported.

7. Click Next, then Finish.

The database configuration is restored.
6 Testing communication

When the SafeGuard Enterprise Server, the database and the SafeGuard Management Center have been set up, you should run a connection test. This section describes the required steps.

6.1 Prerequisites

Make or check the following settings before the connection test.

6.1.1 Ports/connections

The endpoints must create the following connections:

<table>
<thead>
<tr>
<th>SafeGuard endpoint connection to</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>SafeGuard Enterprise Server</td>
<td>Port 80/TCP</td>
</tr>
<tr>
<td></td>
<td>Port 443 when using SSL transport connection</td>
</tr>
</tbody>
</table>

The SafeGuard Management Center must create the following connections:

<table>
<thead>
<tr>
<th>SafeGuard Management Center connection to</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQL database</td>
<td>SQL Server 2005/SQL Server 2008 dynamic port: Port 1433/TCP and Port 1434/TCP</td>
</tr>
<tr>
<td>Active Directory</td>
<td>Port 389/TCP</td>
</tr>
<tr>
<td>SLDAP</td>
<td>Port 636 for the Active Directory import</td>
</tr>
</tbody>
</table>

The SafeGuard Enterprise Server must create the following connections:

<table>
<thead>
<tr>
<th>SafeGuard Enterprise Server connection to</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQL database</td>
<td>Port 1433/TCP and Port 1434/TCP for SQL 2005 (Express) dynamic port</td>
</tr>
<tr>
<td>Active Directory</td>
<td>Port 389/TCP</td>
</tr>
</tbody>
</table>
6.1.2 Authentication method

1. On the computer with SafeGuard Enterprise Server installed, open Internet Information Services (IIS) Manager.
2. In the tree structure, click Internet Information Services. Click "Servername", Web Sites, Default Web Site.
3. Right-click SGNSRV and click Properties.

6.1.3 Proxy server settings for web server and endpoint

Set the proxy server settings as follows:

1. In Internet Explorer, on the Tools menu, click Internet options. Then click Connections and click LAN settings.
2. In LAN Settings, under Proxy servers, clear Use a proxy server for your LAN.
   If a proxy server is required, click Bypass proxy server for local addresses.

6.1.4 Microsoft SQL Server 2005 settings

When using Microsoft SQL Server 2005, set the following:

1. Open Microsoft SQL Server Management Studio.
2. In the left hand pane of the Object Explorer, browse to Security.
3. Right-click Logins and click New Login. Add the following user in Microsoft SQL Server Management Studio (Role "sysadmin"): NT AUTHORITY\NETWORK SERVICE.

6.2 Test the connection (IIS 6 on Windows Server 2003)

1. On the computer with SafeGuard Enterprise Server installed, open Internet Information Services (IIS) Manager.
2. In the tree structure, click Internet Information Services. Click "Servername", Web Sites, Default Web Site. Check that the web page SGNSRV is available in the Default Web Site folder.
3. Right-click SGNSRV and click Browse. A list of possible actions is displayed on the right-hand side of the window.
4. From this list, select Check connection. The possible action is displayed on the right-hand side of the window.
5. To test the connection, click **Invoke**.

The connection test has been successful when the following output is displayed:

![Connection Test Output](image)

### 6.3 Test the connection (IIS 7 on Windows Server 2008)

1. On the computer with SafeGuard Enterprise Server installed, open **Internet Information Services (IIS) Manager**.
2. In the tree structure, click "Servername", **Sites**, **Default Web Site**. Check that the web page **SGNSRV** is available in the **Default Web Site** folder.
3. Right-click **SGNSRV**, select **Application** and click **Browse** to open the **SGNSRV Home** page **Sophos SafeGuard Web Service**.
4. On the **Sophos SafeGuard Web Service** page, a list of possible actions is displayed. On this list, click **CheckConnection**.
5. On the **CheckConnection** page, click **Invoke**.

The connection test has been successful when the following output is displayed:

![Connection Test Output](image)
7 Securing transport connections with SSL

To enhance security SafeGuard Enterprise supports encrypting the transport connections between its components with SSL:

- The connection between the database server and the web server as well as the connection between the database server and the computer on which the SafeGuard Management Center resides may be encrypted with SSL.

- The connection between the SafeGuard Enterprise Server and the SafeGuard Enterprise managed computer may either be secured by SSL or by SafeGuard specific encryption. The advantage of SSL is that it is a standard protocol and therefore a faster connection can be achieved as with using SafeGuard transport encryption.

**Note:** We strongly recommend that you use SSL encrypted communication in this case, except for demo or test setups. If, for some reason, this is not possible and SafeGuard specific encryption is used, there is an upper limit of 1000 clients that connect to a single server instance.

Before activating SSL in SafeGuard Enterprise, a working SSL environment needs to be set up.

7.1 Set up SSL

The following general tasks must be carried out for setting up the web server with SSL:

- Certificate Authority must be installed for issuing certificates used by SSL encryption.
- A certificate must be issued and the IIS server configured to use SSL and point to the certificate.
- The server name specified when configuring the SafeGuard Enterprise Server must be the same as the one specified in the SSL certificate. Otherwise client and server cannot communicate. For each SafeGuard Enterprise Server a separate certificate is needed.
- If you use Network Load Balancer make sure that the port range includes the SSL port.

For further information contact our technical support or see:

- [http://support.microsoft.com/default.aspx?scid=kb;en-us;316898](http://support.microsoft.com/default.aspx?scid=kb;en-us;316898)

7.2 Activate SSL encryption in SafeGuard Enterprise

You may activate SSL encryption in SafeGuard Enterprise as follows:

- Connection between web server and database server:

  Activate SSL encryption when registering the SafeGuard Enterprise Server in the SafeGuard Management Center Configuration Package Tool. For further information, see *Configure the*
database server connection (page 32) or see:

- Connection between the database server and SafeGuard Management Center
  Activate SSL encryption in the SafeGuard Management Center Initial Configuration Wizard, see Configure the database server connection (page 32).

- Connection between SafeGuard Enterprise Server and the SafeGuard Enterprise protected endpoint computer:
  Activate SSL encryption when creating the configuration package for the SafeGuard Enterprise managed endpoints in the SafeGuard Management Center Configuration Package Tool, see Create configuration package for managed computers (page 55).

You can set SSL encryption for SafeGuard Enterprise during first-time configuration of the SafeGuard Enterprise components or later at any time. Create a new configuration package afterwards and deploy it on the respective server or managed computer.
8 Registering and configuring SafeGuard Enterprise Server

The SafeGuard Enterprise Server needs to be registered and configured to implement the communication information between IIS server, database, and SafeGuard protected endpoint. The information is stored in a server configuration package.

You carry out this task in the SafeGuard Management Center. The workflow depends on whether SafeGuard Enterprise Server is installed on the same computer as the SafeGuard Management Center or on a different one.

You may set further properties such as add additional security officers for the selected server, or configure the connection to the database.

8.1 Register and configure SafeGuard Enterprise Server for the current computer

When SafeGuard Management Center and SafeGuard Enterprise Server are installed on the computer you are currently working on, register and configure SafeGuard Enterprise Server.

Note:

This option is not available if Multi Tenancy is installed.

1. Start SafeGuard Management Center.
2. On the Tools menu, click Configuration Package Tool.
3. Select the Servers tab and then select Make this computer an SGN Server.
4. Select Servers and then click Options:
   - SafeGuard Enterprise Server Configuration setup is automatically started.
5. Accept the defaults in all subsequent dialogs.

The SafeGuard Enterprise Server is registered. A server configuration package called <Server>.msi is created and directly installed on the current computer. The server information is displayed in the Servers tab. You may carry out additional configuration.

Note:

If you want to install a new server configuration package (MSI) on the SafeGuard Enterprise Server, make sure that you uninstall the outdated one. Additionally, manually delete the local cache so that it can be updated correctly with new configuration data, such as SSL settings. Then install the new configuration package on the server.
8.2 Register and configure SafeGuard Enterprise Server for a different computer

When the SafeGuard Enterprise Server is installed on a different computer than the SafeGuard Management Center, register and configure SafeGuard Enterprise Server:

1. Start SafeGuard Management Center.
2. On the Tools menu, click Configuration Package Tool
3. Select Servers tab and then click Add....
4. In Server Registration click [...] to select the server’s machine certificate. This is generated when the SafeGuard Enterprise Server is installed. By default it is located in the MachCert directory of the SafeGuard Enterprise Server installation directory. Its file name is <Computername>.cer. If the SafeGuard Enterprise Server is installed on a different computer than the SafeGuard Management Center, this .cer file must be accessible as a copy or a network permission.

Do not select the MSO certificate.

The fully qualified name (FQDN), for example server.mycompany.com and certificate information is displayed.

Note:

When using SSL as transport encryption between endpoint and server, the server name specified here must be identical with the one specified in the SSL certificate. Otherwise they cannot communicate.

5. Click OK.

The server information is displayed in the Servers tab.

6. Click the Server packages tab. The available servers are displayed. Select the required server. Specify the output path for the server configuration package. Click Create Configuration Package.

A server configuration package (MSI) called <Server>.msi is created in the specified location.

7. Confirm the success message with OK.
8. In the Servers tab, click Close.

You have finished registering and configuring SafeGuard Enterprise Server. Install the server configuration package (MSI) on the computer running the SafeGuard Enterprise Server. You may change the server configuration in the Servers tab any time.

Note:

If you want to install a new server configuration package (MSI) on the SafeGuard Enterprise Server, make sure that you uninstall the outdated one. Additionally, manually delete the local
cache so that it can be updated correctly with new configuration data, such as SSL settings. Then install the new configuration package on the server.

### 8.3 Edit SafeGuard Enterprise Server properties

You can edit the properties and settings for any registered server and its database connection at any time.

1. In the SafeGuard Management Center **Configuration Package Tool**, in the **Servers** tab, select the required server.
2. Carry out any of the following:

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scripting allowed</td>
<td>Click to enable use of the SafeGuard Enterprise Management API. This allows for scripting administrative tasks.</td>
</tr>
<tr>
<td>Server roles</td>
<td>Click to select/deselect an available security officer role for the selected server.</td>
</tr>
<tr>
<td>Add server role...</td>
<td>Click to add further specific security officer roles for the selected server if required. You are prompted to select the server certificate. The security officer role is added and can be displayed under <strong>Server roles</strong>.</td>
</tr>
<tr>
<td>Database connection</td>
<td>Click [...] to configure a specific database connection for any registered web server, including database credentials and transport encryption between the web server and the database server. For further information, see <em>Configure the database server connection</em> (page 32). Even if the database connection check has not been successful, a new server configuration package can be created. <strong>Note:</strong> You do not have to rerun the SafeGuard Management Center Configuration Wizard to update the database configuration. Simply make sure that you create a new server configuration package afterwards and distribute it to the respective server. When the updated server package is installed on the server, the new database connection can be used.</td>
</tr>
</tbody>
</table>

3. Create a new server configuration package in the **Server packages** tab.
4. Uninstall the outdated server configuration package, then install the new one on the respective server.

The new server configuration becomes active.
8.4 Register SafeGuard Enterprise Server with Sophos firewall enabled

A SafeGuard Enterprise protected endpoint is unable to connect to SafeGuard Enterprise Server when a Sophos firewall with default settings is installed on the endpoint computer. By default, the Sophos firewall blocks NetBIOS connections which are needed for resolving the SafeGuard Enterprise Server network name.

1. As a workaround, do one of the following:
   - Unblock NetBIOS connections in the firewall.
   - Include the fully qualified name of the SafeGuard Enterprise Server in the server configuration package. For further information, see Register and configure SafeGuard Enterprise Server for a different computer (page 48).
9 Setting up SafeGuard Enterprise on endpoints

SafeGuard Enterprise encryption software can be seamlessly integrated into the user’s normal environment and is easy and intuitive to use. According to your deployment strategy, the endpoints can be equipped with different SafeGuard Enterprise modules and configured to your needs.

Security officers may carry out installation and configuration locally on the endpoints or as part of a centralized software distribution. A central install ensures a standardized installation on multiple endpoints.

