

SOPHOS

SafeGuard® Enterprise 5.50 Installation

Document date: November 2010



Contents

1	SafeGuard Enterprise Overview	3
2	SafeGuard Enterprise components	4
3	Preparing for installation.....	6
4	Setting up SafeGuard Enterprise Database.....	16
5	Setting up SafeGuard Management Center	24
6	Setting up SafeGuard Enterprise Server.....	39
7	Testing communication.....	52
8	Replicating the SafeGuard Enterprise Database.....	57
9	Setting up an organizational structure.....	63
10	SafeGuard configurations for endpoint computers	68
11	Setting up endpoint computers centrally	76
12	Setting up endpoint computers locally	91
13	Installing the SafeGuard Enterprise Client software on computers with multiple operating systems.....	95
14	Installing SafeGuard Configuration Protection	98
15	Preventing uninstallation from the endpoint computer	103
16	Updating SafeGuard Enterprise	104
17	Upgrading Sophos SafeGuard 5.5x to SafeGuard Enterprise	111

18	Upgrading SafeGuard Easy 4.x /Sophos SafeGuard Disk Encryption 4.x to SafeGuard Enterprise.....	113
19	Updating the operating system	121
20	Annex - Best practice scenario	122
21	Technical Support.....	123
22	Copyright.....	124

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 done by the SafeGuard Enterprise 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.

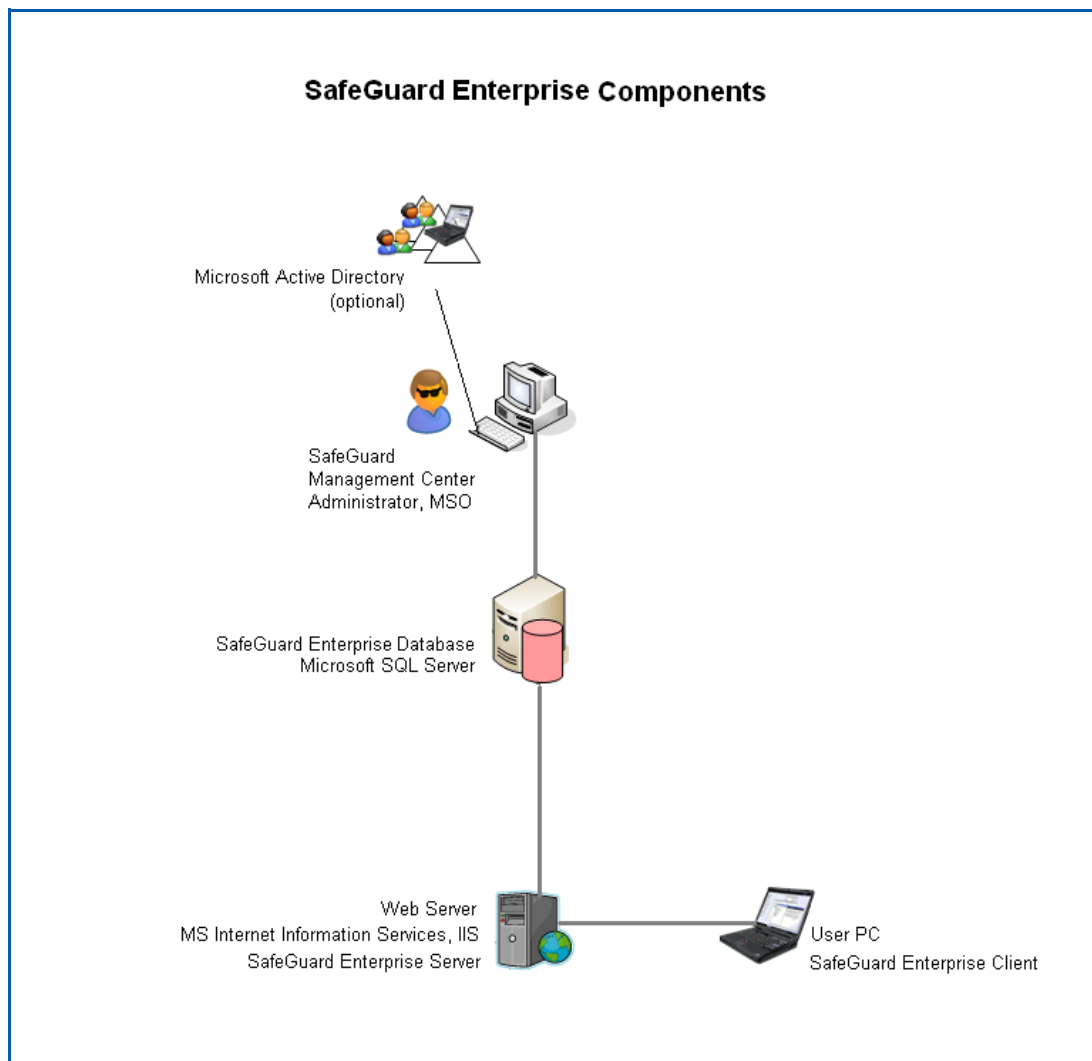
TIP: Our video tutorials are an ideal way to learn about SafeGuard Enterprise. You can find them on the product CD under Tutorials. They describe how SafeGuard Enterprise is installed and how to use the SafeGuard Management Center.

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
<p>SafeGuard Enterprise database(s) based on Microsoft SQL Server Database</p>	<p>The SafeGuard Enterprise database(s) hold all the relevant data such as keys/certificates, information about users & computers, events and policy settings.</p> <p>The database(s) need to be accessed by the SafeGuard Enterprise Server and from just one security officer from the SafeGuard Management Center, usually the MSO.</p> <p>The SafeGuard Enterprise databas(es) can be generated and configured using a wizard or scripts.</p>
<p>SafeGuard Enterprise Server on IIS based web server</p>	<p>Microsoft Internet Information Services (ISS) with .NET Framework 3.0 SP 1 and ASP.NET 2.0</p> <p>The web server used for SafeGuard Enterprise must be based on Internet Information Services (IIS). We recommend using a dedicated IIS server for SafeGuard Enterprise Server. The IIS Server may be clustered.</p> <p>SafeGuard Enterprise Server</p> <p>Interfaces between the 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.</p>
<p>SafeGuard Management Center with .NET Framework 3.0 SP 1, ASP.Net 2.0 on administrator PC</p>	<p>Central management tool for SafeGuard Enterprise for managing keys and certificates, users & computers, and creating SafeGuard Enterprise policies. The SafeGuard Management Center communicates with the database.</p>
<p>Directory Services (optional)</p>	<p>Import of an active directory. It holds the company's organizational structure with users and computers.</p>
<p>SafeGuard Enterprise Client on endpoint computers</p>	<p>Client software for authentication and data encryption on endpoint computers. The SafeGuard Enterprise Client communicates with the SafeGuard Enterprise Server.</p>

3 Preparing for installation

This chapter explains how to prepare for installing SafeGuard Enterprise successfully.

3.1 First steps before installing

You must make some preparations prior to installation. Please read the following list carefully and ensure that you comply with all the points.

General preparations

- Close all open applications.
- You need Window administrator rights.
- Ensure that there is enough free hard disk space. Information about this may be found in the release notes.
- Read the release notes carefully.

Preparations for encryption

- A user account must be set up and active on the endpoint computer.
- Create a full backup of the data on the endpoint computer.
- Check the hard disk(s) for errors for errors with this command `chkdsk :`
`chkdsk %systemdrive% /F /V /L /X`
In some cases you might be prompted to restart the computer and run `chkdsk` again.
You will find more information on this subject in the knowledgebase:
<http://www.sophos.com/support/knowledgebase/article/107799.html>.
- Use the Windows built-in "defrag" tool to locate and consolidate fragmented boot files, data files, and folders on local volumes. You will find more information on this subject in the knowledgebase: <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 the MBR be rewritten. To install SafeGuard Enterprise you need a "spotless" master boot record. The use of imaging/cloning programs may have affected the state of this record.
You can clean the master boot record by booting from a Windows CD and using the command `FIXMBR` within the Windows Recovery Console.
For further information see the knowledgebase:
<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 been restarted, you should 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 should reboot the computer once before SafeGuard Enterprise is installed.

