

SOPHOS

simple + secure

SafeGuard Enterprise Installation guide

Product version: 5.60

Document date: April 2011



Contents

1 SafeGuard Enterprise Overview	3
2 SafeGuard Enterprise components.....	4
3 Getting started.....	6
4 Setting up SafeGuard Enterprise Server.....	14
5 Setting up SafeGuard Enterprise Database.....	22
6 Setting up SafeGuard Management Center.....	31
7 Testing communication.....	43
8 Register and configure SafeGuard Enterprise Server.....	46
9 Setting up SafeGuard Enterprise on endpoint computers.....	50
10 Setting endpoint computers centrally.....	59
11 Setting up endpoint computers locally.....	70
12 Installing SafeGuard Enterprise on computers with multiple operating systems.....	72
13 Setting up SafeGuard Configuration Protection.....	74
14 Replicating the SafeGuard Enterprise Database.....	80
15 Updating SafeGuard Enterprise.....	85
16 Updating the operating system	92
17 Upgrading Sophos SafeGuard to SafeGuard Enterprise.....	93
18 Upgrading SafeGuard Easy 4.x/ Sophos SafeGuard Disk Encryption 4.x to SafeGuard Enterprise 5.6x.....	95
19 About uninstallation.....	102
20 Technical support.....	104
21 Legal notices.....	105

1 SafeGuard Enterprise Overview

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 is easy and intuitive to use. SafeGuard's own authentication system, Power-on Authentication (POA), provides the necessary access protection and offers user-friendly support when recovering credentials.

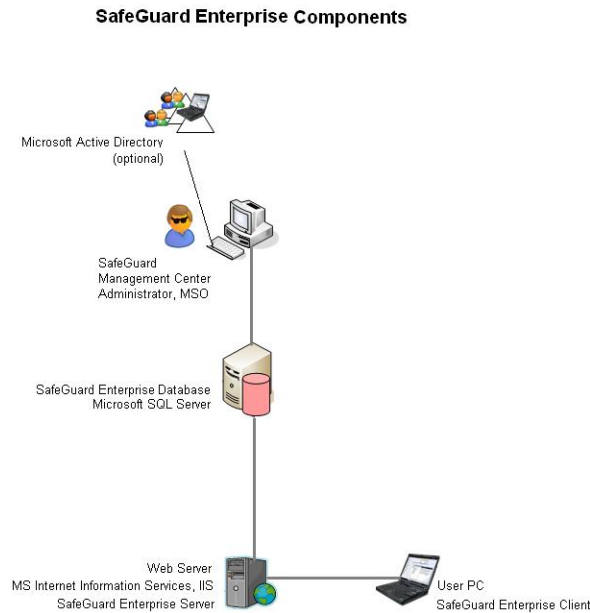
Note: Our video tutorials are an ideal way to learn about SafeGuard Enterprise. You can find them in your product delivery under Tutorials. They describe how SafeGuard Enterprise is installed and how to use the SafeGuard Management Center.

2 SafeGuard Enterprise components

In this chapter you will learn about the SafeGuard Enterprise components and how the individual components work with each other.

One or several Microsoft SQL databases store information about the endpoint computers 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 users' PCs/notebooks read the policies from the database and report successful execution to the database. The communication between the database and the endpoint computers 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:

Component	Description
SafeGuard Enterprise Database(s) based on Microsoft SQL Server Database	The SafeGuard Enterprise Database(s) hold all relevant data such as keys/certificates, information about users & 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

Component	Description
	Enterprise Databas(es) can be generated and configured using a wizard or scripts.
SafeGuard Enterprise Server on IIS based web server	Microsoft Internet Information Services (ISS) with .NET Framework 3.5 SP 1 and ASP.NET 2.0. The web server used for SafeGuard Enterprise must be based on Internet Information Services (IIS). We recommend that you use a dedicated IIS server for SafeGuard Enterprise Server. The IIS Server may be clustered.
	SafeGuard Enterprise Server interfaces between the SafeGuard Enterprise Database and the SafeGuard Enterprise endpoint computers. 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.
SafeGuard Management Center with .NET Framework 3.0 SP 1, ASP.Net 2.0 on administrator computer	Central management tool for SafeGuard Enterprise protected computers, managing keys and certificates, users & computers, and for creating SafeGuard Enterprise policies. The SafeGuard Management Center communicates with the SafeGuard Enterprise Database.
Directory Services (optional)	Import of an active directory. It holds the company's organizational structure with users and computers.
SafeGuard Enterprise Client on endpoint computers	Client software for authentication and data encryption on endpoint computers. The SafeGuard Enterprise Client (managed) communicates with the SafeGuard Enterprise Server. Additionally, standalone computers, Sophos SafeGuard Clients (standalone), that are never connected to a SafeGuard Enterprise Server, can be protected with SafeGuard Enterprise.

3 Getting started

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

- **First-time installation:** An installation wizard simplifies the first time setup of the management components including default policies. To launch this wizard for new SafeGuard Enterprise installations, start **SGNInstallAdvisor.bat** from the root directory of the product delivery.
- **Update installation:** Follow the steps described in this Help.

3.1 System requirements

For hardware and software requirements, service packs and disk space required during installation as well as for effective operation, see the system requirement page of the Sophos website (<http://www.sophos.com/products/enterprise/encryption/safeguard-enterprise/sysreqs.html>).

For specific requirements on endpoint computers, *see General Restrictions* (page 52).

3.2 Language settings

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

3.2.1 Setup wizard language

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.

3.2.2 SafeGuard Management Center language

To set the language of the SafeGuard Management Center inside the SafeGuard Management Center:

1. On the **Tools** menu, click **Options**, and then click **General**. Click **Use user defined language** and select an available language. English, German, French and Japanese are supported.
2. Restart the SafeGuard Management Center and it is displayed in the selected language.

3.2.3 SafeGuard Enterprise language on endpoint computers

To set the language of SafeGuard Enterprise on the endpoint computer, create a policy of the type **General Settings** in the SafeGuard Management Center and select the language in the field **Language used on client** under **Customization**:

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

3.3 Interaction with other SafeGuard products

Note the following interactions.

3.3.1 Compatibility with SafeGuard LAN Crypt

- SafeGuard LAN Crypt 3.7x and SafeGuard Enterprise 5.6x can coexist on the same computer and are fully compatible.

Note:

If SafeGuard Enterprise 5.6x 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 5.6x cannot coexist on the same computer.

If you try to install SafeGuard Enterprise 5.6x 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 are trying 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.

3.3.2 Compatibility with SafeGuard PrivateCrypto and SafeGuard PrivateDisk

SafeGuard Enterprise 5.6x and the standalone products SafeGuard PrivateCrypto (version 2.30 or later) and SafeGuard PrivateDisk (version 2.30 or later), can coexist on the same computer.

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

3.3.3 Compatibility with SafeGuard Removable Media

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

Local keys created with SafeGuard Removable Media older than version 1.20 before switching to SafeGuard Data Exchange can be used on the SafeGuard Enterprise Client. But they are not transferred to the SafeGuard Enterprise Database automatically.

3.3.4 Compatibility with SafeGuard Easy 4.x

SafeGuard Easy 4.x and SafeGuard Enterprise 5.6.x can be installed on the same computer as long as the SafeGuard Device Encryption module of SafeGuard Enterprise is not installed. Since both products install their own GINA (graphical identification and authentication), SafeGuard Enterprise will only work properly if its own GINA is used. To assure proper configuration, SafeGuard Easy 4.x has to be installed without GINA support (use the GINASY=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 5.6.x.

Note:

When SafeGuard Easy 4.x and the SafeGuard Data Exchange 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.

3.4 General security measures

The computers on which SafeGuard Enterprise Server, the SafeGuard Enterprise Database and the SafeGuard Management Center are running should be protected against unauthorized local attack. The following are a few practical measures that should be taken:

- Only use trusted administrators, or apply "two person rule".
- Protect against electronic attacks (firewalls, secure configuration, virus scanner, regular updates, robust passwords etc.).
- Protect against physical access (for example secure rooms).

3.5 Securing transport connection 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 Client (managed) may either be secured by SSL or by SafeGuard specific encryption. The advantage of SSL is that it is a standard protocol and that a faster connection can be achieved as with using SafeGuard transport encryption.

Note:

We strongly recommend that you use SSL encrypted communication between SafeGuard Enterprise Server and the SafeGuard Enterprise Client, except for demo or test setups. If, for some reason, this is not possible and proprietary SafeGuard encryption must be used, there is an upper limit of 1000 clients that connect to a single server instance.

SSL encryption for SafeGuard Enterprise can be set during configuration of the SafeGuard Enterprise components directly after installation. It is also possible to enable it afterwards at any time. There is no need to reinstall the components, if SSL is enabled later on. Merely a new configuration package needs to be created and deployed on the respective server or client.

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

3.5.1 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://msdn2.microsoft.com/en-us/library/ms998300.aspx>
- <http://support.microsoft.com/default.aspx?scid=kb;en-us;316898>
- https://blogs.msdn.com/sql_protocols/archive/2005/11/10/491563.aspx

3.5.2 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 33) or see: <http://www.sophos.com/support/knowledgebase/article/109012.html>.
- 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 33).
- Connection between SafeGuard Enterprise Server and the SafeGuard Enterprise protected endpoint computer:

Activate SSL encryption when creating the configuration package for the SafeGuard Enterprise Client (managed) in the SafeGuard Management Center Configuration Package Tool, *see [Create a SafeGuard Enterprise \(managed\) configuration package](#)* (page 57).

3.6 Installation steps for SafeGuard Enterprise

To install SafeGuard Enterprise follow these installation steps.

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

Note:

For most Client installation packages, 64 bit versions are available for Windows 7 64 bit and Windows Vista 64 bit operating systems (<package name>_64 .msi). If the operating system of the endpoint computer is Windows 7 64 bit or Windows Vista 64 bit, you can install the 64 bit variant of the "Client" .msi packages.

No.	Step	Installation/configuration
1	Prepare for installations.	
SafeGuard Enterprise Server		
2	Set up Internet Information Services (IIS) for SafeGuard Enterprise with .NET Framework 3.5 and ASP.NET 2.0.	
3	Additional configuration for SSL.	
4	Install SafeGuard Enterprise Server on the IIS web server.	SGNServer.msi

No.	Step	Installation/configuration
SafeGuard Enterprise Database		
5	Set up authentication for the SafeGuard Enterprise Master Security Officer. The user account is created for Microsoft SQL Server.	
6 (optional)	Generate the SafeGuard Enterprise Database(s) with a script.	SQL scripts in product delivery, in Tools directory
SafeGuard Management Center		
7	Set up SafeGuard Management Center for central administration (domains, users, keys, policies, etc.).	SGNManagementCenter.msi
8	Basic configuration of administration: Configure the database connections, generate the SafeGuard Enterprise Database(s) and the Master Security Officer.	SafeGuard Management Center Initial Configuration Wizard
9	Register and configure SafeGuard Enterprise Server: Create server configuration package and deploy it on the web server.	Server configuration package: SafeGuard Management Center Configuration Package Tool
10	Create or import organizational structure from Active Directory.	SafeGuard Management Center
SafeGuard Enterprise Client		
11	Install mandatory pre-installation package to prepare endpoint computers for successful installation.	SGxClientPreinstall.msi
12	Install one of the following encryption software packages on the endpoint computers:	
	SafeGuard Device Encryption: <ul style="list-style-type: none"> ■ volume-based encryption ■ file-based encryption (SafeGuard Data Exchange) Valid for both SafeGuard Enterprise Clients (managed) and Sophos SafeGuard Clients (standalone).	SGNClient.msi SGNClient_x64.msi
	SafeGuard Data Exchange: <ul style="list-style-type: none"> ■ file-based encryption ■ without Power-on Authentication Valid for both SafeGuard Enterprise Clients (managed) and Sophos SafeGuard Clients (standalone). Not available for BitLocker Device Encryption support.	SGNClient_withoutDE.msi SGNClient_withoutDE_x64.msi
13 (optional)	Additionally install SafeGuard Configuration Protection: Port protection and management of	SGN_CP_Client.msi

No.	Step	Installation/configuration
	peripheral devices on endpoint computers. Only valid for SafeGuard Enterprise Clients (managed); not available for Sophos SafeGuard Clients (standalone).	
14	Configure endpoint computers: Generate configuration package for managed or standalone endpoint computers and install it on the endpoint computers.	Configuration package: SafeGuard Management Center Configuration Package Tool

3.7 Installation steps for SafeGuard Enterprise Client on multiple operating systems (runtime system)

The so-called Runtime Client 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 SafeGuard Enterprise Clients (managed) and Sophos SafeGuard Clients (standalone).