9.1 About managed and unmanaged endpoints

Endpoints can be configured as follows:

■ **Managed - SafeGuard Enterprise Clients (managed)**

  Central server-based management in SafeGuard Management Center.

  For managed endpoints a connection to the SafeGuard Enterprise Server exists. They receive their policies through the SafeGuard Enterprise Server. The connection may temporarily be disabled, for example during a business trip, but even so the endpoint is defined as managed.

■ **Unmanaged - Sophos SafeGuard Clients (standalone)**

  Local management through configuration packages created in SafeGuard Management Center.

  Unmanaged endpoints are never connected to the SafeGuard Enterprise Server and are not connected to the central management of SafeGuard Enterprise. They operate in standalone mode.

  Unmanaged endpoints receive SafeGuard Enterprise policies by way of configuration packages. They never receive policies over a connection to the SafeGuard Enterprise Server.

  SafeGuard Enterprise policies are created in the SafeGuard Management Center and exported to configuration packages. The configuration packages then need to be deployed by company software distribution mechanisms or installed manually on the endpoints.

  Different installation packages and modules are provided for each type of endpoint.

9.2 Restrictions

Note the restrictions for SafeGuard Enterprise on endpoints described in the following sections.

9.2.1 Restrictions for managed endpoints

Note the following restrictions for managed endpoints.

■ **Restrictions for initial encryption:**
Initial configuration of managed endpoints may involve the creation of encryption policies that may be distributed inside a configuration package to the SafeGuard Enterprise protected endpoints.

However, when the SafeGuard Enterprise protected endpoint is not connected to a SafeGuard Enterprise Server immediately after the configuration package is installed but is temporarily offline, only encryption policies with the following specific settings become immediately active:

Device protection of type volume-based using the Defined Machine Key as encryption key.

For all other policies involving encryption with user-defined keys to become active on the SafeGuard Enterprise protected endpoint, the respective configuration package has to be reassigned to the endpoint’s organizational unit as well. The user-defined keys are then only created after the endpoint is connected to SafeGuard Enterprise Server again.

The reason is that the Defined Machine Key is directly created on the SafeGuard Enterprise protected endpoint at the first restart after installation, whereas the user-defined keys can only be created after the endpoint has been registered at the SafeGuard Enterprise Server.

■ Restrictions for BitLocker Drive Encryption support:

The SafeGuard Data Exchange package (SGNClient_withoutDE.msi/SGNClient_withoutDE_x64.msi) is not available for use with BitLocker Drive Encryption support.

Note: Either SafeGuard Enterprise Device Protection or BitLocker Drive Encryption can be used on Windows Vista or Windows 7 but not both encryption methods simultaneously. If you want to change the encryption type, you must first decrypt all encrypted drives, uninstall the SafeGuard Enterprise encryption software, and then reinstall it with the features you want to use. The installation is aborted if you try to install both features at the same time.

9.2.2 Restrictions for unmanaged endpoints

The following features are not supported for unmanaged endpoints - Sophos SafeGuard Clients (standalone):

■ BitLocker Drive Encryption, BitLocker To Go
■ SafeGuard Configuration Protection
■ File Share

9.3 Preparing endpoints for encryption

Before you deploy SafeGuard Enterprise, we recommend that you prepare as follows.

■ A user account must be set up and active on the endpoints.
■ Ensure that you have Windows administrator rights.
■ Create a full backup of the data on the endpoint.
Drives to be encrypted must be completely formatted and have a drive letter assigned to them.

Sophos provides a hardware configuration file to minimize the risk of conflicts between the POA and your endpoint hardware. The file is contained in the encryption software package. We recommend that you install an updated version of this file before any significant deployment of SafeGuard Enterprise. The file is updated on a monthly basis and made available to download from: http://www.sophos.com/support/knowledgebase/article/65700.html

You can help us improve hardware compatibility by executing a tool that we provide to collect hardware relevant information only. The tool is very easy to use. The collected information is added to the hardware configuration file. For further information, see http://www.sophos.com/support/knowledgebase/article/110285.html.

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

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

In some cases you might be prompted to restart the endpoint and run chkdsk again. For further information, see: http://www.sophos.com/support/knowledgebase/article/107799.html.

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

- Windows XP: Select Application, Winlogon.

Use the Windows built-in defrag tool to locate and consolidate fragmented boot files, data files, and folders on local volumes. For further information, see: http://www.sophos.com/support/knowledgebase/article/109226.html.

Uninstall third party boot managers, such as PROnetworks Boot Pro and Boot-US.

We recommend that you install an updated version of the hardware configuration file before any significant deployment of SafeGuard Enterprise. The file is updated on a monthly basis and made available to download from: http://www.sophos.com/support/knowledgebase/article/65700.html.

If the boot partition on the endpoint has been converted from FAT to NTFS and the endpoint has not been restarted since, restart the endpoint once. Otherwise the installation might not be completed successfully.

For SafeGuard Enterprise Clients (managed) only: Check whether there is a connection to the SafeGuard Enterprise Server. Select this web address in Internet Explorer on the endpoints: http://<ServerIPAddress>/sgnsrv. If the Trans page shows Check Connection, connection to SafeGuard Enterprise Server is successfully established.

### 9.3.1 Prepare for Cloud Storage

The SafeGuard Enterprise module Cloud Storage offers file-based encryption of data stored in the cloud.
Cloud Storage makes sure that local copies of cloud data are encrypted transparently and remain encrypted when stored in the cloud.

The way users work with data stored in the cloud is not changed. The vendor-specific cloud software remains unaffected and can be used in the same way as before to send data to or receive data from the cloud.

To prepare endpoints for Cloud Storage:

■ The cloud storage software provided by the vendor must be installed on the endpoints where you want to install Cloud Storage.

■ The cloud storage software provided by the vendor must have an application or system service stored on the local file system that synchronizes data between the cloud and the local system.

■ The cloud storage software provided by the vendor must store the synchronized data on the local file system.

Note: Cloud Storage only encrypts new data stored in the cloud. If data was already stored in the cloud before installing Cloud Storage, this data is not automatically encrypted. If it is to be encrypted, users first have to remove it from the cloud and then enter it again after Cloud Storage has been installed.

9.3.2 Prepare for BitLocker Drive Encryption support

Note: Before you start the installation, decide if you want to use SafeGuard Enterprise in combination with BitLocker Drive Encryption or SafeGuard Enterprise native Device Protection. The installation is aborted if you try to install both at the same time.

If you want to use SafeGuard Enterprise to manage BitLocker endpoints, carry out the following specific preparations on the endpoint:

■ Windows Vista Enterprise or Ultimate or Windows 7 must be installed on the endpoint.

■ There must be a second partition for the BitLocker system volume with NTFS-formatted text partition with at least 1.5 GB. Microsoft provides a BitLocker partitioning tool.

■ BitLocker Drive Encryption must be installed and activated.

■ If TPM is to be used for authentication, TPM must be initialized, in possession and activated.

■ If you wish to install SafeGuard Enterprise volume-based encryption, you should make sure that no volumes have yet been encrypted with BitLocker Drive Encryption. Otherwise the system may be harmed.

■ To install BitLocker Drive Encryption support, either deactivate User Access Control (UAC) or log on with the built-in Administrator account.

For further information, contact Microsoft Support or see the following web sites:

■ Preparing BitLocker:
9.3.3 Prepare for a "Modify" installation

If an existing SafeGuard Enterprise installation is modified or if features are installed at a later time, the setup might complain that certain components (for example SafeGuard Removable Media Manager) are currently in use. This message is caused by the fact that the selected features share common components that are currently in use and therefore cannot be updated immediately. This message can be ignored since the affected components will be automatically updated upon restart.

This behavior applies to installation in attended and unattended mode.

9.4 Creating configuration packages

Depending on the required configuration, create the appropriate configuration packages for the endpoints in SafeGuard Management Center:

- For managed Windows endpoints - Managed client packages
- For unmanaged Windows endpoints - Standalone client packages
- For Macs - Managed client packages
- When using service accounts for post-installation tasks

The initial configuration package has to be installed on the endpoints with the encryption software.

9.4.1 Create configuration package for managed computers

1. In the SafeGuard Management Center, on the Tools menu, click Configuration Package Tool.
2. Select Managed client packages.
3. Click Add Configuration Package.
4. Enter a name of your choice for the configuration package.
5. Assign a primary SafeGuard Enterprise Server (the secondary server is not necessary).
6. If required, specify a policy group which must have been created beforehand in the SafeGuard Management Center to be applied to the computers. If you want to use service accounts for post-installation tasks on the computer, make sure that you include the respective policy setting in this first policy group, see Service accounts for post-installation tasks (page 57).
7. Select the **Transport Encryption** mode defining how the connection between SafeGuard Enterprise Client and SafeGuard Enterprise Server is to be encrypted, either Sophos encryption or SSL encryption.

The advantage of SSL is that it is a standard protocol and that a faster connection can be achieved as when using SafeGuard transport encryption. For further information, see *Securing transport connections with SSL* (page 45).

8. Specify an output path for the configuration package (MSI).
9. Click **Create Configuration Package**.

The configuration package (MSI) has now been created in the specified directory. You now need to distribute this package to the endpoint computers and deploy it on them.

### 9.4.2 Create configuration package for unmanaged computers

1. In the SafeGuard Management Center, on the **Tools** menu, click **Configuration Package Tool**.
2. Select **Standalone client packages**.
3. Click **Add Configuration Package**.
4. Enter a name of your choice for the configuration package.
5. Specify a **Policy Group** which must have been created beforehand in the SafeGuard Management Center to be applied to the computers.
6. Under **Key Backup Location**, specify or select a shared network path for storing the key recovery file. Enter the share path in the following form: `\network computer\`, for example `\mycompany.edu\`. If you do not specify a path here, the end user is prompted to name a storage location for this file when first logging on to the endpoint computer after installation.

The key recovery file (XML) is needed to enable recovery of Sophos SafeGuard protected computers and is generated on each Sophos SafeGuard protected computer.

**Note:**

Make sure to save this key recovery file at a file location accessible to the helpdesk. Alternatively, the files can be provided to the helpdesk by different mechanisms. This file is encrypted by the company certificate. It can therefore be saved to any external media or to the network to provide it to the help desk for recovery purposes. It can also be sent by e-mail.

7. Under **POA Group**, you can select a POA user group to be assigned to the endpoint computer. POA users can access the endpoint for administrative tasks after the Power-on Authentication has been activated. To assign POA users, the POA group must have been created beforehand in the **Users and Computers** area of the SafeGuard Management Center.
8. Specify an output path for the configuration package (MSI).
9. Click **Create Configuration Package**.

The configuration package (MSI) has now been created in the specified directory. You now need to distribute this package to the endpoint computers and deploy it on them.
9.4.3 Create configuration package for Macs

A configuration package for a Mac contains the server information and the company certificate. The Mac uses this information to report status information (POA on/off, encryption state, ...). Status information is displayed in the SafeGuard Management Center.

1. In the SafeGuard Management Center, on the **Tools** menu, click **Configuration Package Tool**.
2. Select **Managed client packages**.
3. Click **Add Configuration Package**.
4. Enter a name of your choice for the configuration package.
5. Assign a primary SafeGuard Enterprise Server (the secondary server is not necessary).
6. Select **SSL** as **Transport Encryption** for the connection between the endpoint and SafeGuard Enterprise Server. **Sophos** as **Transport Encryption** is not supported for Mac.
7. Specify an output path for the configuration package (ZIP).
8. Click **Create Configuration Package**.

The configuration package (ZIP) has now been created in the specified directory. You now need to distribute this package to your MACs and deploy it on them.

9.4.4 Service accounts for post-installation tasks

If you would like to install SafeGuard Enterprise with a central rollout, we recommend that you configure a service account list. Once an IT administrator is added to the service account list they can log on to endpoints after the installation of SafeGuard Enterprise without activating the Power-on Authentication (POA). This is advisable because normally the first user who logs on to an endpoint after installation is added to the POA as the primary account. Users included in service account lists, however are treated as SafeGuard Enterprise guest users.