New functionality is regularly being added to SafeGuard Enterprise as it is upgradable software. Therefore your version may include new functionality which we were unable to include in the manual or the online help before the editorial deadline. Such modifications are described in the release notes. You should read these carefully before installing.

3.2 System requirements

Refer to the release notes for details of the system requirements for hardware and software, service packs and the disk space required during the installation and for effective operation.

Specific requirements for endpoint computers:

AHCI

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.

Dynamic and GPT disks

Dynamic and GUID partition table (GPT) disks are not supported. In such cases, the installation will be terminated. If such disks can be found on the computer at a later point in time, they will not be supported.

SCSI hard disks

The SafeGuard Enterprise Device Encryption Client does not support systems that are equipped with hard disks attached via a SCSI bus.

3.3 Installation packages

You will find the SafeGuard Enterprise install components on the product CDs in the form of .msi packages.

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 SafeGuard Configuration Protection Client is available for Windows 7 64 bit.

The following .msi packages are provided:

Installation package	Description
SGNServer.msi	SafeGuard Enterprise Server
SGNManagementCenter.msi	SafeGuard Management Center for the central administration of domains, keys, policies, etc.
SGxClientPreinstall.msi	Must be installed on each endpoint computer prior to the encryption software (mandatory). Provides endpoint computers with necessary requirements for successful installation of the encryption software.
SGNClient.msi SGNClient_x64.msi	Volume based encryption and file based encryption with SafeGuard Data Exchange for both SafeGuard Enterprise Clients (managed) and Sophos SafeGuard Clients (standalone).
SGNClient_withoutDE.msi SGNClient_withoutDE_x64.msi	SafeGuard Data Exchange with file based encryption without Power-on Authentication for both SafeGuard Enterprise Clients (managed) and Sophos SafeGuard Clients (standalone).
SGN_CP_Client.msi SGN_CP_Client_x64.msi (available for Windows 7 64 bit)	SafeGuard Configuration Protection: port protection and management of peripheral devices on endpoint computers. This package is NOT available for Sophos SafeGuard Clients (standalone). The 64 bit variant of this package is available for Windows 7 64 bit operating systems.
SGNClientRuntime.msi SGNClientRuntime_x64.msi	Runtime Client enabling booting from a secondary boot volume when multiple operating systems are installed and accessing these volumes when they are encrypted by a SafeGuard Enterprise installation on the primary volume. Available for both SafeGuard Enterprise Clients (managed) and Sophos SafeGuard Clients (standalone).

In addition, configuration packages need to be generated during installation.

3.4 User interface language

You define the language of SafeGuard Enterprise on the Client in the Management Center using the policy type **General Settings > Customization > Client language**:

- If the language of the operating system is selected, the SafeGuard Enterprise product language uses the operating system language setting. If the relevant operating system language is not available in SafeGuard Enterprise, the SafeGuard Enterprise product language will default to English.
- If one of the available languages is selected, the SafeGuard Enterprise product parts on the client side will be displayed in the selected language.

You define the language of the SafeGuard Management Center inside the Management Center:

- Open menu **Extras > Options > General > SafeGuard Management Center language** and select a language.
- Restart the SafeGuard Management Center and it will be displayed in the selected language.

Setup language

The language of the installation and configuration wizards will be matched automatically to the language preferences of the computer's operating system. English, German, French and Japanese are supported for the installation and configuration wizards. For example, if the language of the operating system is English, the installation wizard will be displayed in English as well.

3.5 Interaction with other SafeGuard products

3.5.1 Interaction with SafeGuard LAN Crypt

Note the following:

- SafeGuard LAN Crypt 3.7x and SafeGuard Enterprise 5.50 can coexist on the same computer and are fully compatible.
- SafeGuard LAN Crypt with versions below 3.7x and SafeGuard Enterprise 5.5x cannot coexist on one computer.
If you are trying to install SafeGuard Enterprise 5.50 on a computer with an already installed SafeGuard LAN Crypt of version 3.6x or below, the setup will be cancelled and a respective error message will be displayed.
- SafeGuard LAN Crypt 3.7x and SafeGuard Enterprise with version below 5.35.4 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 of versions below 5.35.4, the setup will be cancelled and a respective error message will be displayed.

3.5.2 Interaction with SafeGuard PrivateCrypto and SafeGuard PrivateDisk

SafeGuard Enterprise 5.5x and the standalone products SafeGuard PrivateCrypto from version 2.30 as well as SafeGuard PrivateDisk from version 2.30 can coexist on the same computer.

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

3.5.3 Interaction 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 you have to uninstall SafeGuard Removable Media prior to installing SafeGuard Data Exchange on the endpoint computer.

3.6 Securing transport connections with SSL

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

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

SafeGuard Enterprise supports configuring a specific database connection for any registered web server.

- The connection between the SafeGuard Enterprise Server and the SafeGuard Enterprise Client 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.

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 point in 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 to the respective server or client.

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

NOTICE:

General security measures:

The computers on which SafeGuard Enterprise Server, the database and the Management Center are running should be protected against unauthorized local attack. The following are a few practical measures that can 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 (e.g. secure rooms)

3.6.1 Setting up SSL

Prior to enabling SSL encryption in SafeGuard Enterprise you need to set up your web server, database server and endpoint computers for it.

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

- 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 on SSL setup refer to the following links or contact our technical support:

<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

3.6.2 Activating SSL encryption in SafeGuard Enterprise

- Connection between web server and database server
SSL encryption can be set when registering the SafeGuard Enterprise Server via the SafeGuard Management Center Configuration Package Tool.
For details see *Registering and configuring SafeGuard Enterprise Server* on page 48.
- Connection between the database server and SafeGuard Management Center
SSL encryption can be set in the SafeGuard Management Center Configuration Wizard.
For details see *Configuring SafeGuard Management Center* on page 26.
- Connection between SafeGuard Enterprise Server and the SafeGuard Enterprise protected endpoint computer
SSL encryption can be enabled when creating the configuration package for the SafeGuard Enterprise Client via the SafeGuard Management Center Configuration Package Tool.
For details see *Creating a SafeGuard Enterprise Client (managed) configuration package* on page 81.

3.7 Installation steps for SafeGuard Enterprise

To install SafeGuard Enterprise with central management via SafeGuard Management Center, follow these installation steps.

	Step	Description	Installation/ Configuration package	Chapter
1	Preparatory measures	Preparations on client and server.		3.1
2	Set up SQL authentication for the SafeGuard Enterprise Security Officer	The user account is created on the Microsoft SQL Server.		4.4
3	Generating database via script (optional)	Generate the SafeGuard Enterprise Database(s) with a script.	SQL scripts on product CD in Tools directory	4.5.2
4	Set up SafeGuard Management Center	Install SafeGuard Management Center on the administrator PC.	SGNManagement Center.msi	5.2
5	Basic configuration, generate database via Wizard	Configure the database connections, generate the SafeGuard Enterprise Database(s) and the Master Security Officer.	SafeGuard Management Center Configuration Wizard	5.3. 5.4
6	Set up IIS Server for SafeGuard Enterprise	Set up Internet Information Services (IIS) with .NET Framework 3.0 and ASP.NET2.0		6.2
7	Set up SafeGuard Enterprise Server	Install SafeGuard Enterprise Server on the IIS web server.	SGNServer.msi	6.3
8	Register and configure SafeGuard Enterprise Server	Generate server configuration package and deploy it on the web server.	SGNServerConfig.msi Server configuration package generated in the SafeGuard Management Center Configuration Package Tool	6.4