Note:

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

Only the SafeGuard Device Encryption installation package can be used. The Runtime Client cannot be operated with SafeGuard Data Exchange only. When the operating system of the endpoint computer is Windows 7 64 bit or Windows Vista 64 bit, you may install the 64 bit variant of the "Client" .msi packages.

To install SafeGuard Enterprise Client on multiple operating systems, follow these installation steps:

No.	Step	Description	Installation/configuration
1	Set up the Runtime system on the endpoint computer.	Install the SafeGuard Client runtime package on the secondary boot volume(s) of the endpoint computer.	SGNClientRuntime.msi SGNClientRuntime_x64.msi
2	Set up the SafeGuard encryption software on the endpoint computers.	Provide endpoint computers with necessary requirements for successful installation of the encryption software (mandatory).	SGxClientPreinstall.msi

No.	Step	Description	Installation/configuration
		Install the SafeGuard Device Encryption installation package on the primary boot volume of the endpoint computer.	SGNClient.msi SGNClient_x64.msi
3	Configure the endpoint computers.	Generate configuration package for managed or standalone endpoint computers and install it on the endpoint computers.	SGNClientConfig.msi Client configuration package generated in the SafeGuard Management Center Configuration Package Tool

3.8 Prepare for installation

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

- Make sure that you have Windows administrator rights.
- Close all open applications.
- Check the system requirements, <http://www.sophos.com/products/enterprise/encryption/safeguard-enterprise/sysreqs.html>.
- Read the release notes.

For preparations on the endpoint computer, *see Prepare for encryption* (page 54).

3.8.1 Download installers

1. Go to <https://secure.sophos.com/support/updates/>.
2. Type your MySophos username and password.
3. On the web page for **Data Protection** downloads, click **SafeGuard Enterprise** and download the SafeGuard Enterprise installers and documentation.
4. Store them in a location where you can access them for installation.

4 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).

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 on IIS. You first have to install and configure Microsoft Internet Information Services (IIS).

4.1 Prerequisites

The following prerequisites must be met:

- You need Windows administrator rights.
- Microsoft Internet Information Services (IIS) must be available.

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

- 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 connection with SSL](#)* (page 9).

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.

- .NET Framework 3.5 Service Pack 1 must be available to you.

You find the program in the SafeGuard Enterprise product delivery.

- ASP.NET Version 2.0.50727 must be available to you.

You find the program your Windows DVD, for example. Depending on the Windows version it may have already been installed by default. You can also download it: <http://www.asp.net/>. ASP.NET is available free of charge.

4.2 Installing and configuring Microsoft Internet Information Services (IIS)

The chapter 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

4.2.1 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>.

4.2.1.1 Check .NET Framework installation and registration

.NET Framework version 3.5 SP 1 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 3.5 SP 1 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 "v3.5".

4.2.1.2 Check ASP.NET registration on IIS 6

ASP.NET Version 2.0.50727 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 2.0.50727 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 2.050727 is installed.
4. To check that the correct version is installed, enter **aspnet_regiis.exe -lv** at the command prompt.

2.0.50727 should be displayed as ASP.NET version.

4.2.1.3 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\v2.0.50727\aspnet_regiis.exe -i
3. To activate the 32 bit version of ASP.Net 2.0.50727, 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 v2.0.50727 (32 bit)**, click **Properties** and set the status to **Allowed**.
6. Click **Apply**, and then **OK**.

4.2.1.4 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.

4.2.2 Install and configure IIS 7 on Microsoft Windows Server 2008

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 all necessary sub-role services. Then select **.NET Extensibility, ISAPI Extensions, ISAPI Filters**.
7. Select **IIS Management Scripts and Tools** that is needed for correct IIS 7 configuration.
8. Click **Next**, then **Install** and then **Close**,

IIS 7 is installed with a default configuration for hosting ASP.NET on Windows Server 2008.

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

4.2.2.1 Check .NET Framework registration on IIS 7

.NET Framework version 3.5. SP 1 is required.

1. To check that .NET Framework is installed and registered with the correct version, *see Check .NET Framework installation and registration* (page 15).

4.2.2.2 Check ASP.NET registration on IIS 7

ASP.NET Version 2.0.50727 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.
2.0.50727 should be displayed as ASP.NET version.

4.2.3 Enable memory recycling

We recommend that you enable **Recycle worker processes** on IIS 6/IIS 7.

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/IIS 7.

4.3 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:

You find detailed information on Web Server hardening in Microsoft Solutions for Security and Compliance: Windows Server 2003 Security Guide which can be downloaded for free from the Microsoft web site.

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

4.3.1 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

4.3.2 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 **Prohibited**
- ASP.NET v.2.50727 **Allowed**

4.3.3 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.

4.3.4 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:

User/Folder	NTFS permissions for E:\inetpub	NTFS permissions for F:\mycompany.web
Administrators	full control	full control
System	full control	full control
Users	execute	execute

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_SRVERNAME on the IIS server accordingly.

The NTFS permissions for file types are as follows:

File type	Recommended NTFS permissions
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)
Static content (.txt, .gif, .jpg, .htm, .html)	Administrators (full control) System (full control) Everyone/User (read-only)

4.3.5 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.

4.3.6 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.

4.4 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. Start **SGNServer.msi**.
2. On the **Welcome** page, click **Next**.
3. Accept the license agreement.
4. Accept the default installation path.
5. Click **Finish** to complete the installation.

SafeGuard Enterprise Server is installed.

Note:

To enhance performance, the concatenation of logged events is deactivated for the SafeGuard Enterprise Database by default after installation of SafeGuard Enterprise Server. However, without concatenation no integrity protection is provided for logged events. Concatenation 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 concatenation manually. For further information, see the Administrator Help, chapter *Reports*.

5 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](#).

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 80).

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 33).

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 time intervals, for example every week or every day.

5.1 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 9).

5.1.1 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 the 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.

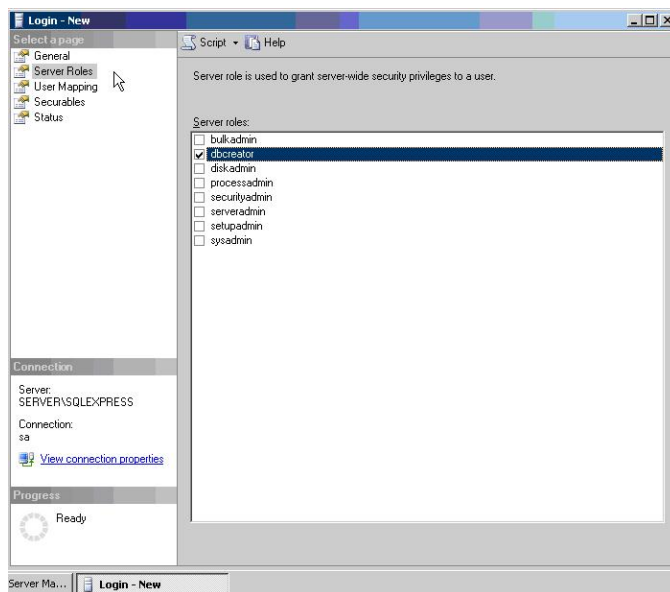
Access Right	SQL Server 2005, SQL Server 2005 Express	SQL Server 2008, SQL Server 2008 Express
Create database		
Server	db_creator	db_creator
Master database	None	None
SafeGuard Enterprise Database	db_ownerpublic (default)	db_ownerpublic (default)
Use database		
Server	None	None
Master database	None	None
SafeGuard Enterprise Database	db_datareaderdd b_datawriter public (default)	db_datareader db_datawriter public (default)

5.1.2 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 Edition. For information on Windows authentication with Windows Server 2003 and SQL server 2005, see: <http://www.sophos.com/support/knowledgebase/article/108339.html>

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**.



5.1.3 Create an SQL account for SQL server logon

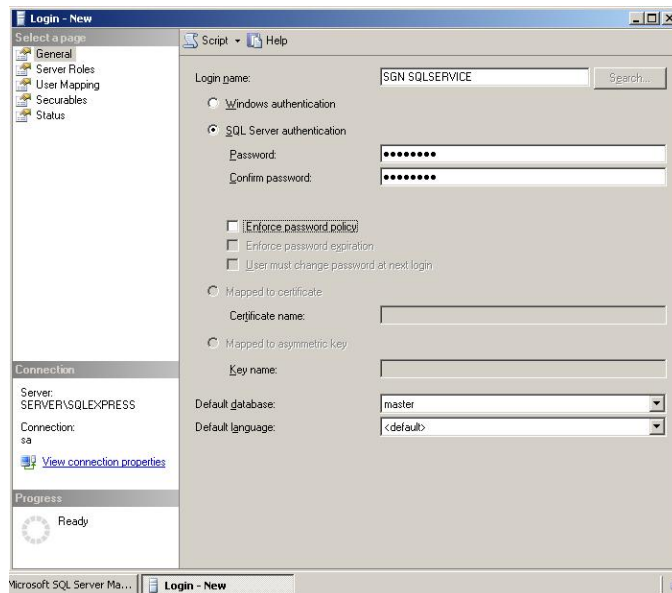
The description of the individual configuration steps below is aimed at SQL administrators. It relates to Microsoft Windows Server 2003 with Microsoft SQL Server 2005 and Microsoft Windows Server 2008 all editions with Microsoft SQL Server 2008 Standard Edition.