With service accounts the workflow is as follows:

- SafeGuard Enterprise is installed on an endpoint.
- After restarting the endpoint, a rollout operator included on a service account list logs on to the endpoint using the windows logon prompt.
- According to the service account list applied to the endpoint the user is identified as a service account and is treated as a guest user.
- The rollout operator is not added to the POA and the POA does not become active. The end user can log on and activate the POA.

**Note:**

You need to create service account lists in a policy and assign it to the first policy group of the first configuration package you install on the endpoint after the encryption software is installed. For further information, see the Administrator Help.
9.5 Installing the encryption software

Setting up SafeGuard Enterprise encryption software on endpoints can be carried out in two ways:

- Install encryption software locally. This is advisable for a trial installation, for example.
- Install encryption software centrally. This ensures a standardized installation on multiple endpoints.

Before you start, check the available installation packages and features for managed and unmanaged endpoints. Installation steps for both variants are identical except that you assign a different configuration package for each of them.

The behavior of the endpoints when first logging on after installing SafeGuard Enterprise and the activation of the Power-on Authentication is described in the *SafeGuard Enterprise User help*.

9.5.1 Installation packages and features

The following table shows the installation packages and features of the Sophos SafeGuard encryption software on endpoints. You find the installation packages in the Installers folder of your product delivery.

**Note:**

When the operating system of the endpoint is Windows 7 64 bit or Windows Vista 64 bit, you may install the 64 bit variant of the installation packages (<package name>_<variant>.msi). The 64 bit package of SafeGuard Configuration Protection is available for Windows 7 64 bit.

Even if it is possible to only install a subset of features in a first-time installation, we recommend that you install the complete SafeGuard Device Protection package from the start.

<table>
<thead>
<tr>
<th>Package</th>
<th>Content</th>
<th>Available for managed endpoints</th>
<th>Available for unmanaged endpoints</th>
</tr>
</thead>
<tbody>
<tr>
<td>SGxClientPreinstall.msi</td>
<td><strong>Pre-installation package</strong>&lt;br&gt;The package must be installed before installing any encryption installation package. Provides endpoints with necessary requirements for successful installation of the current encryption software.</td>
<td>Yes mandatory</td>
<td>Yes mandatory</td>
</tr>
<tr>
<td>SGNClient.msi</td>
<td><strong>SafeGuard Device Protection package</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SGNClient_x64.msi</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Package</td>
<td>Content</td>
<td>Available for managed endpoints</td>
<td>Available for unmanaged endpoints</td>
</tr>
<tr>
<td>---------------------------</td>
<td>--------------------------------------------------------------------------</td>
<td>----------------------------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td><strong>BaseEncryption,SectorBasedEncryption</strong></td>
<td>Full disk encryption for internal and external hard disks. Includes Power-on Authentication. Select installation type Complete, Typical, Custom.</td>
<td><img src="green-checkmark" alt="Available" /></td>
<td><img src="green-checkmark" alt="Available" /></td>
</tr>
<tr>
<td><strong>BitLockerSupport</strong></td>
<td>BitLocker Drive Encryption with SafeGuard Enterprise support. Requires Microsoft BitLocker. Select installation type Custom.</td>
<td><img src="green-checkmark" alt="Available" /></td>
<td><img src="red-x" alt="Not Available" /></td>
</tr>
<tr>
<td><strong>SecureDataExchange</strong></td>
<td>SafeGuard Data Exchange: file-based encryption of data on removable media on all platforms without re-encryption. Select installation type Complete or Custom.</td>
<td><img src="green-checkmark" alt="Available" /></td>
<td><img src="green-checkmark" alt="Available" /></td>
</tr>
<tr>
<td><strong>FileShare</strong></td>
<td>File-based encryption of data on local hard disks and network shares, especially for workgroups. Select installation type Complete or Custom.</td>
<td><img src="green-checkmark" alt="Available" /></td>
<td><img src="red-x" alt="Not Available" /></td>
</tr>
<tr>
<td><strong>CloudStorage</strong></td>
<td>File-based encryption of data stored in the cloud. Local copies of data stored in the cloud are always encrypted transparently. To send data to or receive data from the cloud, vendor-specific software must be used. Select an installation of type Complete or Custom.</td>
<td><img src="green-checkmark" alt="Available" /></td>
<td><img src="green-checkmark" alt="Available" /></td>
</tr>
<tr>
<td>Package</td>
<td>Content</td>
<td>Available for managed endpoints</td>
<td>Available for unmanaged endpoints</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>----------------------------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>ConfigurationProtection</td>
<td>Control and secure endpoints and devices on every interface, port protection. Select an an installation of type Custom. To install SafeGuard Configuration Protection, activate this feature AND install an additional package, see Setting up SafeGuard Configuration Protection (page 71).</td>
<td><img src="checkmark.png" alt="Available" /></td>
<td><img src="x.png" alt="Not Available" /></td>
</tr>
<tr>
<td>SGNClient_withoutDE.msi</td>
<td>SafeGuard file-based encryption package</td>
<td><img src="checkmark.png" alt="Available" /></td>
<td><img src="checkmark.png" alt="Available" /></td>
</tr>
<tr>
<td>SGNClient_withoutDE_x64.msi</td>
<td>SecureDataExchange File-based encryption of data on removable media on all platforms without re-encryption. No Power-on Authentication provided. Select installation type Complete, Typical or Custom.</td>
<td><img src="checkmark.png" alt="Available" /></td>
<td><img src="checkmark.png" alt="Available" /></td>
</tr>
<tr>
<td>FileShare</td>
<td>File-based encryption of data on local hard disks and network shares, especially for workgroups. Select installation type Complete or Custom.</td>
<td><img src="checkmark.png" alt="Available" /></td>
<td><img src="x.png" alt="Not Available" /></td>
</tr>
<tr>
<td>CloudStorage</td>
<td>File-based encryption of data stored in the cloud. Local copies of data stored in the cloud are always encrypted transparently. To send data to or receive data from the cloud, vendor-specific software must be used. Select installation type Complete or Custom.</td>
<td><img src="checkmark.png" alt="Available" /></td>
<td><img src="checkmark.png" alt="Available" /></td>
</tr>
</tbody>
</table>
### 9.5.2 Install the encryption software locally

**Prerequisites:**

- Computers must have been prepared for encryption, see *Preparing endpoints for encryption* (page 52).
- Decide which encryption package and features you need to install.

To install the encryption software locally:

1. Log on to the computer as an administrator.
2. Install the pre-installation package **SGxClientPreinstall.msi** that provides the endpoint computer with the necessary requirements for a successful installation of the current encryption software.

   **Note:** Alternatively, you may install **vcredist_x86.exe** that you can download from here: [http://www.microsoft.com/downloads/details.aspx?FamilyID=766a6af7-ec73-40ff-b072-9112bab119c2](http://www.microsoft.com/downloads/details.aspx?FamilyID=766a6af7-ec73-40ff-b072-9112bab119c2) or check that **MSVCR100.dll** is present in the Windows\WinSxS folder on the computer.

3. Double-click the relevant encryption software package (MSI). A wizard guides you through the necessary steps.

4. In the wizard, accept the defaults on all subsequent dialogs.

   **Note:**

   In a first-time installation, we recommend that you select a **Complete** installation from the start. To only install a subset of features, choose a **Custom** installation and activate/deactivate the features you want.

   SafeGuard Enterprise is installed on the endpoint computer.

5. Go to the location where you saved the relevant configuration package (MSI) created beforehand in SafeGuard Management Center. Specific configuration packages need to be installed for managed and unmanaged endpoint computers, see [Creating configuration packages](page 55).

6. Install the relevant configuration package (MSI) on the computer.

7. After installation, make sure that endpoint computers are restarted twice to activate Power-on-Authentication. The computer must be restarted for a third time to perform a backup of the kernel data on every Windows boot.

   Make sure that the computer is not put into hibernation, sleep or hybrid sleep mode before the third restart to successfully complete the kernel backup.

   SafeGuard Enterprise is set up on the endpoint computer. For more information on the computer's logon behaviour after SafeGuard Enterprise installation, see the [SafeGuard Enterprise User help](#).

### 9.5.3 Installing the encryption software centrally

Installing encryption software centrally ensures a standardized installation on multiple endpoints.

**Note:** Within central software distribution the installation and configuration packages can only be assigned to an endpoint, they cannot be assigned to a user.

For a central installation, do the following:

- Check the available installation packages and features for managed and unmanaged endpoints, see [Installation packages and features](page 58).

- Check the command-line options.

- Check the list of feature parameters for the ADDLOCAL command-line option.

- Check the sample commands.
Prepare the installation script.

9.5.3.1 Prepare the installation script

Prerequisites:

- Computers must have been prepared for encryption.
- Decide which software package and features you need to install.

To install the encryption software centrally:

1. Create a folder called **Software** to use as a central store for all applications.
2. Use your own tools to create a package to be installed on the endpoint computers. The package must include the following in the order mentioned:

   **Note:** When carrying out the installation through Active Directory, use a separate group policy object (GPO) for each package and sort them in the order mentioned below to guarantee a successful installation.

<table>
<thead>
<tr>
<th>Package</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pre-installation package</td>
<td>The mandatory package provides the endpoint computers with the necessary requirements for a successful installation of the current encryption software, for example the required DLL <strong>MSVCR100.dll</strong>.</td>
</tr>
<tr>
<td><strong>SGxClientPreinstall.msi</strong></td>
<td><strong>Note:</strong> If this package is not installed, installation of the encryption software is aborted.</td>
</tr>
<tr>
<td>Encryption software package</td>
<td>For a list of available packages see <em>Installation packages and features</em> (page 58).</td>
</tr>
<tr>
<td>Configuration package for endpoint computers</td>
<td>Use the configuration packages created before in SafeGuard Management Center. Different configuration packages need to be installed for managed and unmanaged endpoint computers, see <em>Creating configuration packages</em> (page 55). Make sure that you delete any outdated ones first created in the SafeGuard Management Center.</td>
</tr>
</tbody>
</table>

3. Create a script with the commands for the pre-configured installation. The script must list which features of the encryption software you want to install, see *Feature parameters for ADDLOCAL option* (page 65). Open a command prompt, and then type the scripting commands. For the command-line syntax, see *Command line options for central installation* (page 64).

4. Distribute this package to the endpoint computers using company software distribution mechanisms.

   The installation is executed on the endpoint computers. The endpoint computers are then ready for use of SafeGuard Enterprise.
5. After installation, make sure that endpoint computers are restarted twice to activate Power-on-Authentication. They must be restarted for a third time to perform a backup of the kernel data on every Windows boot.

Make sure that computers are not suspended or hibernated before the third restart to successfully complete the kernel backup.

Additional configuration may be required to ensure that Power-on Authentication (POA) functions correctly on each hardware platform. Most hardware conflicts can be resolved using the Hotkeys built into the POA. Hotkeys can be configured in the POA after installation or by an additional configuration setting passed to the Windows Installer command msiexec. For further information, see:

http://www.sophos.com/support/knowledgebase/article/107781.html
http://www.sophos.com/support/knowledgebase/article/107785.html

9.5.3.2 Command line options for central installation

For a central installation, we recommend that you prepare a script using the Windows Installer component msiexec. Msiexec automatically carries out a pre-configured SafeGuard Enterprise installation. Msiexec is included in Windows XP, Vista and Windows 7. For further information, see: http://msdn.microsoft.com/en-us/library/aa367988(VS.85).aspx.

Command line syntax

msiexec /i <path+msi package name> /qn ADDLOCAL=ALL | <SGN Features> <SGN parameter>

The command line syntax consists of:

- Windows Installer parameters, which, for example, log warnings and error messages to a file during the installation.
- Sophos SafeGuard features, which are to be installed, for example, full disk encryption.
- Sophos SafeGuard parameters, to specify the installation directory, for example.

Command line options

You can select all available options using msiexec.exe in the prompt. The main options are described below.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/i</td>
<td>Specifies the fact that this is an installation.</td>
</tr>
<tr>
<td>/qn</td>
<td>Installs with no user interaction and does not display a user interface.</td>
</tr>
</tbody>
</table>
### 9.5.3.3 Feature parameters for ADDLOCAL option

You need to define in advance which features are to be installed on the endpoints. The feature names are added as parameters to the command option ADDLOCAL. List the feature after typing the option `ADDLOCAL` in the command:

- Separate the features by comma, not by space.
- Observe upper and lower case.
- If you select a feature, you also need to add all feature parents to the command line.
- You must list the features `Client` and `Authentication` by default.