	Step	Description	Installation/ Configuration package	Chapter
9	Test connection	Check and establish the connection between server, database and SafeGuard Management Center.		7
10	Create/import organization structure	Create a new structure or import an active directory in the SafeGuard Management Center.		9
11	Set up endpoint computers	Provide endpoint computers with necessary requirements for successful installation of the encryption software (mandatory).	SGxClientPreinstall.msi	10-12
		Install the SafeGuard Client installation package on the endpoint computer. Install either with or without Device Encryption.	SGNClient.msi SGNClient_x64.msi SGNClient_withoutDE.msi SGNClient_withoutDE_x64.msi	10-12
		Additionally install Configuration Protection (optional).	SGN_CP_Client.msi SGN_CP_Client_x64.msi	14
12	Configure endpoint computers	Generate configuration package for managed or standalone endpoint computers and install it on the endpoint computer.	SGNClientConfig.msi Client configuration package generated in the SafeGuard Management Center Configuration Package Tool	11.6

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

	Step	Description	Installation/ Configuration package	Chapter
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	13
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	10-12
		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 computer.	SGNClientConfig.msi Client configuration package generated in the SafeGuard Management Center Configuration Package Tool	11.6

4 Setting up SafeGuard Enterprise Database

This chapter describes how to set up a SafeGuard Enterprise Database. It describes the authentication for the database server which you need to be able to generate a SafeGuard Enterprise database. It also gives details on the SQL access rights that are required.

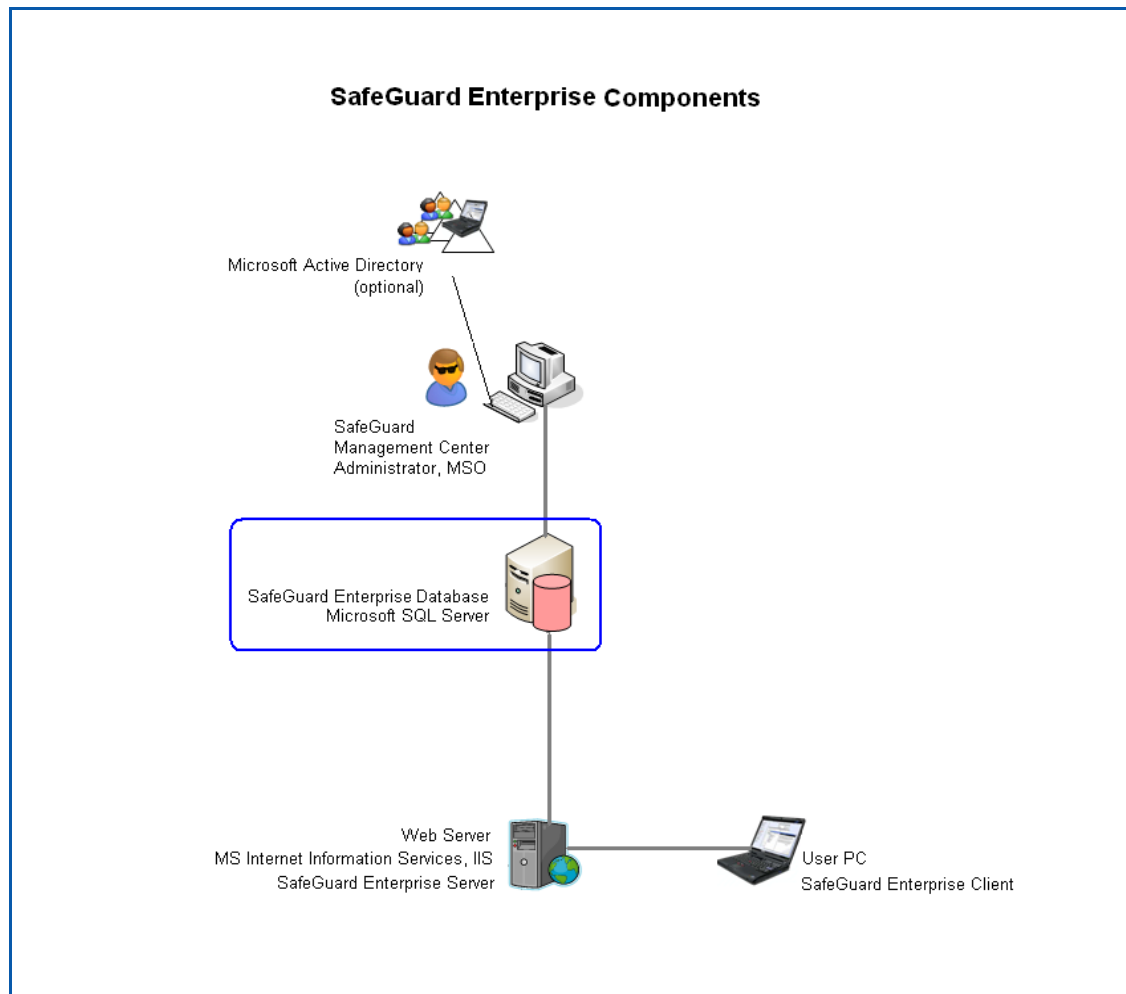
The SafeGuard Enterprise database is an SQL database based on Microsoft SQL Server. It holds all relevant data such as keys/certificates, information about the users and computers, events and policy settings. It can be generated in two different ways:

- by the first SafeGuard Enterprise Security Officer while installing the SafeGuard Management Center, using the SafeGuard Management configuration wizard
- by an SQL administrator using a script

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](#) on page 57.

Multiple tenant-specific SafeGuard Enterprise Databases can be created and maintained for different tenants such as different company locations, organizational units or domains. To configure multi-tenancy see [Configuring for multiple databases \(Multi Tenancy\)](#) on page 31.

Prior to generating SafeGuard Enterprise Database you need to set up an SQL user account for it.



Notice: We recommend operating a permanent online backup for the database. Backup 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, e.g. every week or every day.

4.1 Prerequisites

The following prerequisites must be met:

- Microsoft SQL Server must already be installed and configured. Microsoft SQL 2005 Express Edition is suitable for use in smaller companies, as there are no license fees.
- For performance reasons Microsoft SQL Server should not be installed on the computer on which SafeGuard Enterprise Server is installed.
- Authentication methods and access rights for the database should be clarified.

4.2 Authentication for the database

To be able to access the SafeGuard Enterprise database, the SafeGuard Management Center's first security officer must be authenticated. This can be done in the following ways:

- Windows authentication
- SQL authentication

You can find out from your SQL administrator which authentication method is intended for you, a security officer. You need this information before generating the database and before installing the SafeGuard Management Center.

Use SQL authentication for computers that are not part of a domain, otherwise use Windows authentication. This however requires additional configuration. You will find further information on Windows authentication in our knowledge database: <http://www.sophos.com/support/knowledgebase/article/108339.html>.

If you use SQL authentication, we highly recommend to secure the connection to and from the database server with SSL. For further information see [Securing transport connections with SSL](#) on page 11.

4.3 Rights to access the database

SafeGuard Enterprise is set up in such a way that, to work with the SQL database, it only needs a single user account with minimal access rights for the database. This user account is used by the SafeGuard Management Center and is only issued to the first 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 generated by the company's SQL administrator or by the SafeGuard Management Center security officer. The SafeGuard Management Center security officer needs, for a short time during installation, extended access rights for the SQL database (db_creator) if they are going to generate the SafeGuard Enterprise database themselves. However, after the install, these rights can be revoked 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 on the product CD, CreateDatabase.sql and CreateTables.sql, can be run for this purpose.