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

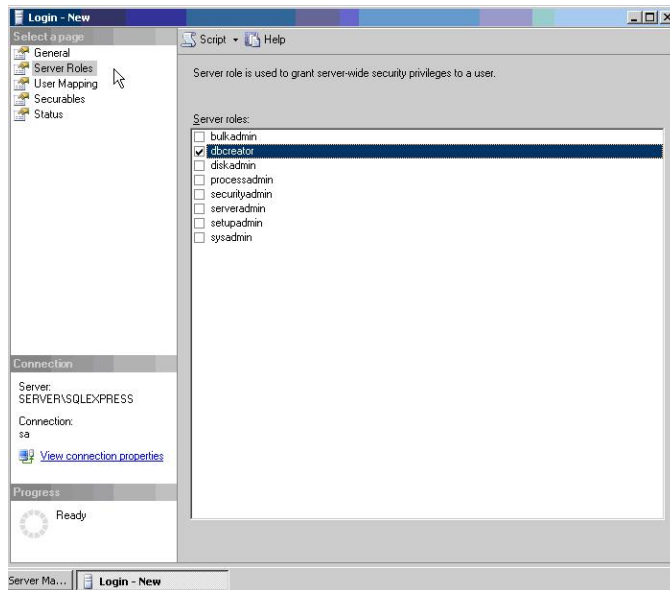
1. Open SQL Server Management Studio. Log on to the SQL Server with your credentials.
2. Open the **Object Explorer**, right-click **Security**, point to **New** and then click **Logins**.

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**.



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

5.2 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:

- in the 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 31) and then continue with changing the relevant access rights, [see *Change access rights for the SafeGuard Enterprise Database*](#) (page 27).

- with SQL scripts provided with 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.

5.2.1 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 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 to start the **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 are created.

5.3 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 required for connecting to the SafeGuard Enterprise Database are described.

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 select **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**.

5.4 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 **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 select **Enabled**.
6. Right-click the protocol **TCP/IP** and select **Enabled**.
7. Additionally, right-click the protocol **TCP/IP** and select **Properties**. In the **IP Addresses** tab, under **IPAll**, leave **TCP Dynamic Ports** blank. Set **TCP Port** to 1433.
8. Restart the SQL Services.

5.5 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**.
6. On the **Protocol and Ports** page, select **TCP** as **Protocol type**. For **Local port**, select **Specific Ports** and enter **1433**. For **Remote Port**, select **All Ports**. 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**.

5.6 Carry out further configuration when using a Windows account for SQL server logon

The description relates to Microsoft Windows Server 2008 with Microsoft SQL Server 2008 Standard Edition and IIS 7. For information on Windows authentication with Windows Server 2003 and SQL server 2005, see: <http://www.sophos.com/support/knowledgebase/article/108339.html>

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: Create files / write data, Delete, and Read permissions**.
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.
14. In **Application Pool Identity**, select **Custom account** and click **Set**.
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**.
19. Right click **Anonymous authentication** and select **Edit**.
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.

6 Setting up SafeGuard Management Center

This chapter 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 does not necessarily need to be installed on one computer only. It 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.

6.1 Prerequisites

The following prerequisites must be met:

- Make sure that you have Windows administrator rights.
- .NET Framework 3.0 Service Pack 1 is installed.
.NET Framework is available free of charge. You may find the program on your Windows DVD, for example. Depending on the Windows version it may have already been installed by default. You can also download it: <http://microsoft.com/downloads>.
- If you want to create a new SafeGuard Enterprise Database during SafeGuard Management Center configuration, you need the necessary SQL access rights, *see Database access rights* (page 22).

6.2 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. In the welcome window, click **Next**.
3. Accept the license agreement.
4. Accept the default installation path.
5. Select the installation type:
 - For the SafeGuard Management Center to support one database only, select **Typical**.
 - For the SafeGuard Management Center to support multiple databases (**Multi Tenancy**), select **Complete**. For further information, *see Multi Tenancy configurations* (page 33).
6. Click **Finish** to complete the installation.

The SafeGuard Management Center is installed. If necessary, restart your computer. Next you carry out initial configuration in the SafeGuard Management Center.

6.3 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.

- Windows 2003 Server Enterprise Edition- Internet Explorer 6 - Enhanced Security Configuration (default installation configuration):

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.

6.4 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.

6.4.1 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.

6.4.2 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.

6.4.3 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**.

6.4.4 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 connection with SSL](#)* (page 9).

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 23) and *see [Carry out further configuration when using a Windows account for SQL server logon](#)* (page 29).

- 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.

6.4.5 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**.

6.4.6 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.

6.4.6.1 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 (<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.

6.4.6.2 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 (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*.

6.4.6.3 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.

6.4.7 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.

1. On the **Company Certificate** page, select **Create a new company certificate**.
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 42).

6.4.8 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.

6.5 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 33).

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*.

6.6 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.

6.7 Logon to the SafeGuard Management Center

Logon to the 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.

6.7.1 Log on in Single Tenancy mode

1. Start the 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**.

The 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.

6.7.2 Log on in Multi Tenancy mode

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

1. Start the 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 from the list and click **OK**. The selected database configuration is connected to the 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**.

The 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.

6.8 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 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 a mixture of them both. 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*.

6.9 Importing the license file

SafeGuard Enterprise has an integrated license counter. By default a fixed number of 5 licenses for every available SafeGuard Enterprise module is part of the installation. This should enable the evaluation of other SafeGuard Enterprise modules easily without any side effects. However, 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*.

6.10 Restore a corrupt SafeGuard Management Center installation

If the installation of the SafeGuard Management Center is corrupted but the database is still intact, the installation can be easily restored by installing the SafeGuard Management Center afresh and 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. In **Database Connection**, select the relevant database server and configure the connection to the database if required. Click **Next**.
3. In **Database Settings** click **Select an available database** and select the relevant database from the list.
4. In **Security Officer Data**, do either 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 the 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 a password for authenticating at the SafeGuard Management Center.
5. Click **Next**, and then **Finish** to complete the SafeGuard Management Center configuration.

The corrupt SafeGuard Management Center installation is restored.

6.11 Restore a corrupt database configuration

A corrupt database configuration can be restored by installing the 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. It avoids having to set up and restore the whole database afresh.

- 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. For further information, see the Administrator Help.
- The passwords for the two .p12 files as well as for the certificate store must be known to you.

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. In **Database Connection**, select **Create a new database**. Under **Database settings**, configure the connection to the database. Click **Next**.
3. In **Security Officer Data**, 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. In **Company Certificate**, 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.

7 Testing communication

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

7.1 Prerequisites

Make or check the following settings before the connection test.

7.1.1 Ports/connections

The endpoint computers must create the following connections:

SafeGuard Client connection to	Port
SafeGuard Enterprise Server	Port 80/TCP Port 443 when using SSL transport connection

The SafeGuard Management Center must create the following connections:

SafeGuard Management Center connection to	Port
SQL database	SQL Server 2005/SQL Server 2008 dynamic port: Port 1433/TCP and Port 1434/TCP
Active Directory	Port 389/TCP
SLDAP	Port 636 for the Active Directory import

The SafeGuard Enterprise Server must create the following connections:

SafeGuard Enterprise Server connection to	Port
SQL database	Port 1433/TCP and Port 1434/TCP for SQL 2005 (Express) dynamic port
Active Directory	Port 389/TCP

7.1.2 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**.
4. Click the **Directory Security** tab.
5. Under **Authentication and Access Control**, click **Edit**. In **Authentication Methods**, select **Enable anonymous access**. Under **Authenticated access**, clear **Integrated Windows authentication**.

7.1.3 Proxy server settings for web server and endpoint computer

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**.

7.1.4 Microsoft SQL Server 2005 settings

When using Microsoft SQL Server 2005, set the following:

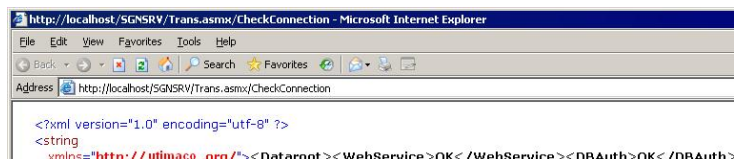
1. Open Microsoft SQL Server Management Studio.
2. In the left hand pane of the **Object Explorer**, browse to **Security**.
3. Right-click **Logins** and click **New Login**. Add the following user in Microsoft SQL Server Management Studio (Role "sysadmin"): **NT AUTHORITY\NETWORK SERVICE**.

7.2 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:

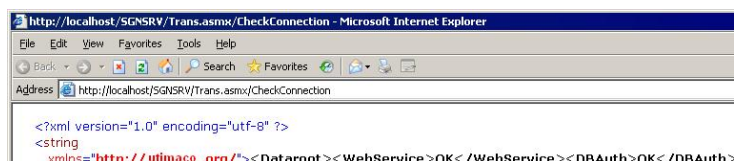


```
<?xml version="1.0" encoding="utf-8" ?>
<string
  xmlns="http://utilmaco.org/"><Dataroot><WebService>OK</WebService><DBAuth>OK</DBAuth
```

7.3 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:



```
<?xml version="1.0" encoding="utf-8" ?>
<string
  xmlns="http://utilmaco.org/"><Dataroot><WebService>OK</WebService><DBAuth>OK</DBAuth
```

8 Register and configure SafeGuard Enterprise Server

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

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 use on the current computer

After 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 the SafeGuard Management Center.
2. On the **Tools** menu, click **Configuration Package Tool**.
3. Select the **Register Server** tab and then select **Make this computer an SGN Server**.
4. Select **Register Server** 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 **Register Server** 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 use on a different computer

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

1. Start the SafeGuard Management Center.
2. On the **Tools** menu, click **Configuration Package Tool**
3. Select **Register Server** 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.edu** and certificate information is displayed.

Note:

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

5. Click **OK**.

The server information is displayed in the **Register Server** tab.

6. Click the **Create Server Configuration Package** 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 **Register Server** 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 **Register Server** 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 Change the SafeGuard Enterprise Server configuration settings

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

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

Element	Description
Scripting allowed	Click to enable use of the SafeGuard Enterprise Management API. This allows for scripting administrative tasks.
Server roles	Click to select/deselect an available security officer role for the selected server.
Add server role...	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 Server roles .
Database connection	<p>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, <i>see Configure the database server connection</i> (page 33). Even if the database connection check has not been successful, a new server configuration package can be created.</p> <p>Note:</p> <p>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. After the updated server package is installed on the server, the new database connection can be used.</p>

3. Create a new server configuration package in the **Create Server Configuration Package** 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 Client 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 use on a different computer](#)* (page 47).

9 Setting up SafeGuard Enterprise on endpoint computers

SafeGuard Enterprise can be seamlessly integrated into the user's normal environment and is easy and intuitive to use. According to your deployment strategy, the endpoint computers 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 computers.

9.1 SafeGuard configurations for endpoint computers

Endpoint computers can be configured as follows:

■ SafeGuard Enterprise Clients (managed)

Central server-based management in the SafeGuard Management Center.

For SafeGuard Enterprise Clients (managed) 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 computer is defined as managed.

■ Sophos SafeGuard Clients (standalone)

Local management in the SafeGuard Management Center.

Sophos SafeGuard Clients (standalone) are never connected to the SafeGuard Enterprise Server any time and is not connected to the central management of SafeGuard Enterprise. It operates in standalone mode.

The most significant difference to SafeGuard Enterprise Clients (managed) is that Sophos SafeGuard Clients (standalone) only 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 endpoint computers.

9.1.1 Installation packages for SafeGuard Enterprise Clients (managed)

Note:

When the operating system of the endpoint computer is Windows 7 64 bit or Windows Vista 64 bit, you may install the 64 bit variant of the “Client” installation packages (<package name>_x64.msi). The 64 bit package of the Configuration Protection Client is available for Windows 7 64 bit.

The following table shows the available installation packages for SafeGuard Enterprise Clients (managed).