The following tables list the features that can be installed on the endpoints. For further information, see: [http://www.sophos.de/support/knowledgebase/article/108426.html](http://www.sophos.de/support/knowledgebase/article/108426.html).

#### 9.5.3.3.1 Features for SafeGuard Device Protection

The table lists the available features for the SafeGuard Device Protection package (SGNClient.msi, SGNClient_x64.msi) to be listed in the ADDLOCAL option.

**Note:**

<table>
<thead>
<tr>
<th>Feature Parents</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client</td>
<td>Authentication</td>
</tr>
</tbody>
</table>
9.5.3.3.2 Features for SafeGuard file-based encryption

The table lists the available features for the SafeGuard file-based encryption package (SGNClient_withoutDE.msi, SGNClient_withoutDE_x64.msi) to be listed in the ADDLOCAL option.

<table>
<thead>
<tr>
<th>Feature Parents</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client</td>
<td>Authentication</td>
</tr>
<tr>
<td></td>
<td>Mandatory. You must state the feature Authentication and its parent feature Client by default.</td>
</tr>
<tr>
<td>Client</td>
<td>SecureDataExchange</td>
</tr>
<tr>
<td>Client</td>
<td>FileShare</td>
</tr>
<tr>
<td>Client</td>
<td>CloudStorage</td>
</tr>
<tr>
<td>Client</td>
<td>ConfigurationProtection</td>
</tr>
<tr>
<td></td>
<td>To install SafeGuard Configuration Protection, activate this feature AND install an additional package, see Setting up SafeGuard Configuration Protection (page 71).</td>
</tr>
</tbody>
</table>
### Feature Parents

<table>
<thead>
<tr>
<th>Feature Parents</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client</td>
<td>ConfigurationProtection</td>
</tr>
</tbody>
</table>

To install SafeGuard Configuration Protection, activate this feature AND install an additional package, see *Setting up SafeGuard Configuration Protection* (page 71).

#### 9.5.3.4 Sample command: SafeGuard Device Protection with File Share

The command installs the following:

- The endpoints are provided with the necessary requirements for successful installation of the current encryption software.
- Log on to endpoints with Windows Vista/Windows 7 Credential Provider.
- SafeGuard Enterprise Power-on Authentication (POA).
- SafeGuard Enterprise full disk encryption (volume-based).
- File Share with file-based encryption of data on local hard disk and network shares.
- Configuration package that configures the endpoint as a managed endpoint and enables connection to the SafeGuard Enterprise Server.
- Log files are created.

**Sample command:**

```
msiexec /i F:\Software\SGxClientPreinstall.msi /qn /log I:\Temp\SGxClientPreinstall.log
```

```
msiexec /i F:\Software\SGNClient.msi /qn /log I:\Temp\SGNClient.log
ADDLOCAL=Client,Authentication,CredentialProvider,
BaseEncryption,SectorBasedEncryption,FileShare
InstallDir=C:\Program Files\Sophos\SafeGuard Enterprise
```

```
msiexec /i F:\Software\SGNConfig_managed.msi /qn /log I:\Temp\SGNConfig_managed.log
```

#### 9.5.3.5 Sample command: SafeGuard file-based encryption

The command installs the following:

- The endpoints are provided with the necessary requirements for successful installation of the current encryption software.
SafeGuard Enterprise

- SafeGuard Data Exchange with file-based encryption of data on removable media.
- SafeGuard File Share with file-based encryption of data on local hard disk and network shares.
- SafeGuard Cloud Storage with file-based encryption of data stored on the cloud.
- Configuration package that configures the endpoint as a managed endpoint and enables connection to the SafeGuard Enterprise Server.
- Log files are created.

Sample command:

```plaintext
msiexec /i F:\Software\SGxClientPreinstall.msi /qn /log I:\Temp\SGxClientPreinstall.log
```

```plaintext
msiexec /i F:\Software\SGNClient_withoutDE.msi /qn /log I:\Temp\SGNClient_withoutDE.log ADDLOCAL=Client, Authentication,SecureDataExchange,FileShare,CloudStorage Installdir=C:\Program Files\Sophos\SafeGuard Enterprise
```

```plaintext
msiexec /i F:\Software\SGNConfig_managed.msi /qn /log I:\Temp\SGNConfig_managed.log
```

9.6 Install the encryption software for Mac

1. Using the web address and download credentials, go to the Sophos web site and download the Sophos SafeGuard Disk Encryption installer for Mac OS X.
2. Locate the installer disk image in the folder to where it was downloaded. Open the disk image. Find Sophos SafeGuard.pkg and double-click it to start the installer.
3. Click Continue. Follow the steps.
4. Enter the Mac OS X administrator credentials when the installer prompts you do to so. This is necessary to allow the installer to make changes.
5. When the installer has finished, restart your Mac.
6. After the restart Sophos SafeGuard Disk Encryption is installed.
7. Power-on Authentication (POA) has not been activated yet, but only displays "Secured by SOPHOS" and continues booting the operating system after about one second. The software will continue to display "Secured by SOPHOS" as long as no SafeGuard user has been created. When the first user is created Power-on Authentication is activated.

Sophos SafeGuard Disk Encryption for Mac places an icon on the right-hand side of the menu bar. Clicking the icon gives you access to the Sophos SafeGuard Disk Encryption user and disk management functions.
**Uninstalling Sophos SafeGuard Disk Encryption for Mac**

To uninstall Sophos SafeGuard Disk Encryption for Mac, use the uninstaller package **Sophos SafeGuard Uninstaller.pkg** in /Library/Sophos SafeGuard. You need to decrypt the hard drive first.

### 9.7 FIPS-compliant installations

The FIPS certification describes security requirements for encryption modules. For example, government bodies in the USA and in Canada require FIPS 140-2-certified software for particularly security-critical information.

SafeGuard Enterprise uses FIPS-certified AES algorithms. By default, a new, faster implementation of the AES algorithms is installed that is not yet FIPS certified.

To use the FIPS certified variant of the AES algorithm, set the FIPS_AES property to 1 (one) when installing the SafeGuard Enterprise encryption software.

This can be done in two ways:

- Add the property to the command line script:

  ```
  msiexec /i F:\Software\SGNClient.msi FIPS_AES=1
  ```

- Use a transform.

### 9.8 Installations on self-encrypting, Opal-compliant hard drives

SafeGuard Enterprise supports the vendor-independent Opal standard for self-encrypting hard drives and offers management of endpoints with hard drives of this type.

To ensure that the support of self-encrypting, Opal-compliant hard drives follows the standard closely, two types of check are carried out at the installation of SafeGuard Enterprise on the endpoint:

- **Functional checks**

  These include, among others, checking whether the drive identifies itself as an "OPAL" hard drive, whether communications properties are correct and whether all Opal features required for SafeGuard Enterprise are supported by the drive.

- **Security checks**

  Security checks ensure that only SafeGuard Enterprise users are registered on the drive and that only SafeGuard Enterprise users own the keys used to software-encrypt non-self-encrypting drives. If other users are found to be registered at installation, SafeGuard Enterprise automatically tries to disable these users. This is a functionality required by the Opal standard with the exception of a few default "authorities" which are required to run an Opal system.
Note: The security checks are repeated when an encryption policy for the drive is applied after successful Opal-mode installation. If they fail in this case, drive management has been manipulated outside of SafeGuard Enterprise in the meantime. In this case, SafeGuard Enterprise denies access to the drive and a corresponding message is displayed.

If any of these checks fail in an unrecoverable way, the installation does not fall back to software-based encryption. Instead all volumes on the Opal drive remain unencrypted.

If you want to force that no Opal checks are performed, use the following command line syntax:

```
MSIEXEC /i <name_of_selected_client_msi>.msi OPALMODE=2
```

Some Opal hard drives may have potential security issues. There is no way to automatically determine which privileges have been assigned to an unknown user/authority that has already been registered on the drive when SafeGuard Enterprise installation/encryption is carried out. If the drive refuses the command to disable such users, SafeGuard Enterprise falls back to software encryption to ensure maximum security for the SafeGuard Enterprise user. As we cannot give any security guarantees for the hard drives themselves, we have implemented a special installation switch to enable you to use drives which may have potential security risks at your own discretion.

For a list of hard drives for which this installation switch is necessary and for further information on supported hard drives, refer to the SafeGuard Enterprise Release Notes.

To apply the installation switch, use the following command line syntax:

```
MSIEXEC /i <name_of_selected_client_msi>.msi
IGNORE_OPAL_AUTHORITYCHECK_RESULTS=1
```

The internal property of the .msi has the same name, if you want to install it using a transform.

For further information on SafeGuard Enterprise with Opal-compliant hard drives, refer to the SafeGuard Enterprise administrator help and user help.
10 Setting up SafeGuard Configuration Protection

With SafeGuard Configuration Protection the interfaces and peripheral devices to be allowed on endpoints can be defined. This prevents that malware or data exports through unwanted channels such as WLAN to be introduced. SafeGuard Configuration Protection can also detect and block harmful hardware such as key loggers.

10.1 Prerequisites and Restrictions

Note the following:

■ To set up SafeGuard Configuration Protection on Windows 7 64 bit operating systems, you may use the 64 bit variants of the "Client" installation packages.

■ SafeGuard Configuration Protection is only available for managed endpoints (SafeGuard Enterprise Clients managed). It is not supported for unmanaged endpoints (Sophos SafeGuard Clients standalone).

■ .NET Version 2.1 has to be installed.

10.2 Install SafeGuard Configuration Protection centrally

When you centrally install SafeGuard Configuration Protection on endpoint computers, use the Windows Installer component msiexec.

The command line is as follows:

```
msiexec /i SGNCPClient.msi /quiet /norestart
```

Carry out the steps in the order mentioned:

1. Prepare for installation on the endpoint computers, see Preparing endpoints for encryption (page 52).
2. Create a folder Software to use as a central store for all applications.
3. Use your own tools to create a package to be installed on the endpoint computers. The package must include the following in the order mentioned:

<table>
<thead>
<tr>
<th>Preparatory installation package</th>
<th>The package provides the endpoint computers with the necessary requirements for a successful installation of the current encryption software, for example the required DLL MSVCR110.dll. <strong>Note:</strong> If this package is not installed, installation of the encryption software is aborted.</th>
</tr>
</thead>
<tbody>
<tr>
<td>SafeGuard Enterprise encryption software package</td>
<td>Install either the SafeGuard Device Protection package or the SafeGuard file-based encryption package. Add ConfigurationProtection as feature to the ADDLOCAL option. On Windows 7 64 bit operating systems, you may use the 64 bit variants of the installation packages.</td>
</tr>
<tr>
<td>SafeGuard Configuration Protection package</td>
<td>Install SGNCPClient.msi. To set up SafeGuard Configuration Protection on Windows 7 64 bit operating systems, you may use the 64 bit variant of the installation packages. Make sure that the computer is not restarted by using parameter /norestart: msiexec /i SGNCPClient.msi /quiet /norestart</td>
</tr>
<tr>
<td>Configuration package for managed endpoint</td>
<td>Use a configuration packages created beforehand in the SafeGuard Management Center. Before installing a new configuration package make sure that you uninstall any outdated ones.</td>
</tr>
</tbody>
</table>

4. To create the script, open a command prompt, and then type the scripting commands.

5. Distribute this package using company software distribution mechanisms to the endpoint computers.

**10.2.1 Sample command: SafeGuard Configuration Protection with Device Protection**

The msiexec commands must be executed in the order specified in the sample. In this sample, the following is installed:

- The endpoints are provided with the necessary requirements for successful installation of the current encryption software.
- SafeGuard Enterprise Power-on Authentication (POA).
- SafeGuard Enterprise full disk encryption (volume-based device protection).
**Note:** SafeGuard Configuration Protection must be listed as feature in the SafeGuard full disk encryption package.

- To initiate the installation of the SafeGuard Configuration Protection module the Configuration Protection installation package is added by specifying an additional msiexec command.
- The configuration package that configures the endpoint as a managed endpoint and enables connection to the SafeGuard Enterprise Server is installed.
- Log files are created.