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

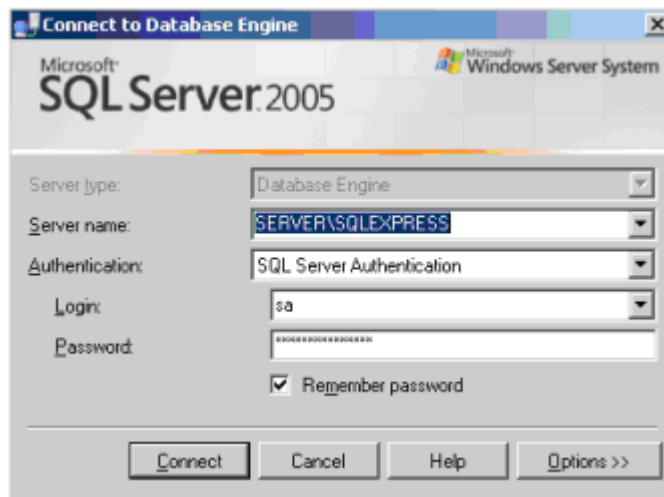
Access Right	SQL Server 2005	SQL Server 2005 Express
Generate database		
Server	db_creator	db_creator
Master database	None	None
SafeGuard Enterprise Database	db_owner public (default)	db_owner public (default)
Use (not generate) database		
Server	None	None
Master database	None	None
SafeGuard Enterprise Database	db_datareader db_datawriter public (default)	db_datareader db_datawriter public (default)

4.4 Setting up an SQL user account for SafeGuard Enterprise

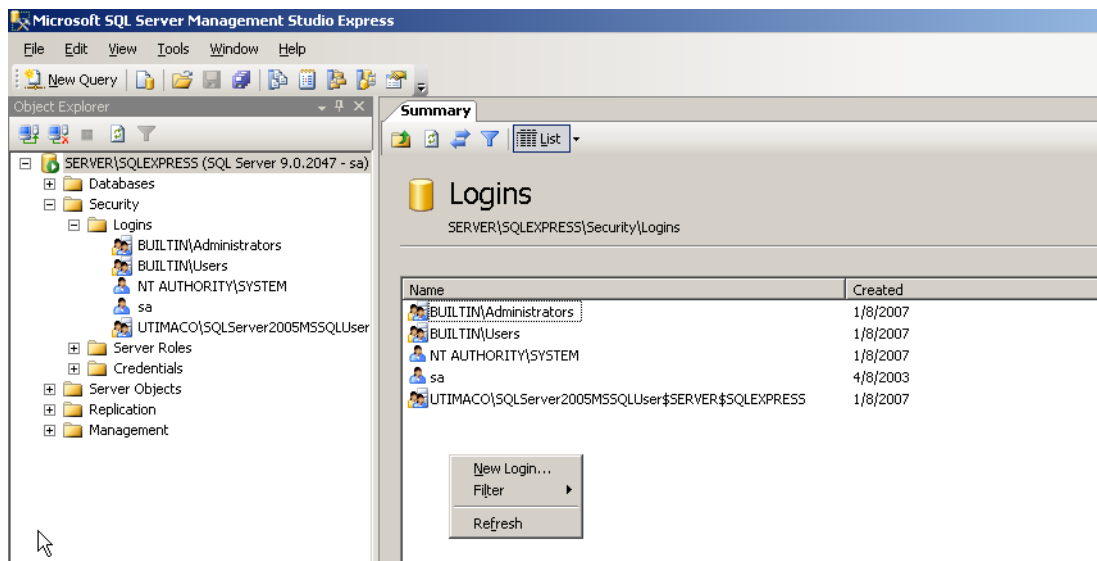
To generate the SafeGuard Enterprise database, a new user has to be created under Microsoft SQL Server for SafeGuard Enterprise, the authentication method needs to be specified and the necessary rights have to be issued.

The description below of the individual configuration steps is aimed at SQL administrators and relates to Microsoft SQL Server 2005 Express Edition.

1. Open the SQL Server Management Studio Express program. Log on to the SQL Server with your credentials.



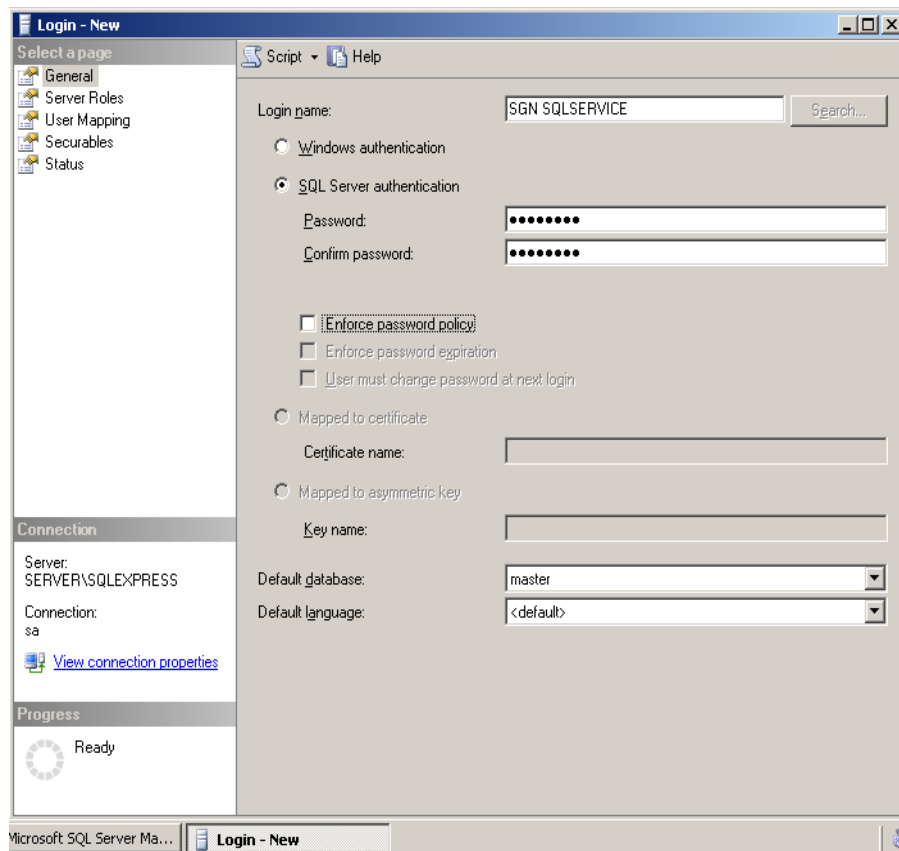
2. In the left-hand navigation window of Microsoft SQL Server Management Studio Express, select **Security > Logins**. In the right-hand window, right-click **New Login**.



3. In **Login - New** under **General**, enter the following:

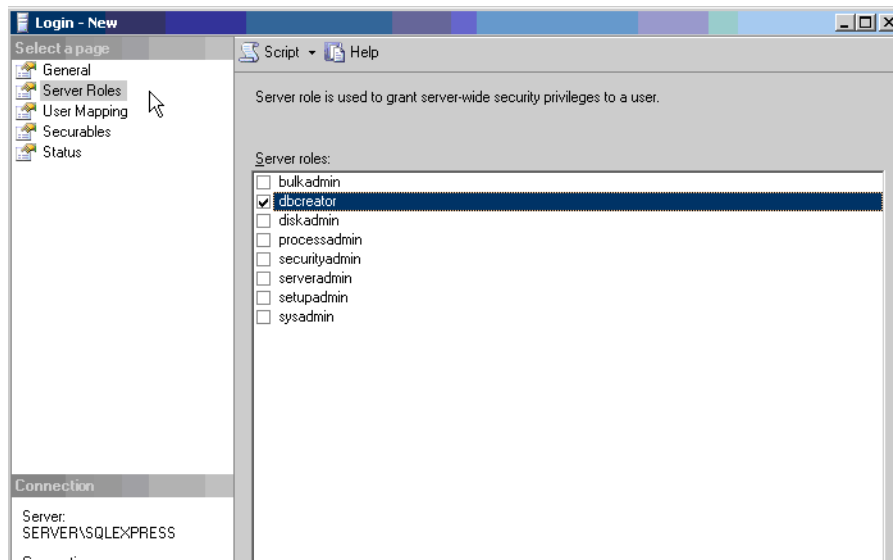
- **Login name:** Name of the new user, e.g. SGN SQLSERVICE.
- Select the required authentication method (recommended: SQL) and assign a password.
- **Disable Enforce password policy.**
- **Default Database:** If a script has not been used to create a SafeGuard Enterprise database yet, select **master**.