Package	Description
SGxClientPreinstall.msi	Must be installed on the endpoint computers before the encryption software (mandatory). Provides endpoint computers with necessary requirements for successful installation of the encryption software.
SGNClient.msi SGNClient_x64.msi	For native SafeGuard Enterprise Clients and for SafeGuard Enterprise Clients with BitLocker support. SafeGuard Enterprise Device Encryption Volume-based encryption with Power-on Authentication SafeGuard Data Exchange Easy data exchange with removable media on all platforms without re-encryption File-based encryption
SGNClient_withoutDE.msi SGNClient_withoutDE_x64.msi	For SafeGuard Enterprise Clients with BitLocker support this package is not available. SafeGuard Data Exchange Easy data exchange with removable media on all platforms without re-encryption File-based encryption without Power-on Authentication
SGN_CP_Client.msi SGN_CP_Client_x64.msi	For native SafeGuard Enterprise Clients and for SafeGuard Enterprise Clients with BitLocker support. The 64 bit variant of this package is available for Windows 7 64 bit operating systems. Configuration Protection Port protection and management of peripheral devices
SGNClientRuntime.msi SGNClientRuntime_x64.msi	Runtime Client enabling starting the computer from a secondary boot volume when multiple operating systems are installed. Accessing these volumes when they are encrypted by a SafeGuard Enterprise installation on the primary volume.

9.1.2 Installation packages for Sophos SafeGuard Clients (standalone)

Note:

When the operating system of the endpoint computer is Windows 7 64 bit or Windows Vista 64 bit, you may install the 64 bit variant of the “Client” installation packages (<package name>_x64.msi).

The following table shows the available installation packages for Sophos SafeGuard Clients (standalone).

Package	Description
SGxClientPreinstall.msi	Must be installed on the endpoint computers before the encryption software (mandatory). Provides endpoint computers with necessary requirements for successful installation of the encryption software.
SGNClient.msi SGNClient_x64.msi	SafeGuard Enterprise Device Encryption Volume-based encryption with Power-on Authentication SafeGuard Data Exchange Easy data exchange with removable media on all platforms without re-encryption File-based encryption
SGNClient_withoutDE.msi SGNClient_withoutDE_x64.msi	SafeGuard Data Exchange Easy data exchange with removable media on all platforms without re-encryption File-based encryption without Power-on Authentication
SGNClientRuntime.msi SGNClientRuntime_x64.msi	Runtime Client enabling starting the computer from a secondary boot volume when multiple operating systems are installed. Accessing these volumes when they are encrypted by a SafeGuard Enterprise installation on the primary volume.

9.2 Restrictions

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

9.2.1 General Restrictions

Note the following general restrictions for SafeGuard Enterprise Clients:

- 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 computer, 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 not located on Dynamic and GUID partition table (GPT) disks is not supported. In such cases, the installation is terminated. If such disks are found on the computer at a later time, they are not supported.
- The SafeGuard Enterprise Device Encryption module does not support systems that are equipped with hard disks attached through a SCSI bus.

9.2.2 Restrictions for SafeGuard Enterprise Clients (managed)

Note the following restrictions for initial encryption of managed clients.

- Restrictions for initial encryption:

Initial configuration of SafeGuard Enterprise Clients (managed) may involve the creation of encryption policies that may be distributed inside a configuration package to the SafeGuard Enterprise Clients.

However, when the SafeGuard Enterprise Client 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 on the SafeGuard Enterprise Client:

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 Client, the respective configuration package has to be reassigned to the client's organizational unit as well. The user-defined keys are then only created after the SafeGuard Enterprise Client is connected to SafeGuard Enterprise Server again.

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

- Restrictions for support of BitLocker Device Encryption:

Installation packages SGNClient_withoutDE.msi/SGNClient_withoutDE_x64.msi are not available for use with BitLocker Device Encryption.

Note:

Either SafeGuard Enterprise volume-based encryption or BitLocker Device 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 the partitions, uninstall the SafeGuard Enterprise Client installation package, 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.

9.2.3 Restrictions for Sophos SafeGuard Clients (standalone)

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

- BitLocker Device Encryption, BitLocker To Go
- Configuration Protection

9.3 Prepare for encryption

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

- Carry out the general preparations, *see [Prepare for installation](#)* (page 13).
- A user account must be set up and active on the endpoint computers.
- Create a full backup of the data on the endpoint computer.
- Sophos provides a hardware configuration list to minimize the risk of conflicts between the POA and your computer hardware. The list is contained in the encryption software installation package.

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: <ftp://POACFG:POACFG@ftp.ou.utimaco.de>

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> and <http://www.sophos.com/support/knowledgebase/article/65700.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 computer and run **chkdsk** again. For further information, see: <http://www.sophos.com/support/knowledgebase/article/107799.html>

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

Windows XP: Select **Application, Winlogon**.

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

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

- If you have used an imaging/cloning tool, we recommend that you rewrite the MBR. To install Sophos SafeGuard you need a clean, unique master boot record. By using imaging/cloning tools the master boot record might no longer be clean.

You can clean the master boot record by starting from a Windows DVD and using the command **FIXMBR** within the Windows Recovery Console. For further information, see:

<http://www.sophos.com/support/knowledgebase/article/108088.html>

- If the boot partition has been converted from FAT to NTFS and the system has not yet been restarted, do not install SafeGuard Enterprise. The installation might not be completed because the file system was still FAT at the time of installation, while NTFS was found when it was activated. In this case you have to restart the computer once before SafeGuard Enterprise is installed.
- 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 endpoint computers: <http://<ServerIPAddress>/sgnsrv>. If the **Trans** page shows **Check Connection**, connection to SafeGuard Enterprise Server is successfully established. For further information, see *Test the connection (IIS 6 on Windows Server 2003)* (page 44).

9.3.1 Specific preparations for BitLocker Drive Encryption support

Note:

You should decide before the installation whether you want to use SafeGuard Enterprise in combination with BitLocker Drive Encryption or SafeGuard Enterprise native volume-based encryption.

The installation is aborted if you try to install both at the same time.

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

- Windows Vista Enterprise or Ultimate or Windows 7 must be installed on the endpoint computer.
- 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 Device 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:

<http://technet2.microsoft.com/WindowsVista/en/library/c61f2a12-8ae6-4957-b031-97b4d762cf311033.mspx?mfr=true>

■ BitLocker FAQ

<http://technet2.microsoft.com/WindowsVista/en/library/58358421-a7f5-4c97-ab41-2bcc61a58a701033.mspx?mfr=true>

9.3.2 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 About creating configuration packages

Depending on the required configuration, create specific configuration packages for the endpoint computers in the SafeGuard Management Center:

- For SafeGuard Enterprise Clients (managed)
- For Sophos SafeGuard Clients (standalone)
- When using service accounts for post-installation task

9.4.1 Create a SafeGuard Enterprise (managed) configuration package

1. In the SafeGuard Management Center, on the **Tools** menu, click **Configuration Package Tool**.
2. Select **Create Configuration Package (managed)**.
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 absolutely essential).
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 Set up SSL* (page 9).

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 SafeGuard Enterprise Client (managed) endpoint computers and deploy it on them.

9.4.2 Create a Sophos SafeGuard (standalone) configuration package

1. In the SafeGuard Management Center, on the **Tools** menu, click **Configuration Package Tool**.
2. Select **Create Configuration Package (standalone)**.
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: `\\networkcomputer\`, 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 help desk. Alternatively, the files can be provided to the help desk 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 access account group to be assigned to the endpoint computer. POA access accounts offer access for administrative tasks on the endpoint computer after the Power-on Authentication has been activated. To assign POA access accounts, 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 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 computers 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 computer 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 computer.
- After restarting the computer, a rollout operator included on a service account list logs on to the endpoint computer using the windows logon prompt.
- According to the service account list applied to the computer 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 computer after the encryption software is installed. For further information, see the Administrator Help.

10 Setting endpoint computers centrally

Setting up endpoint computers centrally ensures a standardized installation on multiple endpoint computers.

Installation and configuration is described for SafeGuard Enterprise Clients (managed) as well as for Sophos SafeGuard Clients (standalone). The installation procedure is identical except that you assign a different configuration package for each of them.

The tasks required for an installation of endpoint computers with Windows BitLocker Device Encryption are described as well. For details on preparing for BitLocker support, [see *Specific preparations for BitLocker Drive Encryption support*](#) (page 55).

The behavior of the endpoint computers when first logging on after installing SafeGuard Enterprise and the activation of the Power-on Authentication is described in the User Help.

Note:

Within central software distribution the installation and configuration packages must only be assigned to a computer, they cannot be assigned to a user.

10.1 Install the encryption software centrally

1. Prepare for installation on the endpoint computers, [see *Prepare for encryption*](#) (page 54).

- 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:

Element	Description
Preparatory installation package SGxClientPreinstall.msi	The package provides the endpoint computers with the necessary requirements for a successful installation of the encryption software, for example the required DLL MSVCR80.dll , version 8.0.50727.4053. Note: If this package is not installed, installation of the encryption software is aborted.
Encryption software installation package	For available packages for managed clients, <i>see Installation packages for SafeGuard Enterprise Clients (managed)</i> (page 50). For available packages for standalone clients, <i>see Installation packages for Sophos SafeGuard Clients (standalone)</i> (page 51).
Configuration package for endpoint computers	Use the configuration packages created beforehand in the SafeGuard Management Center. Different configuration packages need to be installed for managed and standalone endpoint computers, <i>see About creating configuration packages</i> (page 56). Before installing a new configuration package make sure that you uninstall any outdated ones.
Script with commands for pre-configured installation	We recommend that you use the Windows Installer command-line tool msiexec to create the script. For further information, <i>see Command for central installation</i> (page 61) or http://msdn.microsoft.com/en-us/library/aa367988(VS.85).aspx .

- Create a folder **called Software** to use as a central store for all applications.
- To create the script, open a command prompt, and then type the scripting commands.
- Distribute this package to the endpoint computers using company software distribution mechanisms.

The package is executed on the endpoint computers. The endpoint computers are then ready for use of SafeGuard Enterprise.

- After installation, restart the endpoint computers twice to activate the Power-on-Authentication. Restart the computer for a third time to perform a backup of the kernel data on every Windows boot. This backup would never happen if the endpoint computer is only hibernated or transferred into stand-by mode. Ensure that the computer does not move into hibernation or stand-by mode but is restarted for a third time to backup the kernel.

Additional configuration may be required to ensure that the Power-on Authentication (POA) functions correctly on each hardware platform. Most hardware conflict issues can be resolved using the **Hotkeys** built into the POA. Hotkeys can be configured after installation in the POA 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>

10.2 Command for central installation

When you install SafeGuard Enterprise on the endpoint computers centrally, use the Windows Installer component **msiexec**. **msiexec** is included in Windows XP, Vista and Windows 7, and it automatically carries out a pre-configured SafeGuard Enterprise installation. As source and destination for the installation can also be specified, a standard installation on multiple endpoint computers is provided.

For further information, see: [http://msdn.microsoft.com/en-us/library/aa367988\(VS.85\).aspx](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, volume-based encryption.
- Sophos SafeGuard parameters, to specify the installation directory, for example.

Command options

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

Option	Description
<code>/i</code>	Specifies the fact that this is an installation.
<code>/qn</code>	Installs with no user interaction and does not display a user interface.