**Example:**

```plaintext
msiexec /i F:\Software\SGxClientPreinstall.msi /qn /log I:\Temp\SGxClientPreinstall.log

msiexec /i F:\Software\SGNClient.msi /qn /log I:\Temp\SGNClient.log
ADDLOCAL=Client,Authentication,CredentialProvider,BaseEncryption,SectorBasedEncryption,ConfigurationProtection
Installdir=C:\Program Files\Sophos\SafeGuard Enterprise

msiexec /i F:\Software\SGNCPClient.msi /quiet /norestart

msiexec /i F:\Software\SGNClientConfig_managed.msi /qn /log I:\Temp\SGNClientConfig_managed.log
```

### 10.2.2 Sample command: SafeGuard Configuration Protection with file-based encryption

The msiexec commands must be executed in the order specified in the sample. In this sample, the following is installed:

- The endpoints are provided with the necessary requirements for successful installation of the current encryption software.
- SafeGuard Data Exchange with file-based encryption on removable media is installed.
  
  **Note:** SafeGuard Configuration Protection must be listed as feature for the SafeGuard Data Exchange installation package.

- To initiate the installation of the SafeGuard Configuration Protection module the Configuration Protection installation package is added by specifying an additional msiexec command.
The configuration package that configures the endpoint as a managed endpoint and enables connection to the SafeGuard Enterprise Server is installed.

- Log files are created.

**Example:**

```msiexec /i F:\Software\SGxClientPreinstall.msi /qn
/logI:\Temp\SGxClientPreinstall.log```

```msiexec /i F:\Software\SGNClient.msi /qn /log I:\Temp\SGNClient.log
ADDLOCAL=Client,Authentication,
SecureDataExchange,ConfigurationProtection
InstallDir=C:\Program
Files\Sophos\SafeGuard Enterprise```

```msiexec /i F:\Software\SGNCPCClient.msi /quiet /norestart```

```msiexec /i F:\Software\SGNClientConfig_managed.msi /qn /log
I:\Temp\SGNClientConfig_managed.log```

### 10.3 Install SafeGuard Configuration Protection locally

**Prerequisites:**
Computers must have been prepared for encryption, see *Preparing endpoints for encryption* (page 52).

To install SafeGuard Configuration Protection locally:

1. Log on to the computer as an administrator.
2. Install the pre-installation package **SGxClientPreinstall.msi** that provides the endpoint computer with the necessary requirements for a successful installation of the current encryption software.
3. Double-click the Sophos SafeGuard encryption package you want to install (SGNClient.msi or SGNClient_withoutDE.msi). A wizard guides you through the necessary steps.
4. In the wizard, accept the defaults, except as follows: Select an installation of type **Custom**. Under **Features**, make your selection and additionally select **Configuration Protection**.

The Sophos SafeGuard encryption software is installed on the endpoint computer and is enabled for use with SafeGuard Configuration Protection.
5. Double-click the SafeGuard Configuration Protection package (SGNCPClient.msi). A wizard guides you through the necessary steps.

In the wizard, accept the defaults, except as follows: Change the installation path to C:\Program Files\Sophos\SafeGuard Enterprise\ to make sure that the Configuration Protection module is installed in the correct directory.

6. Do not restart the computer.

7. Generate a configuration package of the type "managed" and install it on the endpoint computer immediately after the installation of both software packages.

8. Restart the endpoint computer.

SafeGuard Configuration Protection is installed on the endpoint computer.

10.4 Uninstall SafeGuard Configuration Protection

To uninstall SafeGuard Configuration Protection, carry out the steps in the order mentioned:

1. Uninstall the Sophos SafeGuard configuration package.

2. Double-click the Sophos SafeGuard encryption package installed. A wizard guides you through the necessary steps.

3. In the installation wizard, select an installation type **Modify**.

4. Under **Features**, deselect the feature **Configuration Protection**.

5. When the uninstall is finished, do not restart the computer.

6. Uninstall the SafeGuard Configuration Protection package (SGNCPClient.msi).

7. Restart the computer.

SafeGuard Configuration Protection is removed from the endpoint computer.

10.5 Upgrade SafeGuard Configuration Protection

To upgrade SafeGuard Configuration Protection:

1. Install the latest pre-installation package SGxClientPreinstall.msi to provide endpoint computers with necessary requirements for successful installation of the current encryption software.

2. Install the latest Sophos SafeGuard encryption package on the computer, either SGNClient.msi or SGNClient_withoutDE.msi. To set up SafeGuard Configuration Protection on Windows 7 64 bit operating systems, you may use the 64 bit variants of the encryption packages.

   Do not restart the computer when the installation is completed.

3. In **Add/Remove Programs**, remove the SafeGuard Configuration Protection package.

4. Restart the endpoint computer.

5. Install the latest SafeGuard Configuration Protection package SGNCPClient.msi/SGNCPClient_x64.msi.
6. Restart the endpoint computer.
7. In the SafeGuard Management Center, reassign the relevant Configuration Protection policy to the endpoint computer to reactivate it.

SafeGuard Configuration Protection is upgraded on the endpoint computer.
11 Setting up SafeGuard Enterprise Runtime

The SafeGuard Enterprise encryption software can be installed to protect data even if several operating systems are installed on separate volumes of the endpoint's hard disk (runtime system). SafeGuard Enterprise Runtime enables the following when it is installed on volumes with an additional Windows installation:

- The Windows installation residing on these volumes may successfully be started by a boot manager.
- Partitions on these volumes that have been encrypted by a full SafeGuard Enterprise Client installation with the defined machine key can successfully be accessed.

11.1 Requirements and restrictions

Note the following:

- SafeGuard Enterprise Runtime does not provide any SafeGuard Enterprise encryption features or functionality.
- SafeGuard Enterprise Runtime only supports those operating systems that are also supported by the SafeGuard Enterprise encryption software.
- Operation of USB keyboards may be restricted.
- Only boot managers that become active after Power-on Authentication are supported.
- Support for third party boot managers is not guaranteed. We recommend that you use Microsoft boot managers.
- SafeGuard Enterprise Runtime cannot be updated to a full SafeGuard Enterprise encryption installation.
- The Runtime installation package must be installed before the full version of the SafeGuard Enterprise encryption package is installed.
- Only volumes encrypted with the defined machine key in SafeGuard Enterprise can be accessed.

11.2 Preparations

To set up SafeGuard Enterprise Runtime, carry out the following preparations in the order shown:

1. Make sure that those volumes on which SafeGuard Enterprise Runtime is to run on are visible at the time of installation and can be addressed by their Windows name (for example C:).
2. Decide on which volume(s) of the hard disk SafeGuard Enterprise Runtime is to be installed on. In terms of SafeGuard Enterprise, these volumes are defined as "secondary" Windows installations. There can be several secondary Windows installations. Use the following package: SGNClientRuntime.msi or SGNClientRuntime_x64.msi (on Windows Vista 64 bit, Window 7 64 bit).
3. Decide on which volume of the hard disk the full version of the SafeGuard Enterprise Client is to be installed. In terms of SafeGuard Enterprise, this volume is defined as the "primary" Windows installation. There can only be one primary Windows installation. Use the following package: SGNClient.msi or SGNClient_x64.msi (on Windows Vista 64 bit, Window 7 64 bit). If required, you may additionally install Configuration Protection (SGNCPCClient.msi / SGNCPCClient_x64.msi available for Windows 7 64 bit operating systems).

4. Prepare the computer for encryption, see *Preparing endpoints for encryption* (page 52).

### 11.3 Install SafeGuard Enterprise Runtime

1. Select the required secondary volume(s) of the hard disk where you want to install SafeGuard Enterprise Runtime Client.
2. Start the secondary Windows installation on the selected volume.
3. Install the runtime installation package on the selected volume.
4. Accept the defaults in the subsequent dialog of the installer. You do not need to select special features.
5. Select an installation folder for the runtime installation.
6. Click **Finish** to complete the runtime installation.
7. Select the primary volume of the hard drive where you want to install the SafeGuard Enterprise encryption software.
8. Start the primary Windows installation on the selected volume.
9. Start the pre-installation package SGxClientPreinstall.msi to provide endpoint computers with the necessary requirements for successful installation of the encryption software.
10. Install the SafeGuard Enterprise encryption package on the selected volume.
11. Create a configuration package as required and deploy it on the endpoint computer.
12. Encrypt both volumes with the defined machine key.

### 11.4 Start up from a secondary volume with a boot manager

1. Start the computer.
2. Log on at Power-on Authentication with your credentials.
3. Start the boot manager and select the required secondary volume as boot volume.
4. Restart the computer from this volume.

Each volume encrypted with the defined machine key can be accessed.
12 Replicating the SafeGuard Enterprise Database

To enhance the performance of the SafeGuard Enterprise Database it may be replicated to several SQL servers.

This section describes how to set up replication for the SafeGuard Enterprise Database in a distributed environment. It is assumed that you already have some experience in working with the replication mechanism in Microsoft SQL Server.

Note:
Administration should only be carried out on the master database, not on the replicated databases.

12.1 Merge replication

Merge replication is the process of distributing data from Publisher to Subscribers, allowing the Publisher and Subscribers to make updates independently, and then merging the updates between sites.

Merge replication allows various sites to work autonomously and at a later time merge updates into a single, uniform result. The initial snapshot is applied to Subscribers, and then Microsoft SQL Server tracks changes to published data at the Publisher and at the Subscribers. The data is synchronized between servers continuously, at a scheduled time, or on demand. Because updates are made at more than one server, the same data may have been updated by the Publisher or by more than one Subscriber. Therefore, conflicts can occur when updates are merged.

Merge replication includes default and custom choices for conflict resolution that you can define as you configure a merge publication. When a conflict occurs, a resolver is invoked by the Merge Agent and determines which data will be accepted and propagated to other sites.

12.2 Setting up database replication

Setting up a replication for the SafeGuard Enterprise database is described by means of an example based on Microsoft SQL Server 2005.

In the example, SafeGuard Enterprise is administered exclusively from the database in Vienna. Any changes are passed on by the SafeGuard Management Center to the databases in Graz and Linz by way of the replication mechanism in Microsoft SQL Server 2005. Changes reported by the client computers through the web servers are also passed on to the Microsoft SQL Server 2005 by way of the replication mechanism.
12.2.1 Generate the master database

Set up the SafeGuard Enterprise master database first. In the example, this is the VIENNA database. The procedure for generating the master database is the same as for an SafeGuard Enterprise installation without replication.

- Generate the master database in the SafeGuard Management Center Configuration Wizard. This procedure requires that the SafeGuard Management Center is already installed. For further information, see Start initial SafeGuard Management Center configuration (page 32).

- Generate the master database with an SQL script. You find them in your product delivery. This procedure is often preferred if extended SQL permissions during SafeGuard Management configuration is not desirable. For further information, see Generate SafeGuard Enterprise Database with a script (page 26).

12.2.2 Generate the replication databases Graz and Linz

After setting up the master database, generate the replication databases. In the example, the replication databases are called Graz and Linz.

Note:
Data tables and EVENT tables are held in separate databases. Event entries are not connected by default so that the event database can be replicated to several SQL servers to enhance performance. If EVENT tables are connected, problems may arise during replication of its data records.

To generate the replication databases:

1. Create a publication for the master database in the Management Console of the SQL Server.
   - A publication defines the set of data that is to be replicated.
2. Select all tables, views and stored procedures for synchronization in this publication
3. Create the replication databases by generating a subscription for Graz and a subscription for Linz. The new Graz and Linz databases then also appear in the subscriptions SQL configuration wizard.
4. Close the SQL configuration wizard. The replication monitor shows whether the replication mechanism runs correctly.
5. Make sure to enter the correct database name in the first line of the SQL script. For example, use Graz or use Linz.
6. Generate the snapshots again using the Snapshot Agent.

The replication databases Graz and Linz have been created.

### 12.3 Install and register SafeGuard Enterprise Servers

To install SafeGuard Enterprise Server on the web servers proceed as follows.