Later on you will have to inform the SafeGuard Management Center security officer of the authentication method and the credentials.



4. Now assign the access rights/roles by clicking **Server Roles** on the left:

- To generate the SafeGuard Enterprise database, select **dbcreator**. Once SafeGuard Enterprise has been installed, the database role can be reset to **dbowner**.
- If the SafeGuard Enterprise database has already been created and has been selected as the default database, select **db_datareader**, **db_datawriter** and **public**.



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

4.5 Generating the SafeGuard Enterprise database

After setting up the SQL user account you need to generate the SafeGuard Enterprise database. There are two ways to do so.

- via the SafeGuard Management Center Configuration Wizard
 - This procedure requires that the SafeGuard Management Center is already installed, see [Installing SafeGuard Management Center](#) on page 25.
- via an SQL script you can find on the product CD.
 - This procedure is often preferred if extended SQL permissions during SafeGuard Management Configuration is not desirable.
 - It depends on your enterprise environment which method should be applied. It is best to be clarified between SQL administrator and SafeGuard Enterprise security officer.

4.5.1 Generating SafeGuard Enterprise Database via SafeGuard Management Center

As a security officer, you can easily generate the SafeGuard Enterprise database after installation of the SafeGuard Management Center. The SafeGuard Management Center Configuration Wizard takes you through the basic configuration which also includes database creation, see [Configuring SafeGuard Management Center](#) on page 26.

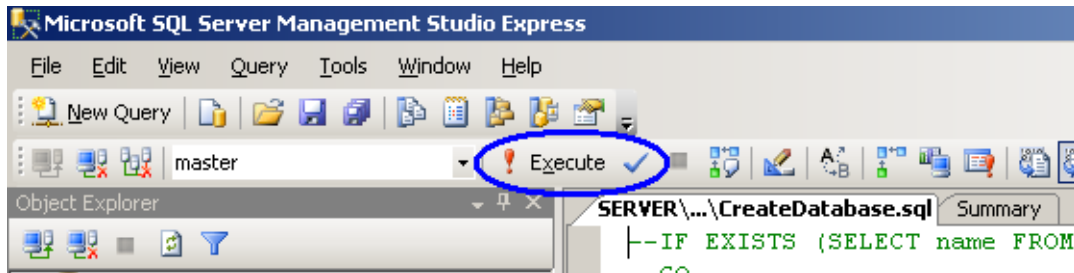
4.5.2 Generating SafeGuard Enterprise Database with a script

If extended SQL permissions during database creation in the Management Center is not desirable, you can also generate the SafeGuard Enterprise database with a script. Two scripts are provided on the product CDs (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 2005 Express Edition.

1. Open script CreateDatabase.sql and check the two target path specifications under FILENAME. They must match the paths specified on your server. Correct them if necessary.
2. Double-click to start the CreateDatabase.sql script. Microsoft SQL Server Management Studio Express is launched.
3. Log on to SQL Server with your credentials.
4. Click the **Execute** button to generate the database.



Next use the CreateTables.sql script off the product CD to generate the tables.

1. Double-click to start the CreateTables.sql script. Microsoft SQL Server Management Studio Express is launched.
2. Enter your credentials for the SQL Server.
3. Select the correct database that you have created for SafeGuard Enterprise. To do this, in the SQL Server login window, click **Options > Connection Properties** and, under **Connect to Database**, select the SafeGuard Enterprise database in which the tables are to be created. Click **Connect**.
4. Click the **Execute** button to generate the tables.

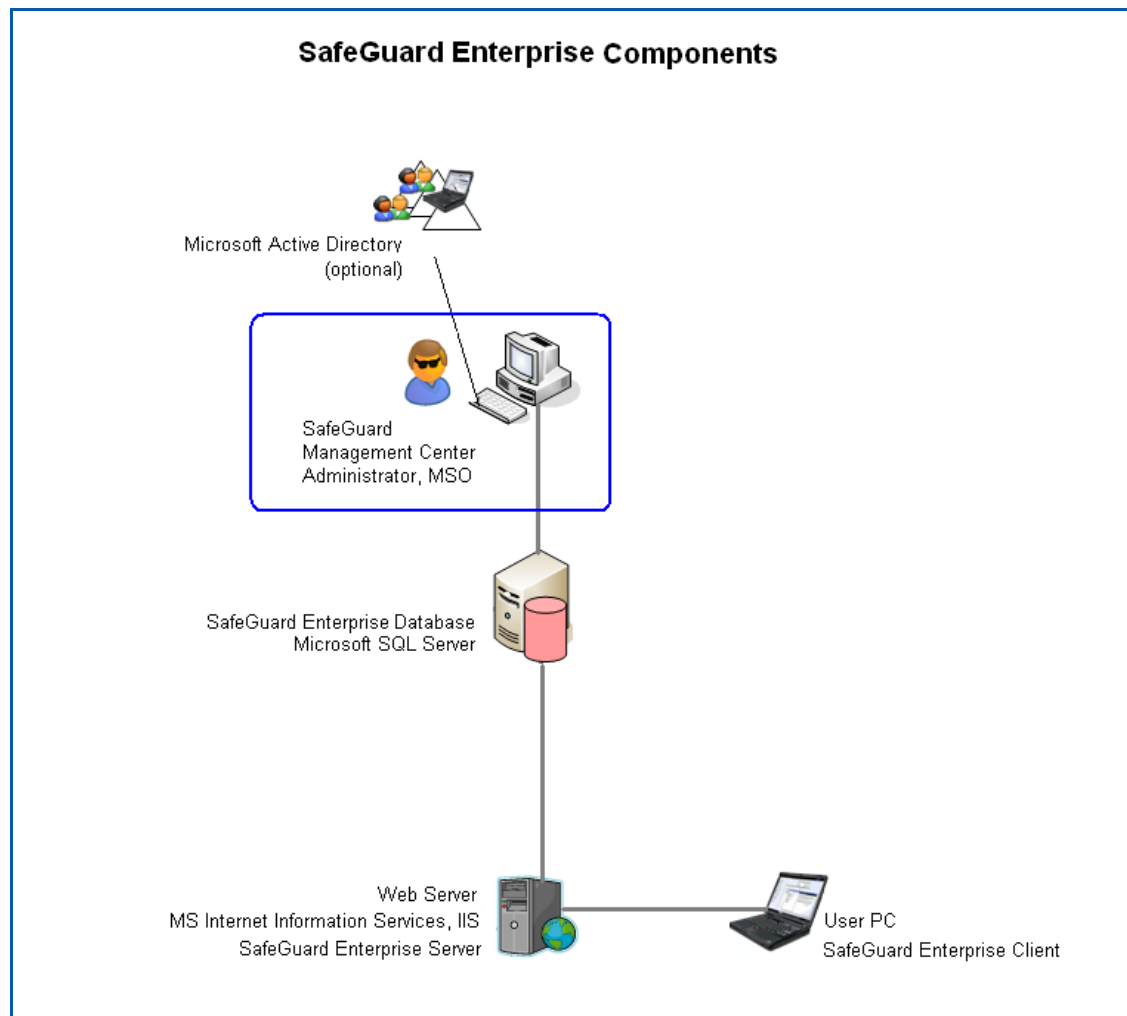
The SafeGuard Enterprise database and the associated tables have been created.

5 Setting up SafeGuard Management Center

This chapter describes how to install and configure the SafeGuard Management Center.

The SafeGuard Management Center is the central administrative tool for SafeGuard Enterprise. You install it on the administrator PCs that you intend to use for managing SafeGuard Enterprise. The 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 databases can be accessed.

The 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.