Option	Description
ADDLOCAL=	Lists the features that are to be installed. If the option is not specified, all features intended for a standard installation are installed. Note the following: Separate the features by comma, not by space. Observe upper and lower case. Add all feature parents of the selected feature to the command line.
ADDLOCAL=ALL	Installs all available features
REBOOT=Force ReallySuppress	Forces or suppresses a restart after installation. If nothing is specified, the restart is forced after installation.
/L* <path + filename>	Logs all warnings and error messages in the specified log file. The parameter /Le <path + filename> only logs error messages
InstallDir= <directory>	Specifies the directory in which the SafeGuard Enterprise Client is to be installed. If no value is specified, the default installation directory is <SYSTEM>:\PROGRAM FILES\SOPHOS.

10.3 SafeGuard Enterprise features (ADDLOCAL)

For a central installation, you must define in advance which Sophos SafeGuard features are to be installed on the endpoint computers. List the feature after typing the option **ADDLOCAL** in the command.

Note:

Even if it is possible to only install a subset of features in a first-time installation, we recommend that you install the Device Encryption feature (volume-based encryption) from the start.

You should decide before the installation whether you want to use SafeGuard Enterprise in combination with BitLocker Device Encryption or native SafeGuard Enterprise encryption only.

The following tables list the SafeGuard Enterprise features that can be installed on the endpoint computers. For further information, see:

<http://www.sophos.de/support/knowledgebase/article/108426.html>.

10.3.1 Features for SafeGuard Device Encryption

Note:

You must list the features **Client** and **Authentication** by default. If you select a feature, you also need to add the feature parents to the command line!

Feature Parents	Feature
Client	<p>Authentication</p> <p>You must state the feature Authentication and its parent feature Client by default.</p>
Client, Authentication	<p>CredentialProvider</p> <p>For computers with Windows Vista, Windows 7 you must select this feature. It enables logon with the Credential Provider.</p>
Client, BaseEncryption	<p>SectorBasedEncryption</p> <p>Installs SafeGuard Enterprise volume-based encryption with the following features:</p> <p>Any volumes, including removable media, can be encrypted with SafeGuard Enterprise volume-based encryption.</p> <p>SafeGuard Enterprise Power-on Authentication (POA)</p> <p>SafeGuard Enterprise Recovery with Challenge/Response</p> <p>Note:</p> <p>Either SectorBasedEncryption OR BitLockerSupport can be specified.</p>
Client	<p>SecureDataExchange</p> <p>SafeGuard Data Exchange with file-based encryption is always installed at local level and for removable media. SafeGuard Data Exchange provides secure encryption for removable media. Data can securely and easily be shared with other users. All encryption and decryption processes run transparently and with minimal user interaction. If you have installed SafeGuard Data Exchange on your computer, SafeGuard Portable is installed as well. SafeGuard Portable enables data to be securely shared with computers that do not have SafeGuard Data Exchange installed.</p> <p>Note:</p> <p>SafeGuard Data Exchange can be installed parallel to the BitLocker Client.</p>
Client	<p>BitLockerSupport</p> <p>Installs BitLocker support for SafeGuard Enterprise with the following functions:</p> <p>Boot volume encryption with BitLocker</p> <p>Encryption of other volumes with BitLocker</p>

Feature Parents	Feature
	<p>BitLocker Pre-Boot Authentication</p> <p>BitLocker Recovery</p> <p>Either SectorBasedEncryption OR BitLockerSupport can be specified.</p> <p>Note:</p> <p>Not available for Sophos SafeGuard Clients (standalone).</p>
Client	<p>ConfigurationProtection</p> <p>Port protection and management of peripheral devices: To install SafeGuard Configuration Protection, you need to list this feature in the msiexec command for the Client installation package AND carry out additional installation steps, <i>see Setting up SafeGuard Configuration Protection</i> (page 74).</p> <p>Note:</p> <p>Not available for Sophos SafeGuard Clients (standalone).</p>

10.3.2 Features for SafeGuard Data Exchange

Note:

You must list the feature **Client** and **Authentication** by default. If you select a feature, you also need to add the feature parents to the command line!

Feature Parents	Feature
Client	<p>Authentication</p> <p>You must state the feature Authentication and its parent feature Client by default.</p>
Client	<p>SecureDataExchange</p> <p>SafeGuard Data Exchange with file-based encryption is always installed at local level and for removable media. SafeGuard Data Exchange provides secure encryption for removable media. Data can securely and easily be shared with other users. All encryption and decryption processes run transparently and with minimal user interaction. If you have installed SafeGuard Data Exchange on your computer, SafeGuard Portable is installed as well. SafeGuard Portable enables data to be</p>

Feature Parents	Feature
	securely shared with clients that do not have SafeGuard Data Exchange installed.
Client	<p>ConfigurationProtection</p> <p>Port protection and management of peripheral devices: To install SafeGuard Configuration Protection you need to list this feature in the msiexec command for the Client installation package AND carry out additional installation steps, <i>see Setting up SafeGuard Configuration Protection</i> (page 74).</p> <p>Note:</p> <p>Not available for Sophos SafeGuard Clients (standalone).</p>

10.3.3 Sample command for volume- and file-based encryption

The command given below has the following effect:

- The endpoint computers are provided with the necessary requirements for successful installation of the encryption software.
- SafeGuard Enterprise Power-on Authentication is installed.
- SafeGuard Enterprise volume-based encryption is installed.
- SafeGuard Data Exchange with file-based encryption is installed by specifying **SecureDataExchange**.
- A log file is created.
- SafeGuard Enterprise Client (managed) configuration package is run.

Example:

```
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,BaseEncryption,SectorBasedEncryption,  
SecureDataExchange
```

```
InstallDir=C:\Program Files\Sophos\SafeGuard Enterprise
```

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

10.3.4 Sample command for BitLocker support on Windows Vista

The command given below takes the following effect:

- The endpoint computers are provided with the necessary requirements for successful installation of the encryption software.
- Users log on to their PCs using Windows Vista Credential Provider.
- SafeGuard Enterprise BitLocker support with BitLocker volume-based encryption is installed.
- SafeGuard Data Exchange with file-based encryption is installed by specifying **SecureDataExchange**.
- A log file is created.
- The SafeGuard Enterprise Client (managed) configuration package is then run.

Note:

When installing SafeGuard Enterprise with BitLocker, make sure that only **BitLockerSupport** is run. Do not add SafeGuard Enterprise **BaseEncryption** to the command line.

Example:

```
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,BitLockerSupport,SecureDataExchange
```

```
InstallDir=C:\Program Files\Sophos\SafeGuard Enterprise
```

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

10.4 FIPS-compliant installation

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 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.

10.5 Installation on endpoint computers with self-encrypting, Opal-compliant hard drives

SafeGuard Enterprise supports the vendor-independent Opal standard for self-encrypting hard drives and offers management of endpoint computers 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 computer:

■ 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. Should 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, installation does not fall back to software-based encryption. Instead all volumes on the Opal disk remain unencrypted.

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 msi's internal property has the same name, should you opt for an installation with .mst files or use for example ORCA to modify your .msi file.

For further information on SafeGuard Enterprise in combination with Opal-compliant hard drives, refer to the SafeGuard Enterprise administrator help and user help.

11 Setting up endpoint computers locally

If you want to carry out a trial installation on an endpoint computer, it might be useful to install SafeGuard Enterprise locally first.

Installation and configuration is described for SafeGuard Enterprise Clients (managed) as well as for Sophos SafeGuard Clients (standalone). The installation procedure is identical except that you assign a different configuration package for each of them.

The tasks required for an installation of endpoint computers with Windows BitLocker Device Encryption are described as well. For details on preparing for BitLocker support, *see [Specific preparations for BitLocker Drive Encryption support](#)* (page 55).

The behavior of the endpoint computers when first logging on after installing SafeGuard Enterprise and the activation of the Power-on Authentication is described in the User Help.

11.1 Install the encryption software locally

To install the encryption software locally:

1. Prepare for installation on the endpoint computers, *see [Prepare for encryption](#)* (page 54).
2. Log on to the computer as an administrator.
3. Install the pre-installation package **SGxClientPreinstall.msi** that provides the endpoint computer with the necessary requirements for a successful installation of the 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> or check that **MSVCR80.dll**, version 8.0.50727.4053 is present in the Windows\WinSxS folder on the computer.

4. Double-click the relevant <client> installation package (MSI) to start the encryption software installation wizard. It guides you through the necessary steps.
5. Accept the defaults on the subsequent dialogs.
6. If prompted, select the install type and the features to your needs. Customers installing SGNClient.msi or SGNClient_x64.msi do one of the following:
 - Select **Complete** to install both SafeGuard Enterprise Device Encryption and Data Exchange.
 - Select **Typical** to install SafeGuard Enterprise Device Encryption only.
 - Select **Custom** to install BitLocker Device Encryption. Under **Features**, select **Device Encryption**, activate **BitLocker Support** and clear **Base Encryption**.

Note:

Even if it is possible to only install a subset of features in a first-time installation, we recommend that you install the Device Encryption feature (volume-based encryption) from the start.

7. Accept the defaults on all subsequent dialogs to complete the installation wizard.

SafeGuard Enterprise is installed on the endpoint computer.

8. Go to the location where you have saved the relevant configuration package (MSI) created beforehand in the SafeGuard Management Center. Different configuration packages need to be installed for managed and standalone endpoint computers, [see About creating configuration packages](#) (page 56).
9. Install the relevant configuration package (MSI) on the computer.

SafeGuard Enterprise is set up on the endpoint computer. Next log on to the computer for the first time after installation. See the User Help for the behavior of the computer after SafeGuard Enterprise installation.

12 Installing SafeGuard Enterprise on computers with multiple operating systems

The SafeGuard Enterprise encryption software can be installed on a computer to protect its data even if several operating systems are installed on separate volumes of the hard disk. SafeGuard Enterprise provides a so-called 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.

12.1 Requirements and restrictions

Note the following:

- SafeGuard Enterprise Runtime does not provide any SafeGuard Enterprise Client specific 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 Client installation.
- The Runtime installation package must be installed before the full version of the SafeGuard Enterprise Client installation package is installed.
- Only volumes encrypted with the defined machine key in SafeGuard Enterprise can be accessed.

12.2 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 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. 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, Windows 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, Windows 7 64 bit). If required, you may additionally install Configuration Protection (SGN_CP_Client.msi / SGN_CP_Client_x64.msi available for Windows 7 64 bit operating systems).

12.3 Set up 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 disk where you want to install SafeGuard Enterprise Client.
8. Start the primary Windows installation on the selected volume.
9. Start the preparatory installation package SGxClientPreinstall.msi to provide endpoint computers with the necessary requirements for successful installation of the encryption software.
10. Install the SafeGuard Enterprise Client installation package on the selected volume.
11. Create a configuration package for a SafeGuard Enterprise Client (managed) or Sophos SafeGuard Client (standalone) as required and deploy it to the endpoint computer.
12. Encrypt both volumes with the defined machine key.

12.4 Start up from a secondary volume with a boot manager

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

Each volume encrypted with the defined machine key can be accessed.

13 Setting up SafeGuard Configuration Protection

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

13.1 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 SafeGuard Enterprise Clients (managed). It is not supported for Sophos SafeGuard Clients (standalone).
- .NET Version 2.0 has to be installed.