1. Install SafeGuard Enterprise Server on server WS_1.
2. Install SafeGuard Enterprise Server on server WS_2.
3. Register both servers in the SafeGuard Management Center: On the Tools menu, click Configuration Package Tool, and then click Register Server. On the Register Server tab, click Add.
   - You are prompted to add the server certificates ws_1.cer and ws_2.cer. You find them in the \Program Files\Sophos\Sophos SafeGuard\MachCert\ folder. These certificates are needed to create the appropriate configuration packages.

The SafeGuard Enterprise Servers are installed and registered.

### 12.4 Create the configuration packages for the GRAZ database

You need to create the configuration packages for the GRAZ database: one for server WS_1 to communicate with the GRAZ database and one for the SafeGuard Enterprise Clients GRAZ connecting to web service WS_1.

1. In the SafeGuard Management Center, on the Tools menu, click Options, and then click Database connections.
2. In Database Connection, select WS_1 as Database Server and GRAZ as Database. Click OK.
3. On the Tools menu, click Configuration Package Tool, and then click Create Server Configuration Package. Select the WS_1 server, select the output path and click Create Configuration Package.

4. Switch to the Create Configuration Package (managed) tab. Click Add Configuration Package and enter a name for the package. Under Primary Server select the correct server the SafeGuard Enterprise Clients GRAZ are to be connected to: WS_1. Select the output path and click Create Configuration Package.

The SafeGuard Enterprise Server and Client configuration packages for the GRAZ database have been created in the defined location.

12.5 Create the configuration packages for the LINZ database

You need to create the configuration packages for the LINZ database: One for server WS_2 to communicate with the LINZ database and one for the SafeGuard Enterprise Clients LINZ connecting to web service WS_2.

1. In the SafeGuard Management Center, on the Tools menu, click Options, then click Database Connection

2. In Database Connection, select WS_2 as Database Server and LINZ as Database. Click OK.

3. On the Tools menu, click Configuration Package Tools and then click Create Server Configuration Package. Select the WS_2 server, select the output path and click Create Configuration Package.

4. Switch to the Create Configuration Package (managed) tab. Click Add Configuration Package and enter a name for the package. Under Primary Server select the correct server the SafeGuard Enterprise Clients LINZ are to be connected to: WS_2. Select the output path and click Create Configuration Package. Click Close.

5. Link the SafeGuard Management Center to the VIENNA database again: On the Tools menu, click Options, then click Database Connection.

The SafeGuard Enterprise Server and Client configuration packages for the LINZ database have been created in the defined location.

12.6 Install the SafeGuard Enterprise Server configuration packages

1. Install the server configuration package ws_1.msi on web service WS_1 which is to communicate with the GRAZ database.

2. Install the server configuration package ws_2.msi on web service WS_2 which is to communicate with the LINZ database.

3. Test the communication between the SafeGuard Enterprise Servers and these databases, see Test the connection (IIS 6 on Windows Server 2003) (page 43).
12.7 Setup the endpoint computers

To install the encryption software on endpoint computers, see *Installing the encryption software centrally* (page 62).

**Note:**

For configuration of the endpoints, make sure that you install the correct configuration package after installation:

1. Install the GRAZ configuration package on the endpoints that are to be connected to the GRAZ server WS_1.
2. Install the LINZ client configuration package on the endpoints that are to be connected to the LINZ server WS_2.

For information on updating replicated SafeGuard Enterprise databases, see *Upgrade SafeGuard Enterprise replicated databases* (page 85).
13 About upgrading

SafeGuard Enterprise 5.5x or above can be directly upgraded to the latest version of SafeGuard Enterprise without changing any previous settings. If you want to upgrade from older versions, you must first upgrade to version 5.50.

An upgrade to the latest version of Sophos SafeGuard comprises upgrading the following components. Carry out the upgrade in the order shown below:

1. SafeGuard Enterprise Database
2. SafeGuard Enterprise Server
3. SafeGuard Management Center
4. SafeGuard Enterprise protected endpoint computers

Note:

When upgrading from SafeGuard Enterprise 5.x to SafeGuard Enterprise 6, you need to manually import a default evaluation license for SafeGuard Cloud Storage and SafeGuard File Share. This license file is provided in your product delivery.

When upgrading from SafeGuard Enterprise below 5.30, please contact your sales partner in advance to request a valid license. From SafeGuard Enterprise 5.30 onwards the import of a valid license file is required.

13.1 Upgrade the SafeGuard Enterprise database and database schema

Prerequisites:

- A SafeGuard Enterprise database version 5.50 or above must be installed. Older versions must first be updated to version 5.50.
- SQL migration scripts are needed for the upgrade. You find them in the Tools directory of your software delivery. Make sure that they are present on the database computer.
- .NET Framework 4 is required. It must be installed before the upgrade. It is provided in the SafeGuard Enterprise software delivery.
- Make sure that you have Windows administrator rights.

To upgrade the SafeGuard Enterprise database and database schema:

1. Close all instances of SafeGuard Management Center.
2. Create a backup of the SafeGuard Enterprise database.
3. Open Microsoft SQL Server Management Studio.
4. In the Object Explorer, right-click the SafeGuard Enterprise database and click Properties.
5. In the Database Properties window, select the Options page on the left. Under State, Restrict Access, select SINGLE-USER mode for running the SQL migration scripts.
6. In the Object Explorer, right-click the SafeGuard Enterprise database and click New Query.
7. Use the SQL migration scripts to update the database schema. The database must be converted version by version to the current version. Depending on the version installed, start the following SQL scripts in sequence, for example:
   a) 5.5x > 5.60: Run `MigrateSGN550_SGN560.sql`
   b) 5.6x > 6.0: Run `MigrateSGN560_SGN60.sql`
   If you have changed the default database name during installation, change the `USE SafeGuard` command in the script so that it reflects the current name accordingly.

8. In the Database Properties window, select the Options page on the left. Under State, Restrict Access, select MULTI-USER mode.

9. Upgrade one instance of SafeGuard Management Center by installing the latest version of the SafeGuard Management Center installation package (SGNManagementCenter.msi) from the product's install folder.

10. Start the upgraded SafeGuard Management Center.

    The database consistency is now checked automatically. If the cryptographic checksums of some tables are found incorrect, warning messages are displayed. To repair the tables select Repair in the relevant dialog. The checksums for the modified tables are recalculated.

    The latest version of the SafeGuard Enterprise database is ready for use.

13.1.1 Upgrade SafeGuard Enterprise replicated databases

When the SafeGuard Enterprise Database is to be upgraded and replicated databases are in use, we recommend that you uninstall the replicated databases before starting the upgrade on the master database.

Upgrading the SafeGuard Enterprise Database requires running special SQL migration scripts which might otherwise conflict with replicated databases.

To upgrade the replicated database:

1. Uninstall the replicated databases.
2. Carry out the steps for upgrading the master database and database schema, see Upgrade the SafeGuard Enterprise database and database schema (page 84).
3. Set up the replication databases anew, see Replicating the SafeGuard Enterprise Database (page 79).

13.2 Upgrade SafeGuard Enterprise Server

Prerequisites

- SafeGuard Enterprise Server 5.50 or higher must be installed. Versions below 5.50 must first be upgraded to SafeGuard Enterprise Server 5.50.
.NET Framework 4 and ASP.NET 4 is required. It must be installed before the upgrade. It is provided in the SafeGuard Enterprise product delivery. You can also download it for free from: http://www.microsoft.com/downloads

Make sure that you have Windows administrator rights.

To upgrade SafeGuard Enterprise Server:

1. Install the latest version of the SafeGuard Enterprise Server installation package.

SafeGuard Enterprise Server is upgraded to the latest version. It is automatically restarted and is ready for use.

13.3 Upgrade SafeGuard Management Center

Prerequisites:

- SafeGuard Management Center 5.50 or above must be installed. Versions below 5.50 must first be upgraded to SafeGuard Management Center 5.50.

- SafeGuard Enterprise database and SafeGuard Enterprise Server must have been upgraded to the latest version. For successful operation, version numbers of SafeGuard Enterprise database, SafeGuard Server and SafeGuard Management Center must match.

- SafeGuard Management Center 6 can manage SafeGuard Enterprise protected endpoints 5.5x and above.

- .NET Framework 4 is required. It must be installed before the upgrade. It is provided in the SafeGuard Enterprise product delivery.

- Make sure that you have Windows administrator rights.

- When upgrading from SafeGuard Enterprise 5.x to SafeGuard Enterprise 6, you need to manually import a default evaluation license for SafeGuard Cloud Storage and SafeGuard File Share. This license file is provided in your product delivery.

To upgrade SafeGuard Management Center:

1. Install the latest version of the SafeGuard Management Center installation package with the required features, see About migrating (page 90).
2. Start the SafeGuard Management Center. The behavior when starting the SafeGuard Management Center for the first time after the upgrade depends on the features installed:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The feature Multi Tenancy is not installed.</td>
<td>You are prompted to enter the SafeGuard Management Center security officer credentials.</td>
</tr>
<tr>
<td>The feature Multi Tenancy is newly installed.</td>
<td>The SafeGuard Management Center Configuration Wizard starts and prompts you to select which database is to be used. The wizard already preselects a previously used database. Select the required database and finish the wizard.</td>
</tr>
<tr>
<td>The feature Multi Tenancy is uninstalled.</td>
<td>The database configuration that has been used latest will be used in the upgraded SafeGuard Management Center.</td>
</tr>
</tbody>
</table>

3. In the SafeGuard Management Center, import the default evaluation license `DefaultLicense_CSFS.xml` for SafeGuard Cloud Storage and SafeGuard File Share from the following Sophos product folder `Sophos\SafeGuard Enterprise\Management Center`.

SafeGuard Management Center is upgraded to the latest version.

**Note:**

Existing SafeGuard Enterprise policies might have been modified when upgrading from a version below 5.40 as the policy structure has changed with version 5.35. In this case, reconfigure them as necessary.

After upgrading SafeGuard Management Center to the latest version, do not transfer existing POA users to SafeGuard Enterprise protected endpoints 5.5x or 5.6x. They would be interpreted as normal users in this case and registered as users on the respective endpoints.

### 13.4 Upgrade endpoints

This section is valid for both managed and unmanaged endpoints.

**Prerequisites**

- SafeGuard Enterprise encryption software version 5.5x or above must be installed. Older versions must first be upgraded to version 5.50.

  SafeGuard Management Center 6 and SafeGuard Enterprise Server 6 can manage SafeGuard Enterprise protected endpoints version 5.5x or above.

- SafeGuard Enterprise database and SafeGuard Enterprise Server must have been upgraded to the latest version. For successful operation, version numbers of SafeGuard Enterprise database, SafeGuard Server and SafeGuard Management Center must match.

  A mixture of endpoint encryption software versions should only be present during the time of the upgrade, but should be avoided for general use.
Make sure that you have Windows administrator rights.

To upgrade SafeGuard Enterprise protected endpoints:

1. Install the latest pre-installation package SGxClientPreinstall.msi that provides the endpoint with the necessary requirements for a successful installation of the current encryption software. Do not uninstall previous pre-installation packages.

2. From the product’s install folder, install the latest version of the respective SafeGuard Enterprise encryption software version by version until the latest version is reached, see Installing the encryption software centrally (page 62).

   Windows Installer recognizes the features that are already installed and only installs these again. If Power-on Authentication is installed, an updated POA kernel is also available after a successful update (policies, keys etc.). Sophos SafeGuard is automatically restarted on the computer.

   To install new features with the upgrade, select an installation of type Custom. Then select the new features and the ones to be upgraded. With an unattended installation, use the ADDLOCAL= property to select the features you want (existing and new).

3. In the SafeGuard Management Center that has been upgraded to the latest version, create a new configuration package and deploy it on the endpoints.

   Note: Installing a configuration package from a previous version on an endpoint that has been upgraded to the latest version is not supported. If you try to install an older configuration package over a newer one, the installation is aborted.

4. Delete all outdated or unused configuration packages on the endpoints for security reasons.

   The latest version of the SafeGuard Enterprise encryption software with the selected features is installed on the endpoints.

13.4.1 Migrate endpoints

You can migrate Sophos SafeGuard protected endpoints with an unmanaged configuration to a managed configuration. In this way, endpoints are defined in SafeGuard Management Center as objects which can be managed and which have a connection to the SafeGuard Enterprise Server.