5.1 Prerequisites

The following prerequisites must be met:

- You need Windows administrator rights.
- .NET Framework 3.0 Service Pack 1 must be installed on the administrator PC. You can download it from <http://microsoft.com/downloads>.
- If you want to create a new SafeGuard Enterprise database during SafeGuard Management configuration, you need the necessary SQL access rights, see [Rights to access the database](#) on page 18.

5.2 Installing SafeGuard Management Center

You will find the required SGNManagementCenter.msi install package on the product CD.

1. Start SGNManagementCenter.msi from the product folder.
2. Click Next in the welcome window.
3. Accept the license agreement.
4. Select an installation path.
5. Select the installation type:
 - To install SafeGuard Management Center to support one database only, select an installation of type **Typical**.
 - To install SafeGuard Management Center to support multiple databases, select an installation of type **Custom**. Then activate the feature **Multi Tenancy**. This feature is not installed with an installation of type **Typical**.

For further information on the configuration of **Multi Tenancy** see [Configuring for multiple databases \(Multi Tenancy\)](#) on page 31.
6. Confirm that the installation has completed successfully.

The SafeGuard Management Center is installed. If necessary, restart your computer.

5.3 Configuring SafeGuard Management Center

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

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.

To ease configuration previously created configurations can also be imported from files or newly created database configurations can be exported to be reused at a later point in time.

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

Prerequisites

You should have the following information ready. Where necessary, you can obtain this information from your SQL administrator.

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

5.4 Carrying out initial configuration

To start the Configuration Wizard for initial configuration of the SafeGuard Management Center proceed as follows.

Hint: You need to carry out the following steps if for Single Tenancy as well as for Multi Tenancy configurations.

1. Start the SafeGuard Management Center. The SafeGuard Management Center Configuration Wizard opens automatically and guides you through the necessary steps.
2. In **Database Connection** configure the connection to the database server:

Select the SQL database server from the 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.

3. For the SafeGuard Management Center to be able to communicate with the database, you must specify an authentication method for the database access, either Windows NT authentication or SQL authentication.

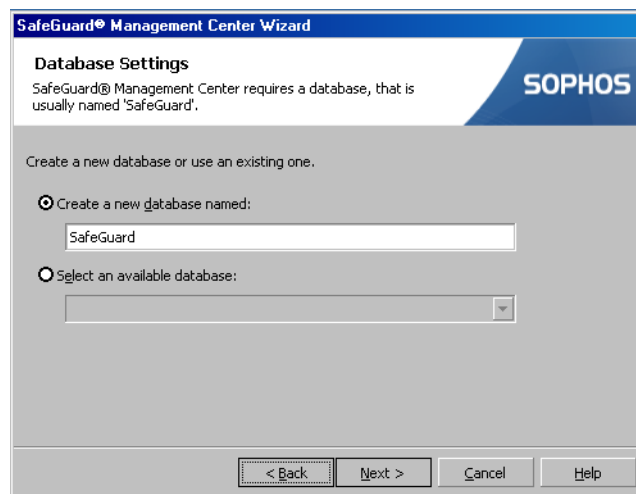
Notice: Use SQL authentication for computers that are not part of a domain, otherwise use Windows authentication. This, however, requires additional configuration.

If you use SQL authentication, we strongly recommend to secure the connection to the database with SSL to encrypt the transport of the SQL credentials.

SSL encryption requires a working SSL environment on the SQL database server which you have to set up in advance, see [Securing transport connections with SSL](#) on page 11.

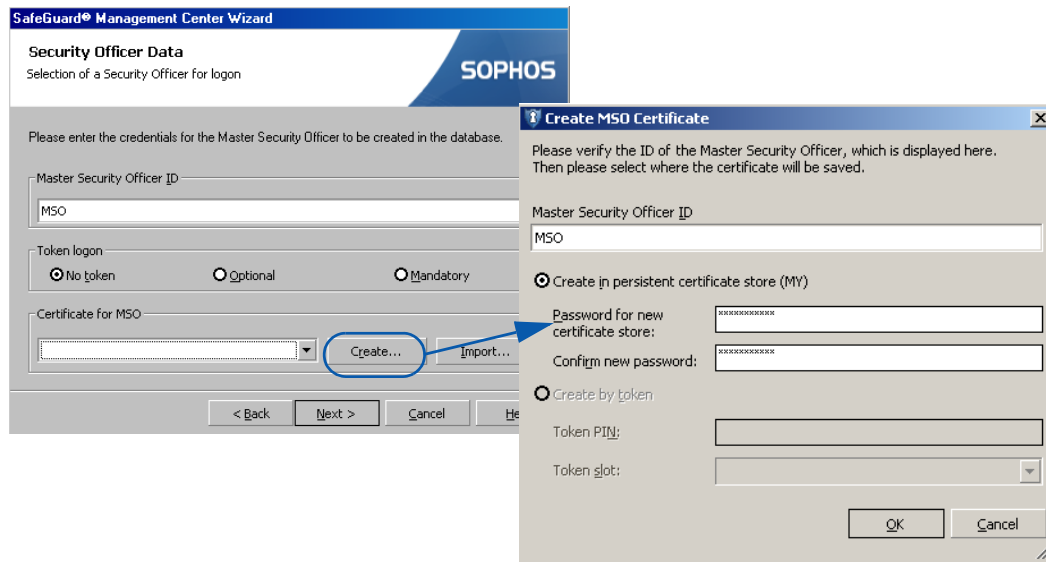
- a) Activate **Use SQL Server Authentication:** Enter the credentials for the SQL user account that your SQL administrator has created, in this example "sa" is used.

- b) Activate **Use SSL** to secure the connection between SafeGuard Management Center and SQL database server. If you have selected **SQL Server Authentication** this is strongly recommended in order to encrypt the transport of the SQL credentials.
4. Determine whether an existing or a new database will be used to store administration data.
- If a database does not yet exist, select **Create a new database named**. Enter a name for the new database, here "SafeGuard". To do this, you need the relevant SQL access rights, see [Rights to access the database](#) on page 18.
 - If a database has already been created or if you have already installed the Management Center on another administrator PC, click **Select an available database** and select the relevant database from the list.



5. Create a Master Security Officer (MSO).

Enter a name for the MSO. Initially, we recommend setting **Token logon** to **no token**. Logon with token or smartcard requires separate configuration which must be carried out within the Management Center. See the Administrator help, chapter Token and Smartcards. Once you have entered a name for the MSO click **Create**.



6. Enter the password for the certificate store twice and confirm with **OK**. The MSO certificate created is saved locally as a backup.

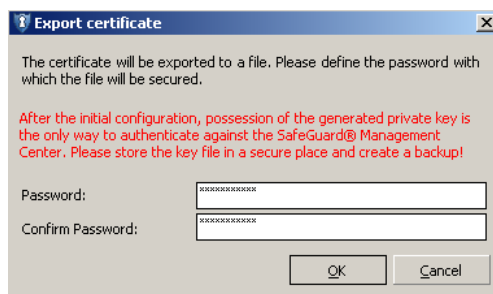
Notice: Make a note of this password! It is your private key for the SafeGuard Management certificate store. You will need it later to log on to the Management Center.

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.

7. The file in which the MSO certificate is stored - the so-called .p12 file - is secured by a password.

Thus, the MSO certificate has additional protection. Enter the password for the .p12 file twice and confirm with **OK**. The password must consist of 8 alphanumeric characters.



8. Enter a storage location for the certificate.

Notice: Create a backup of the private key (p12 file) for the MSO as in case of PC failure the key will be lost and SafeGuard Enterprise will have to be reinstalled. This applies to all SafeGuard generated security officer certificates.

The MSO certificate has now been created.

The screenshot shows a dialog box titled "Certificate for MSO". At the top, there is a "Token logon" section with three radio buttons: "No token" (selected), "Optional", and "Mandatory". Below this is a section for the certificate name, with a dropdown menu showing "CN=MSO, OU=Sophos SafeGuard@ Officer ..." and two buttons: "Create..." and "Import...". At the bottom of the dialog are four buttons: "< Back", "Next >", "Cancel", and "Help".