13.2 Install SafeGuard Configuration Protection centrally

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

The command line is as follows:

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

To successfully install SafeGuard Configuration Protection centrally, carry out the steps in the order mentioned:

1. Prepare for installation on the endpoint computers, [see *Prepare for encryption*](#) (page 54).

- 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:

<p>Preparatory installation package SGxClientPreinstall.msi</p>	<p>The package provides the endpoint computers with the necessary requirements for a successful installation of the encryption software, for example the required DLL MSVCR80.dll, version 8.0.50727.4053.</p> <p>Note:</p> <p>If this package is not installed, installation of the encryption software is aborted.</p>
<p>SafeGuard Enterprise Client installation package</p>	<p>Use either SafeGuard Device Encryption (SGNClient.msi) or SafeGuard Data Exchange (SGN_withoutDe.msi). 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.</p> <p>Add ConfigurationProtection as feature to the ADDLOCAL option.</p>
<p>SafeGuard Configuration Protection installation package</p>	<p>Use SGN_CP_Client.msi. To set up SafeGuard Configuration Protection on Windows 7 64 bit operating systems, you may use the 64 bit variant of the “Client“ installation packages.</p> <p>Make sure that the computer is not restarted by using parameter /norestart: msiexec /i SGN_CP_Client.msi /quiet /norestart</p>
<p>Configuration package for SafeGuard Enterprise Client (managed)</p>	<p>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.</p>
<p>Script with commands for pre-configured installation</p>	<p>We recommend that you use the Windows Installer command-line tool msiexec to create the script.</p>

- Create a folder **Software** to use as a central store for all applications.
- To create the script, open a command prompt, and then type the scripting commands.
- Distribute this package using company software distribution mechanisms to the endpoint computers.

13.2.1 Sample command for SafeGuard Configuration Protection with SafeGuard Device Encryption

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

- The endpoint computers are provided with the necessary requirements for successful installation of the encryption software.
- SafeGuard Device Encryption with volume-based encryption is installed.
- SafeGuard Configuration Protection must be listed as feature for the SafeGuard Device Encryption Client installation package.
- To initiate the installation of the SafeGuard Configuration Protection module a separate installation package must be added by specifying an additional msixec command.
- A log file is created.
- The configuration package for the SafeGuard Enterprise Client (managed) is run.

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,BaseEncryption,SectorBasedEncryption,ConfigurationProtection
```

```
InstallDir=C:\Program Files\Sophos\SafeGuard Enterprise
```

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

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

13.2.2 Sample command for SafeGuard Configuration Protection with SafeGuard Data Exchange

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

- The endpoint computers are provided with the necessary requirements for successful installation of the encryption software.
- SafeGuard Data Exchange with file-based encryption is installed.
- SafeGuard Configuration Protection must be listed as feature for the SafeGuard Data Exchange Client installation package.
- To initiate the installation of the SafeGuard Configuration Protection module a separate installation package must be added by specifying an additional msiexec command.
- A log file is created.
- The configuration package for the SafeGuard Enterprise Client (managed) is run.

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\SGN_CP_Client.msi /quiet /norestart
```

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

13.3 Install SafeGuard Configuration Protection locally

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

1. Prepare for installation on the endpoint computers, [see Prepare for encryption](#) (page 54).
2. Log on to the computer as an administrator.
3. Install the preparatory installation package **SGxClientPreinstall.msi** that provides the endpoint computer with the necessary requirements for a successful installation of the encryption software.
4. Select one of the following SafeGuard Enterprise Client installation packages to be installed on the endpoint computer. 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 Device Encryption (SGNClient.msi/SGNClient_x64.msi)
 - SafeGuard Data Exchange (SGNClient_withoutDE.msi/SGNClient_withoutDE_x64.msi)
5. In the installation wizard, select an installation of type **Custom**. Under **Features**, make sure to additionally select **Configuration Protection**.
6. Install the SafeGuard Configuration Protection installation package SGN_CP_Client.msi/SGN_CP_Client_x64.msi (available for Windows 7 64 bit operating systems).

Change the installation directory to C:\Program Files\Sophos\SafeGuard Enterprise\ to make sure that the Configuration Protection module is installed in the SafeGuard Enterprise directory.
7. Do not restart the computer.
8. Generate a configuration package for the SafeGuard Enterprise Client (managed) and install it on the endpoint computer immediately after the installation of the encryption software.
9. Restart the endpoint computer.

SafeGuard Configuration Protection is installed on the endpoint computer.

13.4 Uninstall SafeGuard Configuration Protection

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

1. Uninstall the SafeGuard Enterprise Client (managed) configuration package.
2. Start the SafeGuard Enterprise Client installation package on the computer, either SGNClient.msi or SGNClient_withoutDE.msi or the respective 64 bit variant.
3. In the installation wizard, select an installation of 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 installation package SGN_CP_Client.msi/SGN_CP_Client_x64.msi.

7. Restart the computer.

SafeGuard Configuration Protection is removed from the endpoint computer.

13.5 Update SafeGuard Configuration Protection

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

1. Start the preparatory installation package SGxClientPreinstall.msi to provide endpoint computers with necessary requirements for successful installation of the encryption software.
2. Start the latest SafeGuard Enterprise Client installation package on the computer, either SGNClient.msi or SGNClient_withoutDE.msi or the respective 64 bit variant to update it. 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.

Do not restart the computer when the update is finished.

3. In **Add/Remove Programs**, remove the SafeGuard Configuration Protection Client SGN_CP_Client.msi.
4. Restart the endpoint computer.
5. Install the latest SafeGuard Configuration Protection Client installation package SGN_CP_Client.msi/SGN_CP_Client_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 updated on the endpoint computer.

14 Replicating the SafeGuard Enterprise Database

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

This chapter 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.

14.1 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.

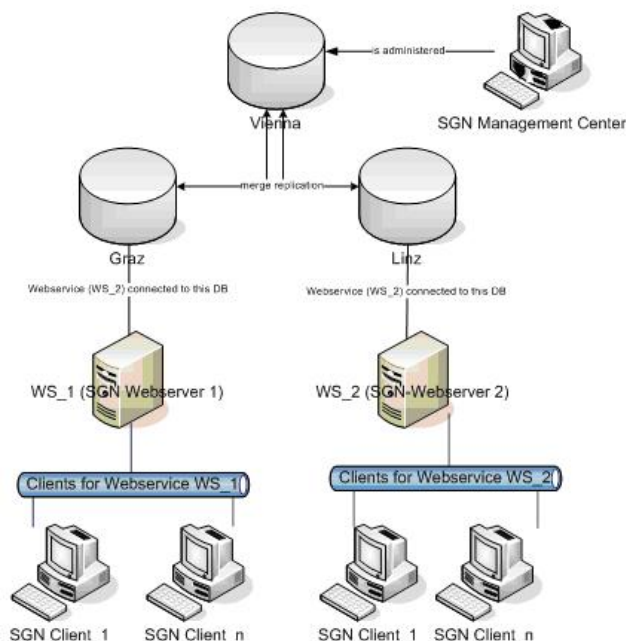
Merge replication allows various sites to work autonomously and at a later time merge updates into a single, uniform result. The initial snapshot is applied to Subscribers, and then Microsoft SQL Server tracks changes to published data at the Publisher and at the Subscribers. The data is synchronized 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.

14.2 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.



14.2.1 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 33).

- Generate the master database with an SQL script you can find in the product directory.

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 27).

14.2.2 Generate the replication databases Graz and Linz

After setting up the master database, you may 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 concatenated by default so that the event database can be replicated to several SQL servers to enhance

performance. If EVENT tables are concatenated, 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.

14.3 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**.
4. You are prompted to add the server certificates **ws_1.cer** and **ws_2.cer**. You find them in the **\Program Files\Sophos\SafeGuard Enterprise\MachCert** folder. These certificates are needed to create the appropriate configuration packages.

The SafeGuard Enterprise Servers are installed and registered.

14.4 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.

14.5 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.

14.6 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 44).

14.7 Install SafeGuard Enterprise Client software and configuration on the endpoint computers

You install the SafeGuard Enterprise Client software in the same way as for SafeGuard Enterprise Clients without replication. For further information, [see *Command for central installation*](#) (page 61).

Note:

For the correct configuration make sure to install the correct client configuration package after you have installed each SafeGuard Enterprise Client:

1. Install the GRAZ client configuration package on those clients to be connected to the GRAZ server WS_1.
2. Install the LINZ client configuration package on those clients to be connected to the LINZ server WS_2.

For information on updating replicated SafeGuard Enterprise databases, [see *Update SafeGuard Enterprise replicated databases*](#) (page 86).

15 Updating SafeGuard Enterprise

If you have already installed a previous version of SafeGuard Enterprise, you can update SafeGuard Enterprise by installing the latest version. Direct updating to SafeGuard Enterprise version 5.6x is supported by SafeGuard Enterprise version 5.40 onwards. When updating from older versions, you must first update to SafeGuard Enterprise 5.40.

Apart from the SafeGuard Enterprise Database, the updates for SafeGuard Enterprise Server, SafeGuard Management Center, and SafeGuard Enterprise protected endpoint computers are the same as a new installation.

From SafeGuard Enterprise 5.30 onwards the import of a valid license file is required that covers all rolled out clients. If the amount of licenses is exceeded, policy transport is blocked after the update of the backend. Please contact your sales partner in advance to request a license file.

Note:

It is essential that you update the components in the order shown below. Any update from an earlier version to the current version of SafeGuard Enterprise will only succeed if you follow this sequence:

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

15.1 Update SafeGuard Enterprise Database

Prerequisites

- SafeGuard Enterprise Database 5.20 or higher must be installed.
- The SQL scripts that are to be run must be present on the database computer.
- .NET Framework 3.0 Service Pack 1 must be installed for successfully updating to the latest version.
- Make sure that you have Windows administrator rights.
- Back up the database before starting the update.

In the Tools folder of your product delivery several SQL scripts are provided for updating the database.

To update the database:

1. Take all SafeGuard Enterprise Servers (IIS servers) connected to the relevant SafeGuard Enterprise Database offline.
2. Close the SafeGuard Management Center.

3. Set the relevant database to SINGLE_USER mode for running the SQL scripts so that you have exclusive access to the database.
4. The database must be converted version by version to the current version. Depending on the version installed, start the following SQL scripts in sequence:
 - a) 5.20 > 5.3x: Run **MigrateSGN520_SGN530.sql** or **MigrateSGN520_SGN535.sql**.
Existing SafeGuard Enterprise policies will be modified as the policy structure has changed from version 5.20 to 5.3x.
 - b) 5.3x > 5.35: Run **MigrateSGN530_SGN535.sql**
 - c) 5.3x > 5.4x: Run **MigrateSGN530_SGN535.sql**
 - d) 5.35 > 5.4x: Run **MigrateSGN535_SGN540.sql**
 - e) 5.4x > 5.5x: Run **MigrateSGN540_SGN550.sql**
 - f) 5.5x > 5.6x: Run **MigrateSGN550_SGN560.sql**
5. Set the relevant database to MULTI_USER mode again.

After you update the database, the cryptographic check sums of some tables might no longer be correct. When you start the SafeGuard Management Center warning messages are displayed accordingly. You can repair the tables in the relevant dialog.

The latest version of SafeGuard Enterprise Database is ready for use.

Note:

In the next step, update the Safeguard Management Center to the latest version. Otherwise it will show an error message.