Prerequisites

- Back up the endpoint before starting the upgrade.
- Make sure that you have Windows administrator rights.
- Sophos SafeGuard encryption software on the endpoints does not have to be uninstalled. Sophos SafeGuard version 5.5x or above must be installed on the endpoints. Older versions must be upgraded version by version until version 5.50 is reached.
To migrate endpoints:

1. Install the latest pre-installation package **SGxClientPreinstall.msi** that provides the endpoint with the necessary requirements for a successful installation of the current encryption software. Do not uninstall previous pre-installation packages.

2. From the product’s install folder, install the latest version of the respective Sophos SafeGuard encryption software, see *Installing the encryption software centrally* (page 62).

   Windows Installer recognizes the features that are already installed and only installs these again. If Power-on Authentication is installed, an updated POA kernel is also available after a successful update (policies, keys etc.). Sophos SafeGuard is automatically restarted on the endpoint.

   To install new features with the upgrade, select an installation type **Custom**. Then select the new features and the ones to be upgraded. With an unattended installation, use the ADDLOCAL= property to select the features you want (existing and new).

3. In SafeGuard Management Center, on the **Tools** menu, click **Configuration Package Tool**. Click **Create Configuration Package (managed)**.

4. Assign this package to the endpoint using a group policy.

   Authentication is disabled as the user-computer assignment is not upgraded. After upgrading, the endpoints are therefore unprotected!

5. The user needs to restart the endpoint. The first logon is still achieved with Autologon. New keys and certificates are assigned to the user.

6. The user needs to restart the endpoint for a second time. Log on at the Power-on Authentication. The endpoints are protected again only after the second restart.

7. Delete outdated and unused configuration packages.

The Sophos SafeGuard protected endpoint is now connected to the SafeGuard Enterprise Server.

### 13.5 Upgrade SafeGuard Configuration Protection

To upgrade SafeGuard Configuration Protection, see *Upgrade SafeGuard Configuration Protection* (page 75).
14 About migrating

This section describes migration scenarios that involve a change in your Sophos encryption software license. It covers migration of server-side software as well as endpoint software.

The following migration scenarios to SafeGuard Enterprise 6 are described:

- Migrating from Sophos Disk Encryption 5.61 (managed by Sophos Enterprise Console 5.1).
- Migrating from SGE/SDE 5.5 or above.
- Migrating from SGE/SDE 4.x
- Migrating endpoints to a different license.

Note: For a successful migration, you need a valid license.

14.1 Migrating from Sophos Disk Encryption 5.61

To migrate from Sophos Disk Encryption 5.61 (managed by Sophos Enterprise Console 5.1) to SafeGuard Enterprise 6 carry out the following steps:

- To 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 on separate servers.
- In the SafeGuard Management Center configuration wizard, select a new database to be created and import the company certificate exported from Enterprise Console.
- In SafeGuard Management Center, create the endpoint 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 preformed on them.

14.2 Migrating from SGE/SDE 5.5x or above

You can migrate SafeGuard Easy/Sophos SafeGuard Disk Encryption 5.5x or above to SafeGuard Enterprise 6 with central management to make use of comprehensive management features, for example user and computer management or extensive logging functionality.

To migrate SGE/SDE 5.5x or above to SafeGuard Enterprise 6:

- Migrate the management console.
Migrate the endpoints.

14.2.1 Migrate the management console

Prerequisites
- You do not have to uninstall SafeGuard Policy Editor.
- .NET Framework 4 with ASP.NET 4 is required. It must be installed before. It is provided in the SafeGuard Enterprise product delivery.
- Set up the latest version of SafeGuard Enterprise Server before migration. For further information, see Setting up SafeGuard Enterprise Server (page 12).
- Make sure that you have Windows administrator rights.

To migrate the management console:

1. On the computer on which SafeGuard Policy Editor is installed, start SGNManagementCenter.msi from the product’s install folder. A wizard guides you through installation. Accept the default options.
2. If prompted, restart the computer.
3. Start SafeGuard Management Center to carry out initial configuration, see Configuring SafeGuard Management Center (page 31).
4. Configure the SafeGuard Enterprise policies to your needs.

SafeGuard Policy Editor has been migrated to SafeGuard Management Center.

14.2.2 Migrate endpoints

You can migrate Sophos SafeGuard protected endpoints with an unmanaged configuration to a managed configuration. In this way, endpoints are defined in SafeGuard Management Center as objects which can be managed and which have a connection to the SafeGuard Enterprise Server.

Prerequisites
- Back up the endpoint before starting the upgrade.
- Make sure that you have Windows administrator rights.
- Sophos SafeGuard encryption software on the endpoints does not have to be uninstalled. Sophos SafeGuard version 5.5x or above must be installed on the endpoints. Older versions must be upgraded version by version until version 5.50 is reached.

To migrate endpoints:

1. Install the latest pre-installation package SGxClientPreinstall.msi that provides the endpoint with the necessary requirements for a successful installation of the current encryption software. Do not uninstall previous pre-installation packages.
2. From the product’s install folder, install the latest version of the respective Sophos SafeGuard encryption software, see *Installing the encryption software centrally* (page 62).

   Windows Installer recognizes the features that are already installed and only installs these again. If Power-on Authentication is installed, an updated POA kernel is also available after a successful update (policies, keys etc.). Sophos SafeGuard is automatically restarted on the endpoint.

   To install new features with the upgrade, select an installation type **Custom**. Then select the new features and the ones to be upgraded. With an unattended installation, use the `ADDLOCAL=` property to select the features you want (existing and new).

3. In SafeGuard Management Center, on the **Tools** menu, click **Configuration Package Tool**. Click **Create Configuration Package (managed)**.

4. Assign this package to the endpoint using a group policy.

   Authentication is disabled as the user-computer assignment is not upgraded. After upgrading, the endpoints are therefore unprotected!

5. The user needs to restart the endpoint. The first logon is still achieved with Autologon. New keys and certificates are assigned to the user.

6. The user needs to restart the endpoint for a second time. Log on at the Power-on Authentication. The endpoints are protected again only after the second restart.

7. Delete outdated and unused configuration packages.

The Sophos SafeGuard protected endpoint is now connected to the SafeGuard Enterprise Server.

### 14.3 Migrating from SGE 4.5/ SDE 4.6

You can migrate SafeGuard Easy (SGE) 4.5x as well as Sophos SafeGuard Disk Encryption 4.6x directly to SafeGuard Enterprise 6.

To migrate from SGE 4.5x/SDE 4.6x:

- Set up the management console SafeGuard Management Center.
- Migrate the endpoints.

This section describes the necessary steps and explains which features can be migrated and details the limitations.

#### 14.3.1 Set up the management console

If you have no SafeGuard Management installed, install the latest version. For further information, see *Setting up SafeGuard Management Center* (page 30).

If you have a previous version of SafeGuard Management Center installed, upgrade to the latest version. For further information, see *Upgrade SafeGuard Management Center* (page 86).
14.3.2 **Migrate endpoints**

Direct endpoint migration has been tested and is supported for SafeGuard Easy 4.5x. A direct upgrade should also work for versions between 4.3x and 4.4x. Direct upgrade is not supported for versions older than 4.3x, so these must be upgraded to SafeGuard Easy 4.50 first.

Direct endpoint migration has been tested and is supported for Sophos SafeGuard Disk Encryption 4.6x.

Hard drive encryption is maintained, so there is no need to decrypt and re-encrypt the hard drive. It is not necessary to uninstall SafeGuard Easy/Sophos SafeGuard Disk Encryption 4.x.

14.3.2.1 **Prerequisites**

The following prerequisites must be met:

- SafeGuard Easy/Sophos SafeGuard Disk Encryption must be running on the following operating system:
  
  Windows XP Professional Workstation Service Pack 2, 3

- Windows Installer Version 3.01 or higher has to be installed.

- The hardware must meet the system requirements of SafeGuard Enterprise 6.

- When using special software (for example Lenovo middleware), it must meet the system requirements of SafeGuard Enterprise 6.

- Migration is supported, if the hard disks are encrypted with the following algorithms: AES128, AES256, 3DES, IDEA.

- Users need a valid Windows account and password. If they do not know their Windows password, because they have previously been logged on to Windows using Secure Automatic Logon, the Windows user password has to be reset before migration and the new password has to be forwarded to the users.

14.3.2.2 **Limitations**

- Migration of endpoints with only the SGNClient_withoutDE.msi package installed is not supported. You have to uninstall this package first.

- Only the SafeGuard Device Protection package with the standard features can be installed (SGNClient.msi). If the SGNClient_withoutDE.msi package is to be installed in addition, this has to be done in a separate step as a direct upgrade is not supported for this package.

- The following installations cannot be migrated to SafeGuard Enterprise and a migration should not be attempted.

  **Note:**

  If you start migrating in the following cases, an error message is displayed (error number 5006).
Twin Boot installations
Installations with active Compaq Switch
Lenovo Computrace installations
Hard disks that are partially encrypted, for example with boot sector encryption only.
Hard disks with hidden partitions
Hard disks that have been encrypted with one of the following algorithms: XOR, STEALTH, DES, RIJNDAEL, Blowfish-8, Blowfish-16
Multi-boot scenarios with a second Windows or Linux partition

- Removable media that have been encrypted with one of the following algorithms cannot be migrated: XOR, STEALTH, DES, RIJNDAEL, Blowfish-8, Blowfish-16.

**Note:**
There is a risk of data being lost in these cases. After migration, data on the removable medium cannot be accessed with SafeGuard Enterprise any more.

- Removable media with Super Floppy volumes cannot be transformed after migration.

- Removable media can be converted to a SafeGuard Enterprise compatible format. After conversion, an encrypted data medium can only be read with SafeGuard Enterprise and only at the one endpoint where it was converted.

### 14.3.2.3 Preparing endpoints

- Prepare the endpoints for installation of the encryption software, see *Preparing endpoints for encryption* (page 52).

- We recommend that you create a valid kernel backup and save this backup in a location that can always be accessed, for example a network share. For further information, see your SafeGuard Easy 4.5x/Sophos SafeGuard Disk Encryption 4.6x manuals/help, chapter *Saving the system kernel and creating emergency media*.

- To reduce the risk of data loss, we recommend that you create a test environment for the first migration.

- When migrating from older versions of SafeGuard Easy, first upgrade to version 4.50.

- Leave the computers switched on throughout the migration process.

- The administrator should keep the users’ Windows credentials at hand in case users have forgotten their Windows passwords after migration. Users need a valid Windows account and password. If they do not know their Windows password, because they have previously been logged on to Windows using Secure Automatic Logon, the Windows user password has to be reset before migration and the new password has to be forwarded to them.

  **Note:** If users do not know their Windows password, they will not be able to log on to SafeGuard Enterprise. In this case pass-through to Windows is rejected. Thus, there is the risk of data loss as users will not be able to access their computers anymore.
### 14.3.2.4 Which functionality is migrated

The table below shows which functionality is migrated and how it is handled in SafeGuard Enterprise.