9. Click **Next**.

10. Create a new company certificate. Enter a name of your choice. The company certificate is used to differentiate between different SafeGuard Management installations. For security reasons, you should create a backup of the company certificate after initial configuration under **Tools > Options > Certificate** and store it in a safe location. In combination with the MSO certificate it allows for restoring a broken SafeGuard Enterprise database configuration.

The screenshot shows a dialog box titled "SafeGuard Management Center Wizard" with a sub-header "Company Certificate". Below the sub-header is the text "Create or restore the global certificate for your company" and the SOPHOS logo. There are two radio buttons: "Create a new company certificate" (selected) and "Restore using an existing company certificate". Under "Create a new company certificate", there is a text box for the company name and a note: "Please enter the company name to be stored in the company certificate. This is used to visually separate different installations." Under "Restore using an existing company certificate", there are three text boxes labeled "Subject:", "Serial number:", and "Expiry date:", and an "Import..." button. At the bottom are four buttons: "< Back", "Next >", "Cancel", and "Help".

11. Click **Next**, then **Finish**.

A configuration file is automatically created.

The initial configuration of the SafeGuard Management Center is now complete. The SafeGuard Management Center opens automatically.

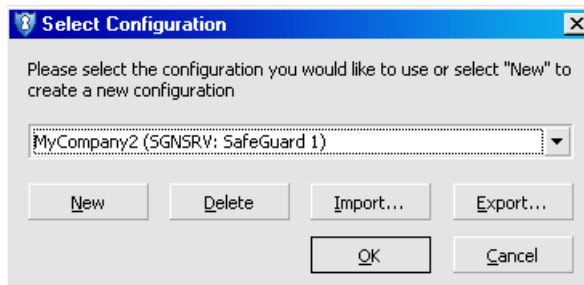
5.5 Configuring for multiple databases (Multi Tenancy)

To configure further database configurations to make use of Multi Tenancy proceed as follows.

Prerequisite: The feature Multi Tenancy must have been installed via a Custom installation.

Initial configuration must have been carried out, see [Carrying out initial configuration](#) on page 27.

1. Start the SafeGuard Management Center.
2. The existing database configuration created during initial configuration is displayed. Select the task you would like to carry out:



- To create a further SafeGuard Enterprise Database configuration, click **New**.
- To choose to work on an existing database, select it from the drop-down list and click **OK**.
- To import an existing database configuration from a file, click **Import...**
- To save a database configuration to a file, click **Export...**

3. Continue with the selected task.

5.5.1 Creating further database configurations

To create a further SafeGuard Enterprise Database configuration after initial configuration, proceed as follows:

1. Start the SafeGuard Management Center. The **Select Configuration** dialog will be displayed.
2. Click **New**. The SafeGuard Management Center Configuration Wizard opens automatically.
3. The Wizard will guide you through the necessary steps of creating a new database configuration, see [Carrying out initial configuration](#) on page 27. Make your settings as required. The new database configuration will be generated.
4. To authenticate to the SafeGuard Management Center you are prompted to select the Security Officer name for this configuration and to enter their certificate store password. Confirm with **OK**.

The SafeGuard Management Center will be opened and connected to the new database configuration. When the SafeGuard Management Center is started for the next time, you can select the new database from the list.

5.5.2 Connecting to an existing database configuration

To work on an existing database configuration, proceed as follows:

1. Start the SafeGuard Management Center. The **Select Configuration** dialog will be displayed.
2. Select the required database configuration from the drop-down list and click **OK**. The selected database configuration is connected to the Management Center and will become active.
3. To authenticate to the SafeGuard Management Center you are prompted to select the Security Officer name for this configuration and to enter their certificate store password. Confirm with **OK**.

The SafeGuard Management Center will be opened and connected to the selected database configuration.

5.5.3 Exporting a configuration to a file

To save a database configuration in order to reuse it later on, you may export it to a file. To do so, proceed as follows:

1. Start the SafeGuard Management Center. The **Select Configuration** dialog will be displayed.
2. Click **Export...**
3. To secure the configuration file you are prompted to enter and confirm a password that will encrypt the parts configuration file. Click **OK**.



4. Specify a file name and storage location for the exported configuration file *.SGNConfig.
5. In case this configuration already exists you are asked if you want to overwrite the existing configuration.

The database configuration is saved to the specified storage location.

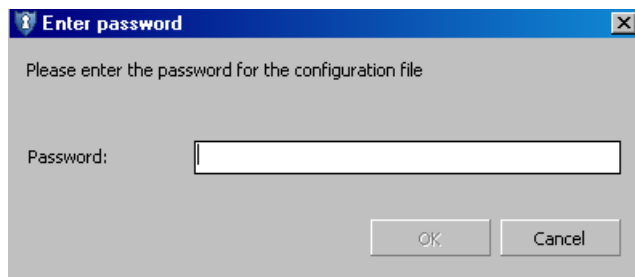
5.5.4 Importing a configuration

To use or change a database configuration you may import a previously created configuration into the SafeGuard Management Center. There are two ways to do so:

- via the SafeGuard Management Center (for Multi Tenancy)
- by double-clicking the configuration file (for Single and Multi Tenancy)

5.5.5 Importing a configuration via the SafeGuard Management Center

1. Start the SafeGuard Management Center. The **Select Configuration** dialog will be displayed.
2. Click **Import...**, locate the required configuration file and click **Open**.
3. Enter the password for the configuration file defined during the export and click **OK**.



4. The selected configuration will be displayed. Confirm to activate it with **OK**.
5. To authenticate to the SafeGuard Management Center you are prompted to select the Security Officer name for this configuration and to enter their certificate store password. Confirm with **OK**.

The SafeGuard Management Center will be opened and connected to the imported database configuration.

5.5.6 Importing a configuration by double-clicking the configuration file (Single and Multi Tenancy)

Notice: Note that this task is possible in Single-Tenancy and Multi Tenancy mode.

It is also possible to export a configuration and distribute it to several security officers. The security officers then only need to directly double-click the configuration file to open a fully configured SafeGuard Management Center.

This is advantageous when you use SQL authentication for the database and to avoid that the SQL password is known by every administrator. You then only need to enter it once, create a configuration file and distribute it to the respective Security Officers' computers.

Prerequisite: The initial configuration of the SafeGuard Management Center must have been carried out.

1. Start the SafeGuard Management Center via the product folder of the **Start** menu.
2. Select **Options** from **Tools** menu and select the tab **Database Connection**.
3. Enter or confirm the credentials for the SQL Database Server connection.
4. Click **Export configuration** to export this configuration to a file.
5. Enter and confirm a password for the configuration file.
6. Enter a file name and select a storage location.
7. Distribute this configuration file to the security officers' computers. Let them know the password for this file as well as the certificate store password needed to authenticate at the SafeGuard Management Center.
8. The security officers just need to double-click the configuration file.
9. They are prompted to enter the password for the configuration file.
10. To authenticate to the SafeGuard Management Center, they are prompted to enter their certificate store password.

The SafeGuard Management Center starts with the imported configuration and this configuration will be made the new default configuration.

5.5.7 Fast switching of database configurations

To ease administrative task for several tenants SafeGuard Management Center allows for fast switching of database configurations.

To switch to another database configuration:

1. In the Management Center select **Change configuration...** from the **File** menu.
2. Select the database you want to switch to from the drop-down list.
3. Select **OK**.

The Management Center is automatically restarted with the selected configuration.

Notice: Note that this task is only possible in Multi Tenancy mode.

5.6 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.