15.2 Update SafeGuard Enterprise replicated databases

When the SafeGuard Enterprise Database is to be updated to a later version and replicated databases are in use, it is best to uninstall the replicated databases before starting the update on the master database.

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

To update the replicated database:

1. Uninstall the replicated databases.
2. Run the SQL migration scripts on the master database. You can find it in the Tools folder of your product delivery, *see Update SafeGuard Enterprise Database* (page 85).
3. Set up the replication databases anew, *see Replicating the SafeGuard Enterprise Database* (page 80).

15.3 Update SafeGuard Enterprise Server

Prerequisites

- SafeGuard Enterprise Server 5.35 or higher must be installed. Versions below 5.35 must first be updated to SafeGuard Enterprise Server 5.40.
- .NET Framework 3.0 Service Pack 1 must be installed. AP.NET 2.0 must be updated to version 2.0.
- Make sure that you have Windows administrator rights.

To update SafeGuard Enterprise Server:

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

SafeGuard Enterprise Server is updated. It is automatically restarted and is ready for use.

15.4 Update SafeGuard Management Center

Prerequisites

- SafeGuard Management Center 5.40 or later must be installed. Versions below 5.40 must first be updated to SafeGuard Management Center 5.40.
- SafeGuard Enterprise database and SafeGuard Enterprise Server must have been updated to the latest version.
- The SafeGuard Enterprise database has already been updated to the latest version. For successful operation, version numbers of SafeGuard Enterprise database and SafeGuard Management Center must match.
- .NET Framework 3.0 Service Pack 1 must be installed. ASP.NET must be updated to version 2.0.
- Make sure that you have Windows administrator rights.
- You need a valid licence file. Contact your sales partner in advance to request it.

Note:

If SafeGuard Management Center is installed on a computer with SafeGuard Enterprise Client installed, first update the SafeGuard Enterprise Client software to version 5.6x. Then update SafeGuard Management Center to version 5.6x. Updating SafeGuard Management Center only, can lead to failed logons at Windows level.

After updating SafeGuard Management Center to version 5.6x, POA users should not be transferred to SafeGuard Enterprise Clients 5.4x or 5.5x. This is not supported in this case as the POA user would take ownership of the computer!

To update SafeGuard Management Center:

1. Install the latest version of the SafeGuard Management Center installation package with the required features, *see Setting up SafeGuard Management Center* (page 31).
2. Import the license file.
3. Start the SafeGuard Management Center. The behavior when starting the SafeGuard Management Center for the first time after the update depends on the features installed:

Option	Description
The feature Multi Tenancy is not installed.	You are prompted to enter the SafeGuard Management Center security officer credentials.
The feature Multi Tenancy is newly installed.	The SafeGuard Management Center Configuration Wizard starts and prompt 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.
The feature Multi Tenancy is uninstalled.	The database configuration that has been used latest will be used in the SafeGuard Management Center.

SafeGuard Management Center is updated to the latest version.

Note:

- Scripting API: The default configuration file has been renamed and stored in a different location. Make sure that the path and file name is changed to the new location when using the following method with parameter **confFilePathName: AuthenticateOfficer (string OfficerName, string PinOrPassword, string confFilePathName)**.
- Existing SafeGuard Enterprise policies might have been modified as the policy structure has changed from SafeGuard Enterprise version 5.30 upwards.

15.5 Update SafeGuard Enterprise protected computers

Prerequisites

- SafeGuard Enterprise Client 5.40 or later must be installed. Older versions must first be updated to SafeGuard Enterprise Client 5.40.

SafeGuard Management Center 5.6x and SafeGuard Enterprise Server 5.6x can manage SafeGuard Enterprise Clients (managed and standalone) version 5.40 or later. A mixture of Client versions should only be present during the time of the update, but should be avoided for general use.

Note:

After updating SafeGuard Management Center to version 5.6x, POA users should not be transferred to SafeGuard Enterprise Clients 5.4x or 5.5x. This is not supported in this case as the POA user would take ownership of the computer!

- SafeGuard Enterprise Database, SafeGuard Enterprise Server and SafeGuard Management Center must have been updated to the latest version.
- SafeGuard Enterprise Client 5.6x cannot to be connected to a SafeGuard Enterprise Server below version 5.6x.
- Make sure that you have Windows administrator rights.

This section is valid for both managed and standalone endpoint computers.

To update SafeGuard Enterprise protected computers:

1. Install the preparatory MSI package **SGxClientPreinstall.msi**, which provides the endpoint computer with the necessary requirements for a successful installation of the current encryption software.
2. Install the respective encryption software installation package (*Client*.msi) version by version until the latest version is reached, [see *Install the encryption software centrally*](#) (page 59) or [see *Install the encryption software locally*](#) (page 70).

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.).

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

3. If the configuration of the endpoint computer has changed, for example when the policy settings have changed, create a new configuration package.
4. Delete all outdated or unused configuration packages on the endpoint computers for security reasons.
5. Deploy the new configuration package on the respective endpoint computers.

If you try to install an older configuration package over a newer one, the installation is aborted.

The endpoint computer is updated with the latest version of the encryption software with the selected features.

Note:

Users imported when only SafeGuard Data Exchange was installed before, are not automatically imported into the Power-on Authentication when SafeGuard Device Encryption is installed later. You must trigger a user update, for example by temporarily assigning a key to the directory root.

15.6 Update Sophos SafeGuard Clients (standalone) with volume-based encryption

If you want to enhance a Sophos SafeGuard Client (standalone) on which only the SafeGuard Data Exchange module with file-based encryption is installed, with volume-based encryption, you need to carry out the following steps. These steps are necessary to guarantee a secure and correct authentication at the Power-on Authentication.

1. Uninstall the SafeGuard Data Exchange installation package (SGNClient_withoutDE.msi/SGNClient_withoutDE_x64.msi).
2. Uninstall the configuration package.
3. Install the SafeGuard Enterprise Device Encryption installation package with volume- and file-based encryption (SGNClient.msi/SGNClient_x64.msi). Select the features **Device Encryption** and **Data Exchange** when prompted and finish the installation wizard.
4. Create a new configuration package and deploy it on the computer.

The Sophos SafeGuard Client (standalone) has been enhanced with volume-based encryption.

Note:

The key recovery file as well as the local keys created during the installation of the Data Exchange installation package are still available.

15.7 Upgrade Sophos SafeGuard Client (standalone) to SafeGuard Enterprise Client (managed)

You can upgrade endpoint computers with a Sophos SafeGuard Client (standalone) configuration to a SafeGuard Enterprise Client (managed) configuration. In this way, the endpoint computers are defined in the SafeGuard Management Center as objects which can be managed and which have a connection to the SafeGuard Enterprise Server.

Prerequisites

- Back up the endpoint computer before starting the upgrade.
- Make sure that you have Windows administrator rights.

To upgrade Sophos SafeGuard Client (standalone) to SafeGuard Enterprise Client (managed):

1. In the SafeGuard Management Center, on the **Tools** menu, click **Configuration Package Tool**. To create the configuration package for the SafeGuard Enterprise Client (managed), click **Create Configuration Package (managed)**.
2. Assign this package to the endpoint computer using a group policy.

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

3. Restart the endpoint computer. The first logon is still achieved with Autologon. New keys and certificates are assigned to the user.
4. Restart the endpoint computer for a second time. Log on at the Power-on Authentication. The computers are protected again only after the second restart.
5. Delete outdated and unused configuration packages.

The Sophos SafeGuard Client (standalone) is now a SafeGuard Enterprise Client (managed).

15.8 Update SafeGuard Configuration Protection Client

To update the SafeGuard Configuration Protection Client module, [see *Update SafeGuard Configuration Protection*](#) (page 79).

16 Updating 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 Vista to Windows 7 with SafeGuard Enterprise installed.

17 Upgrading Sophos SafeGuard to SafeGuard Enterprise

You can easily upgrade Sophos SafeGuard to the SafeGuard Enterprise suite with central management in order to make use of the full functionality of SafeGuard Enterprise, for example user and computer management, extensive logging functions.

Sophos SafeGuard comprises the following products:

- Sophos SafeGuard Disk Encryption available with ESDP (Endpoint Security and Data Protection)
- SafeGuard Easy: From version 5.50 onwards, SafeGuard Easy is the new product name for the SafeGuard Enterprise Standalone solution.

The upgrade consists of the following steps:

- The SafeGuard Policy Editor must be upgraded to the SafeGuard Management Center.
- Sophos SafeGuard (standalone) protected endpoint computers must be equipped with a SafeGuard Enterprise (managed) configuration.

17.1 Upgrade SafeGuard Policy Editor to SafeGuard Management Center

Prerequisites

- You do not have to uninstall SafeGuard Policy Editor.
- SafeGuard Enterprise Server must be installed and updated to the latest version.
- Make sure that you have Windows administrator rights.

To upgrade, simply install SafeGuard Management Center on the computer where SafeGuard Policy Editor has been set up.

1. Start SGNManagementCenter.msi from the install folder of your product delivery. A wizard guides you through the necessary steps.
2. On the **Welcome** page, click **Next**.
3. Accept the license agreement.
4. Accept the default installation path.
5. Select the installation type:
 - To install SafeGuard Management Center to support one database only, select **Typical**.
 - To install SafeGuard Management Center to support multiple databases (**Multi Tenancy**), select **Complete**. For further information, [see Multi Tenancy configurations](#) (page 33).
6. Click **Finish** to complete the installation.
7. If necessary, restart your computer.
8. Start the SafeGuard Management Center to carry out initial configuration, [see Configuring SafeGuard Management Center](#) (page 32).

The SafeGuard Policy Editor has been upgraded to the SafeGuard Management Center.

17.2 Upgrade Sophos SafeGuard Client (standalone) to SafeGuard Enterprise Client (managed)

You can upgrade endpoint computers with a Sophos SafeGuard Client (standalone) configuration to a SafeGuard Enterprise Client (managed) configuration. In this way, the endpoint computers are defined in the SafeGuard Management Center as objects which can be managed and which have a connection to the SafeGuard Enterprise Server.

Prerequisites

- Back up the endpoint computer before starting the upgrade.
- Make sure that you have Windows administrator rights.

To upgrade Sophos SafeGuard Client (standalone) to SafeGuard Enterprise Client (managed):

1. In the SafeGuard Management Center, on the **Tools** menu, click **Configuration Package Tool**. To create the configuration package for the SafeGuard Enterprise Client (managed), click **Create Configuration Package (managed)**.
2. Assign this package to the endpoint computer using a group policy.

Authentication is disabled as the user-computer assignment is not upgraded. After upgrading, the endpoint computers are therefore unprotected!
3. Restart the endpoint computer. The first logon is still achieved with Autologon. New keys and certificates are assigned to the user.
4. Restart the endpoint computer for a second time. Log on at the Power-on Authentication. The computers are protected again only after the second restart.
5. Delete outdated and unused configuration packages.

The Sophos SafeGuard Client (standalone) is now a SafeGuard Enterprise Client (managed).

18 Upgrading SafeGuard Easy 4.x/ Sophos SafeGuard Disk Encryption 4.x to SafeGuard Enterprise 5.6x

SafeGuard Easy (SGE) 4.5x as well as Sophos SafeGuard Disk Encryption 4.6x can be directly upgraded to SafeGuard Enterprise 5.6x by installing the SafeGuard Device Encryption Client installation package on the computer.