<table>
<thead>
<tr>
<th>SafeGuard Easy/Sophos SafeGuard Disk Encryption</th>
<th>Migration</th>
<th>SafeGuard Enterprise</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encrypted hard drives</td>
<td>Yes</td>
<td>The hard drive keys are protected by Power-on Authentication. So they are at no time exposed. If Boot Protection mode has been selected in SafeGuard Easy, the current version has to be uninstalled. The hard drive encryption algorithm is not changed by migration. Therefore the actual algorithm for this type of migration may differ from the general SafeGuard Enterprise policy.</td>
</tr>
<tr>
<td>Encrypted removable media (only applicable when migrating from SafeGuard Easy)</td>
<td>Yes</td>
<td>Encrypted removable media, for example USB flash drive, can be converted to the SafeGuard Enterprise format. Note: After conversion, an encrypted data medium can only be read with SafeGuard Enterprise and only at the endpoint where it was converted. The conversion needs to be confirmed in each case.</td>
</tr>
<tr>
<td>Encryption algorithms</td>
<td>To some degree</td>
<td>The algorithms AES128, AES256, 3DES, IDEA can be migrated. AES-128 and 3-DES however, are not available for selection in the SafeGuard Management Center for media that is to be newly encrypted.</td>
</tr>
<tr>
<td>SafeGuard Easy/Sophos SafeGuard Disk encryption user names and passwords</td>
<td>No</td>
<td>Windows user names and passwords are used in SafeGuard Enterprise. So, there is no need to reuse the SafeGuard Easy/Sophos SafeGuard Disk Encryption user names. Note: After migration, the first user to log on to Windows is set as primary user within the POA (unless they are specified on the Service Account list).</td>
</tr>
<tr>
<td>Policies</td>
<td>No</td>
<td>To make sure that all settings are consistent, no automatic migration is executed. The policies have to be reset in the SafeGuard Management Center.</td>
</tr>
<tr>
<td>Pre-Boot Authentication</td>
<td>No</td>
<td>Pre-Boot Authentication (PBA) is replaced by the SafeGuard Enterprise Power-on Authentication (POA).</td>
</tr>
<tr>
<td>Installations without GINA</td>
<td>Yes</td>
<td>Installations without GINA are migrated to SafeGuard Enterprise with SGNGINA installed.</td>
</tr>
</tbody>
</table>
The token/smartcard hardware can continue to be used in SafeGuard Enterprise. However, the credentials are not migrated. The tokens used before therefore need to be re-issued in SafeGuard Enterprise and set up using policies. Credentials in file form on token/smartcards remain as such, but can only be used to log on to endpoints with SafeGuard Easy/Sophos SafeGuard Disk Encryption support. If necessary, the token/smartcard middleware in use has to be upgraded to a version supported by SafeGuard Enterprise.

Logon with Lenovo Fingerprint Reader can continue to be used in SafeGuard Enterprise. The fingerprint reader hardware and software has to be supported by SafeGuard Enterprise and the fingerprint user data have to be rolled out again.

14.3.2.5 **Start migration**

**Note:** The installation can be carried out on a running SGE/SDE system. No decryption of encrypted hard drives or volumes is necessary. It is best performed centrally in unattended mode. Installation using the setup folder is not recommended.

Use the SafeGuard Device Protection package (SGNClient.msi) from the product’s install folder with the standard feature set. The SafeGuard package SGNClient_withoutDE.msi cannot be used for migration.

To migrate the endpoints:

1. Double-click WIZLDR.exe from the SafeGuard Easy/Sophos SafeGuard Disk Encryption program folder of the endpoint that is to be migrated. This starts the Migration Wizard.
2. In the Migration Wizard, enter the SYSTEM password and click **Next**. In **Destination folder**, click **Next**, and then click **Finish**. A migration configuration file SGMEMIG.cfg is created.
3. In Windows Explorer, rename this file from SGMEMIG.cfg to SGE2SGN.cfg.

   **Note:** Owner/creator rights have to be set for this file and the file path where it is stored during migration. Otherwise, migration may fail and a message stating that SGE2SGN.cfg cannot be found, is displayed.
4. Enter the “msiexec” command at the command prompt to install the following on the endpoints: the latest pre-installation package, the latest SafeGuard Device Protection package. Add the parameter MIGFILE stating the file path of the migration configuration file SGE2SGN.cfg:

Example:

```
msiexec /i \Distributionserver\Software\Sophos\SafeGuard\SGxClientPreinstall.msi
msiexec /i \Distributionserver\Software\Sophos\SafeGuard\SGNClient.msi
/L*VX"\Distributionserver\Software\Sophos\SafeGuard\%Computername%.log"
MIGFILE=\\Distributionserver\Software\Sophos\SafeGuard\SGE2SGN.cfg
```

■ If the migration has been successful, SafeGuard Enterprise is ready on the computer.
■ If the migration fails, SafeGuard Easy/Sophos SafeGuard Disk Encryption can still be used on the computer. In such cases, SafeGuard Enterprise is automatically removed.

### 14.3.2.6 Log on to the endpoint after migration

To log on to the endpoint after migration:

1. Restart the endpoint. The first logon is still achieved with Autologon. New keys and certificates are assigned to the user.
2. Restart the endpoint for a second time. Log on at the Power-on Authentication. The endpoints are protected again only after the second restart.
3. To be able to decrypt the hard disk or add and remove keys for hard disk encryption, restart the endpoint again.

After successful migration the following is available in SafeGuard Enterprise after logging on at the Power-on Authentication:

■ the keys and algorithms of encrypted volumes.

  Encrypted volumes remain encrypted and the encryption keys are automatically converted to a SafeGuard Enterprise compatible format.

■ the keys and algorithms for encrypted removable media (applicable only when upgrading from SafeGuard Easy).

  They have to be converted to a SafeGuard Enterprise compatible format.

### 14.3.2.7 Configure migrated endpoint computers

Endpoints are initially configured by configuration packages which, among other things, activate the Power-on Authentication.

**Prerequisites:**
Endpoint configuration should take place only after migration and only after the POA has been activated and the user has successfully logged on to Windows on the migrated endpoint.

1. In SafeGuard Management Center, on the **Tools** menu, click **Configuration Package Tool** and create the initial configuration package with the required policy settings.

   The policies transferred with the first configuration package should correspond to the previous configuration of the SafeGuard Easy/Sophos SafeGuard Disk Encryption endpoint.

   If no configuration package is installed after migration, all drives that were encrypted with SafeGuard Easy/Sophos SafeGuard Disk Encryption will stay encrypted.

2. Install the configuration package on the endpoints.

**14.3.2.8 Convert keys for encrypted removable media**

   Encrypted removable media remain encrypted, but the keys have to be converted to a format that is compatible with SafeGuard Enterprise.

   The appropriate policy for volume-based encryption has to be present on the endpoint before conversion. Otherwise the keys are not converted.

   **Note:**

   After conversion, an encrypted data medium can only be read with SafeGuard Enterprise 6 and only at the one endpoint where it was converted.

   1. Detach the media from the endpoint and reinsert it. This ensures that you can decrypt removable media or add and remove keys for removable media encryption.
   2. In Windows Explorer, double-click the media you want to access.
   3. You are prompted to confirm the transformation of the encryption keys into a SafeGuard Enterprise compatible format.
      - If you confirm the conversion, full access to the migrated data is provided.
      - If you reject the conversion, the migrated data can still be opened for reading and writing.

**14.4 Migrate endpoints to a different license**

You can migrate endpoints with only file-based encryption installed (SGNClient_withoutDE.msi) to also support SafeGuard Device Protection - full disk encryption (SGNClient.msi):

1. On the endpoint, uninstall the SGNClient_withoutDE.msi package.
2. Uninstall the relevant configuration package.
3. From the product’s install folder, install the SGNClient.msi package. A wizard guides you through installation. Accept the default options, make sure to select a **Complete** setup to install all encryption features available.
4. Create a new configuration package and deploy it on the endpoint.

   **Note:**
The local keys created during the installation of the SGNClient_withoutDE.msi installation package are still available.

To add SafeGuard Configuration Protection on an endpoint, see Setting up SafeGuard Configuration Protection (page 71).

14.5 Migrating the operating system

Once SafeGuard Enterprise is installed, it is only possible to update the Service Pack version of the operating system series installed. You can, for example install a Windows XP Service Pack update.

However, you cannot migrate from one operation system series to a different one when SafeGuard Enterprise is installed. For example, you cannot migrate from Windows XP to Windows 7 when SafeGuard Enterprise is installed.
15 About uninstallation

This section covers the following topics:

■ Preventing uninstallation of Sophos SafeGuard encryption software
■ Uninstallation best practices
■ Uninstalling Sophos SafeGuard encryption software

15.1 Uninstallation best practice

When the SafeGuard Enterprise encryption software is installed on the same computer as SafeGuard Management Center, make sure that you follow this uninstallation procedure to be able to continue using one of them:

1. Uninstall SafeGuard Management Center.
2. Uninstall the configuration package.
3. Uninstall the encryption software.
4. Install the package afresh that you want to continue using.

15.2 Uninstalling SafeGuard Enterprise encryption software

Uninstalling the SafeGuard Enterprise encryption software from endpoint computers involves the following steps:

■ Decrypt encrypted data.
■ Uninstall the encryption software.

The appropriate policies must be effective on the endpoint computers to allow for decryption and uninstallation.

15.2.1 Preventing uninstallation on the endpoints

To provide extra protection for endpoints, we recommend that you prevent local uninstallation of SafeGuard Enterprise on endpoints. In a Machine specific settings policy, set Uninstallation allowed to No and deploy the policy on the endpoints. Uninstallation attempts then are cancelled and the unauthorized attempts are logged.
15.2.2 Decrypt encrypted data

The following prerequisites must be met:

- To decrypt encrypted volumes, all volume-based encrypted volumes must have a drive letter assigned to them.

1. In SafeGuard Management Center, edit the current policy of the type Device Protection that is assigned to the computers you want to decrypt. Select the targets and set User may decrypt volume to Yes. Assign the policy to the respective endpoint computers.

2. Create a decryption policy of the type Device Protection, select the targets that are to be decrypted and set the Media encryption mode to No encryption.

3. In Users & Computers, create a group for the computers you want to decrypt: right-click and click New > Create new group.

4. Assign the decryption policy to the domain node of this group and activate it. In the Policies tab of the domain node, check that the priority is set to 1 and that No override is activated. Check that only members of this group will be affected by this policy using the Activation tab.

5. Add the computers you want to decrypt to this new group.

6. On the endpoint computer that is to be decrypted, synchronize with the SafeGuard Enterprise Server to make sure that the policy update has been received and is active.

7. Open Windows Explorer. Right-click the volume that should be decrypted and click Encryption > Decryption.

Make sure that the decryption is completed successfully.

Note: Endpoints can be shut down and restarted during encryption/decryption. If decryption is followed by an uninstallation, we recommend that the endpoint is not suspended or hibernated during decryption.

15.2.3 Start uninstallation

The following prerequisites must be met:

- Encrypted data has to be decrypted properly to be able to access it afterwards. The decryption process must be completed. Proper decryption is particularly important when uninstallation is triggered by Active Directory.

    Also, all encrypted removable media must be decrypted before uninstalling the last accessible SafeGuard Enterprise protected endpoint. Otherwise users may not be able to access their data any more. As long as the SafeGuard Enterprise database is available, data on removable media can be recovered.

- To uninstall SafeGuard Device Protection, all volume-based encrypted volumes must have a drive letter assigned to them.
Make sure that you always uninstall the complete package with all features installed.

1. In SafeGuard Management Center, edit the policy of the type **Machine-specific settings**. Set **Uninstallation allowed** to **Yes**.

2. In **Users & Computers**, create a group for the endpoints you want to uninstall: right-click and click **New > Create new group** or use the group you created for decrypting data.

3. Assign the uninstallation policy to the domain node of this group and activate it. In the **Policies** tab of the domain node, check that the priority is set to 1 and that **No override** is activated. Check that only members of this group will be affected by this policy using the **Activation** tab.

4. Add the endpoints you want to uninstall to the group.

5. To start uninstallation, use one of the following methods:
   - To uninstall locally on the endpoint, synchronize with the SafeGuard Enterprise Server to make sure that the policy update has been received and is active. Then select **Start > Programs > Control Panel > Add or Remove Programs > Sophos SafeGuard Client > Remove**.
   - To uninstall centrally use the software distribution mechanism of your choice. Make sure that all required data has been decrypted properly before uninstallation starts.
16 Technical support

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

- Visit the SophosTalk community at http://community.sophos.com/ and search for other users who are experiencing the same problem.
- Visit the Sophos support knowledgebase at http://www.sophos.com/support/.
- Download the product documentation at http://www.sophos.com/support/docs/.
- Send an email to support@sophos.com, including your Sophos software version number(s), operating system(s) and patch level(s), and the text of any error messages.
17 Legal notices

Copyright © 1996 - 2012 Sophos Group. All rights reserved. SafeGuard is a registered trademark of Sophos Group.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the documentation can be reproduced in accordance with the license terms or you otherwise have the prior permission in writing of the copyright owner.

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

You find copyright information on third party suppliers in the Disclaimer and Copyright for 3rd Party Software document in your product directory.