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

This chapter describes how to upgrade to Sophos SafeGuard and explains which features can be migrated and details the limitations.

18.1 Prerequisites

- Direct upgrade 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 upgrade is supported for Sophos SafeGuard Disk Encryption 4.6x.
- 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 for SafeGuard Enterprise 5.6x.
- When using special software (for example Lenovo middleware), it must meet the system requirements for SafeGuard Enterprise 5.6x.
- Upgrading may only take place if the hard disks are encrypted with the following algorithms: AES128, AES256, 3DES, IDEA.
- Users need a valid Windows account and password. In case 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 the upgrade and the new password has to be forwarded to the users. For further information see [see *Preparing for upgrade*](#) (page 98).

18.2 Limitations

- Only the SafeGuard Device Encryption installation package with the standard features can be installed (SGNClient.msi). If the module SafeGuard Data Exchange is to be installed in addition

(SGNClient_withoutDE.msi), this has to be done in a separate step as a direct upgrade is not supported for this package.

- The following installations cannot be upgraded to SafeGuard Enterprise and installing SafeGuard Enterprise should not be attempted.

Note:

If you start an upgrade in the cases mentioned below, 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 upgraded: XOR, STEALTH, DES, RIJNDAEL, Blowfish-8, Blowfish-16.

Note:

There is a risk of data being lost if a removable device has been encrypted with one of the algorithms XOR, STEALTH, DES, RIJNDAEL, Blowfish-8, Blowfish-16. The data on the removable medium cannot be accessed with Sophos SafeGuard after upgrading!

- Removable media with Super Floppy volumes cannot be transformed after upgrading.
- 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 computer where it was converted.

18.3 Which functionality is upgraded

The table below shows which functionality is upgraded and how it is mapped in SafeGuard Enterprise.

SafeGuard Easy/Sophos SafeGuard Disk Encryption	Upgrade	SafeGuard Enterprise
Encrypted hard disks	Yes	The hard disk keys are protected by SafeGuard Enterprise Power-on Authentication. So the hard disk key is at no time exposed. If Boot Protection mode has been selected in SafeGuard Easy, the

SafeGuard Easy/Sophos SafeGuard Disk Encryption	Upgrade	SafeGuard Enterprise
		current version has to be uninstalled. The hard disk's encryption algorithm is not changed by the upgrade. Therefore the actual algorithm for this type of upgraded hard disk may differ from the general SafeGuard Enterprise policy.
Encrypted removable media (only applicable when migrating from SafeGuard Easy)	Yes	Encrypted data 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 computer where it was converted. The conversion needs to be confirmed in each case.
Encryption algorithms	To some degree	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.
Challenge/Response	To some degree	The Challenge/Response procedure is maintained.
User names	No	As the Windows user names are used in SafeGuard Enterprise, there is no need to reuse the SafeGuard Easy/Sophos SafeGuard Disk Encryption specific user names. So registering the upgraded computers is done in the same way as with a new SafeGuard Enterprise installation: by centrally assigning or locally registering the computer's users. Note: After the upgrade, 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).
User passwords	No	As the Windows passwords are used in SafeGuard Enterprise, there is no need to reuse the SafeGuard Easy/Sophos SafeGuard Disk Encryption specific passwords. SafeGuard Easy/Sophos SafeGuard Disk Encryption passwords are therefore not upgraded.
Policies, settings (for example minimum password length)	No	To ensure that all the settings are consistent, no automatic upgrade is executed. The policies have to be reset in the SafeGuard Management Center.
Pre-Boot Authentication	No	Pre-Boot Authentication (PBA) is replaced by the Sophos SafeGuard Power-on Authentication (POA).

SafeGuard Easy/Sophos SafeGuard Disk Encryption	Upgrade	SafeGuard Enterprise
Installations without GINA	Yes	Installations without GINA are upgraded to SafeGuard Enterprise with SGNGINA installed.
Tokens/smartcards (only applicable when migrating from SafeGuard Easy)	To some degree	The token/smartcard hardware can continue to be used in SafeGuard Enterprise. However, the credentials are not upgraded. The tokens used in SafeGuard Easy therefore need to be re-issued in SafeGuard Enterprise and, as with every other SafeGuard Enterprise endpoint computer, set up using policies. SafeGuard Easy credentials in file form on token/smartcards remain as such, but can only be used to log on to computers with SafeGuard Easy support. If necessary, the token/smartcard middleware in use has to be updated to a version supported by SafeGuard Enterprise.
Logon with Lenovo Fingerprint Reader	To some degree	Fingerprint logon 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. For further information on fingerprint logon, see the User Help.

18.4 Preparing for upgrade

- To reduce the risk of data loss, we recommend that you create a full backup of the computers that are to be upgraded.

Carry out the steps that are recommended before installing the encryption software, for example use **chkdsk** and **defrag**. For further information, *see [Prepare for encryption](#)* (page 54). See also:

chkdsk: <http://www.sophos.com/support/knowledgebase/article/107799.html>.

defrag: <http://www.sophos.com/support/knowledgebase/article/109226.html>.

- 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 path. 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 upgrade.
- When upgrading from older versions of SafeGuard Easy, first upgrade to version 4.50.
- Leave the computers switched on throughout the upgrade process.

- The security officer should keep the users' Windows credentials at hand in case users have forgotten their Windows passwords after upgrading. This can happen if users have previously logged on to the Pre-Boot Authentication and have later been logged on with Windows Secure Autologon (SAL), so that they have never used their Windows credentials.

Note:

Users need to know their password for Windows logon before upgrading. This is essential as a Windows password cannot be set after upgrade and installation of SafeGuard Enterprise. If users do not know their Windows password because they have used Secure Automatic Logon in SafeGuard Easy/Sophos SafeGuard Disk Encryption, they will not be able to log on to SafeGuard Enterprise. In this case pass-through to Windows is rejected and users cannot log on to SafeGuard Enterprise. Thus, there is the risk of data loss as users will not be able to access their computers anymore.

18.5 Start the upgrade

Note:

The installation can be carried out on a running SafeGuard Easy/Sophos SafeGuard Disk Encryption system. No decryption of encrypted hard drives or volumes is necessary.

Use the SafeGuard Device Encryption Client installation package (SGNClient.msi) from the installation folder with the standard feature set. The client package SGNClient_withoutDE.msi cannot be used for upgrading. The installation is best performed centrally in unattended mode. Installation using the setup folder is not recommended!

To upgrade:

1. Double-click WIZLDR.exe from the SafeGuard Easy/Sophos SafeGuard Disk Encryption program folder of the endpoint computer that is to be upgraded. 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 **SGEMIG.cfg** is created.
3. In Windows Explorer, rename this file from **SGEMIG.cfg** to **SGE2SGN.cfg**.

Note: Owner/creator rights have to be set for this file and the file path where it is stored during the upgrade. Otherwise, the upgrade 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 SafeGuard Enterprise preinstallation package as well as the SafeGuard Enterprise Device Encryption Client installation package on the SafeGuard Easy/Sophos SafeGuard Disk Encryption endpoint. 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 upgrade is successful, SafeGuard Enterprise is ready on the computer.
- If the upgrade fails, SafeGuard Easy/Sophos SafeGuard Disk Encryption can still be used on the computer. In such cases, SafeGuard Enterprise is automatically removed.

18.6 Log on to the endpoint computer after the upgrade

To log on to the computer that has been upgraded from SafeGuard Easy 4.5x/Sophos SafeGuard Disk Encryption 4.6x to SafeGuard Enterprise 5.6x:

1. Restart the upgraded endpoint computer. The first logon is still achieved with Autologon. New keys and certificates are assigned to the user.
2. Restart the endpoint computer for a second time. Log on at the Power-on Authentication. The computers 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 computer again.

After successful upgrade 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.

18.7 Configure the upgraded endpoint computers

Endpoint computers are initially configured by configuration packages which, among other aspects, activate the Power-on Authentication.

Prerequisites:

Endpoint configuration should take place only after the upgrade and only after the POA has been activated and the user has successfully logged on to Windows on the upgraded computer.

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 computer.

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

2. Install the configuration package on the endpoint computers.

18.8 Convert keys for encrypted removable media

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

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

Note:

Therefore, after conversion, an encrypted data medium can only be read with SafeGuard Enterprise and only at the one endpoint computer where it was converted during migration!

1. Detach the media from the computer and reinsert it again. 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.

Newly added removable media are encrypted, as with any SafeGuard Enterprise computer, if the appropriate policy configuration is present on the endpoint computer.

19 About uninstallation

- When the SafeGuard Enterprise Client encryption software is installed on the same computer as SafeGuard Management Center, SafeGuard Enterprise Server or SafeGuard Web Help Desk, make sure that you follow this unistallation procedure to be able to continue using one of them:
 1. Uninstall SafeGuard Management Center, SafeGuard Enterprise Server or SafeGuard Web Help Desk.
 2. Uninstall the SafeGuard Enterprise Client configuration package.
 3. Uninstall the SafeGuard Enterprise Client encryption software.
 4. Install the package afresh that you want to continue using. To use SafeGuard Management Center, make sure that you import the old machine certificate after installation. To use SafeGuard Enterprise Client encryption software, make sure that you install the client configuration package after installing the encryption software.
- Before uninstalling the encryption software, first uninstall the configuration package.
- You cannot uninstall the encryption software for volumes that are encrypted with a user-specific key that is not assigned to you.
- When uninstalling SafeGuard Device Encryption Client volumes which have been encrypted using the default machine key, they are automatically decrypted. To decrypt volumes encrypted using other keys, create and assign an appropriate policy before uninstalling SafeGuard Device Encryption.
- During uninstallation of the encryption software which includes the decryption of encrypted volumes, do not shut down or restart the endpoint computer. Doing so will generate an error message from the uninstaller.
- If the uninstallation is triggered via Active Directory, make sure that all volume-based encrypted volumes have been decrypted properly beforehand.
- After an uninstallation, some files and registry entries may not be removed. Please see the Sophos knowledge database (keywords "SGN & uninstall") on how to clean the installation manually. A manual cleanup is necessary to successfully reinstall the encryption software on the same computer.
- If you have installed SafeGuard Device Encryption and SafeGuard Data Exchange on one computer, you cannot uninstall SafeGuard Device Encryption alone. You must uninstall the complete package.
- You should decrypt all encrypted removable media before uninstalling the last accessible SafeGuard Enterprise Client. Otherwise you may not be able to access your data any more. As long as you keep your SafeGuard Enterprise database the data on the removable media can be recovered.

19.1 Preventing uninstallation from the endpoint computers

To provide extra protection for endpoint computers, you can prevent local uninstallation of Sophos SafeGuard. In a **Machine specific settings policy**, set **Uninstallation allowed** to **No** and deploy the policy on the endpoint computers. If this kind of policy applies to the endpoint computer, uninstallation attempts are cancelled and the unauthorized attempt is logged.

Note:

If you use a demo version, you should not activate this policy setting or in any case deactivate it before the demo version expires to provide for easy uninstallation.

20 Technical support

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

- Visit the SophosTalk forum 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.

21 Legal notices

Copyright © 1996 - 2011 Sophos Group. All rights reserved. SafeGuard is a registered trademark of Sophos Group.

Sophos is a registered trademark 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.

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 licence terms or you otherwise have the prior permission in writing of the copyright owner.

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