5.6.1 Logon in Single Tenancy mode

1. Start the SafeGuard Management Center via the **Start** menu.
2. You will see a logon dialog.



3. Log on as an MSO and enter the certificate store password specified during initial configuration. Click **OK**.

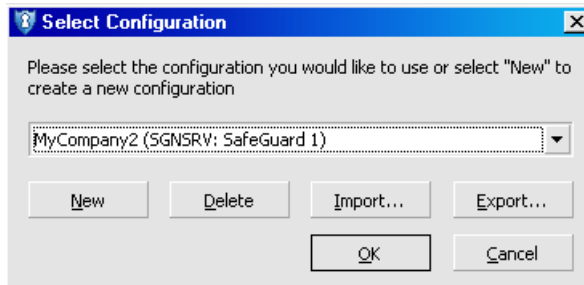
Hint: If you enter an incorrect password, an error message will be displayed and a delay will be imposed for the next logon attempt. The delay period will be increased with each failed logon attempt. Failed attempts will be logged.

The SafeGuard Management Center is opened.

5.6.2 Logon in Multi Tenancy mode

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

1. Start the SafeGuard Management Center via product folder of the **Start** menu. The **Select Configurations** dialog will be displayed.



2. Select the database configuration you want to use from the drop-down list and click **OK**. The selected database configuration is connected to the Management Center and will become active.
3. To authenticate to the SafeGuard Management Center you are prompted to select the Security Officer name for this configuration and to enter their certificate store password. Confirm with **OK**.



The SafeGuard Management Center will be opened and connected to the selected database configuration.

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

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

5.7 Installing SafeGuard Management Center on further computers

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

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

The following steps relate to the configuration of a second Management Center installation.

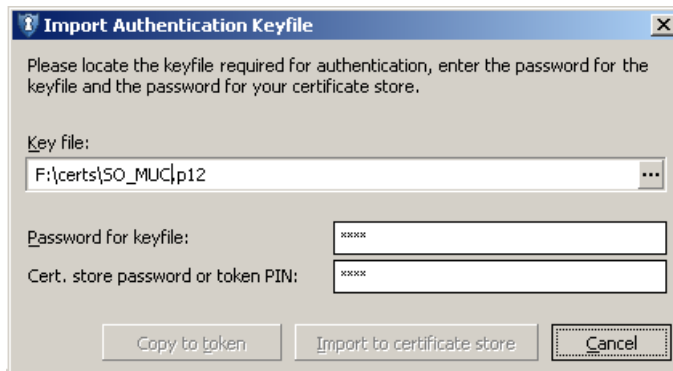
1. Install SGNManagementCenter.msi on a further computer with the required features.
2. Open the SafeGuard Management Center. The Configuration Wizard is started.
3. Select the database to which this Management Center instance is to be connected to.
4. The **SafeGuard Management Center Authentication** dialog is displayed. Select an authorized person from the drop-down list. If Multi Tenancy is enabled, the Authentication dialog shows at which configuration the user is going log on to.
5. Now enter the password for the certificate store.

Notice: After entering this password, a certificate store is created for the current user account and is protected by this password. You require only this password for any subsequent logon.

6. Click OK.

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

7. To import the data, click Yes.



8. Click OK. This will start the import process.
9. Click [...] to select the key file.

10. Now enter the **password for keyfile**.

11. Enter the password for the certificate store previously defined in **Cert. store password or token PIN**.

12. Click **Import to certificate store**.

Click **Copy to token** to store the certificate on a token.

13. You need to enter the password once more to initialize the certificate store.

Certificates and private keys are now contained in the certificate store.

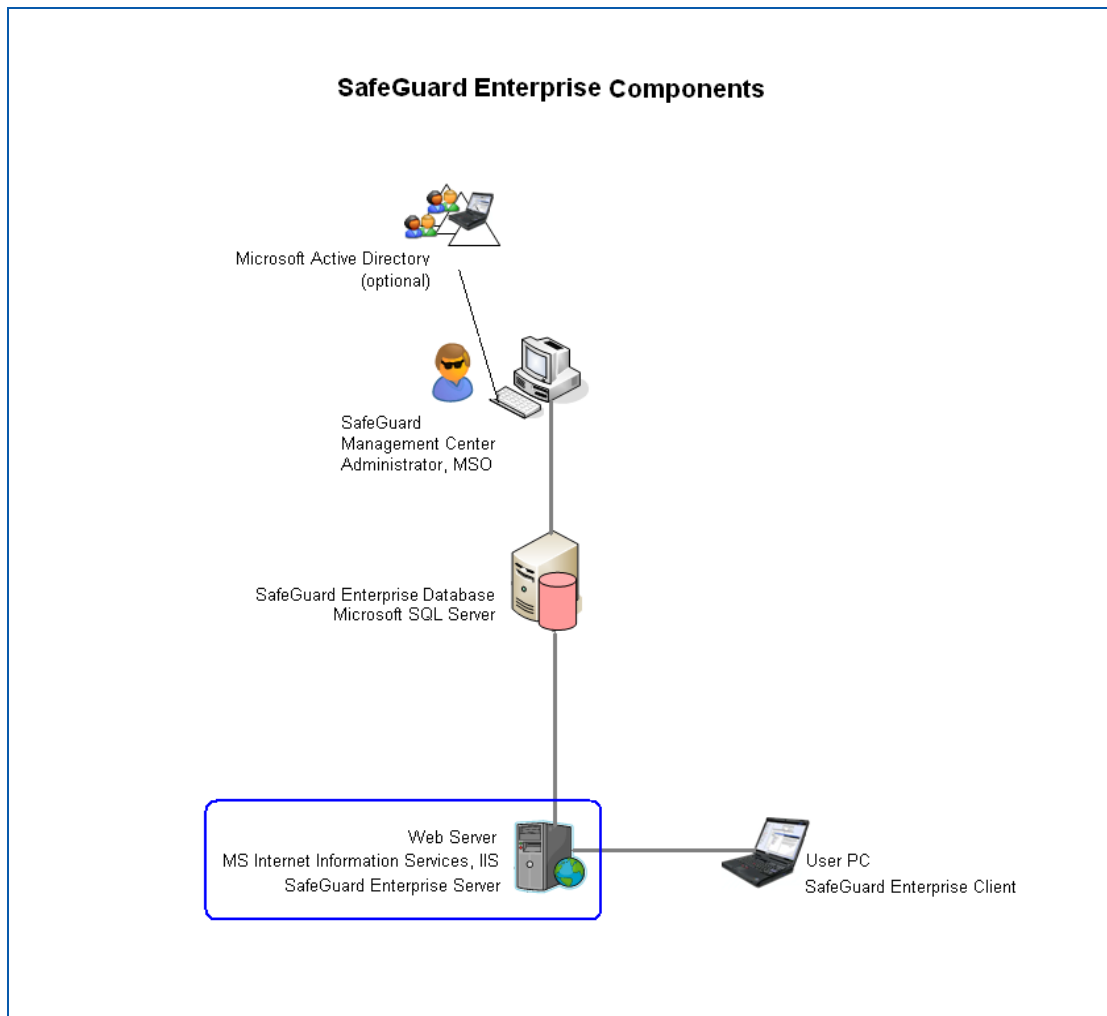
Logging on to the SafeGuard Management Center then requires the password to the certificate store.

6 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 an IIS-based web server.

We recommend to use a dedicated IIS server for the SafeGuard Enterprise Server. This will improve 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 an IIS server. To do this, you first have to configure Microsoft Internet Information Services (IIS).



6.1 Prerequisites

The following prerequisites must be met (in this sequence):

- You need Windows administrator rights.
- Microsoft Internet Information Services (IIS) must be installed and hardened.
IIS is available free of charge. You will find the program e.g. on your Windows CD or on the Microsoft website.
- If you use SSL transport encryption between SafeGuard Enterprise Server and Enterprise Client you have to set up the IIS for it in advance, see [Securing transport connections with SSL](#) on page 11:
 - 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 3.0 Service Pack 1 is installed.
.NET Framework is available free of charge. You will find the program e.g. on your Windows CD. Depending on the Windows version it will have already been installed by default.
- ASP.NET 2.0 is activated. This is automatically checked and correctly set during installation.
- For Windows Server 2008, **IIS Management Scripts and Tools** needs to be enabled.

6.2 Configuring Microsoft Internet Information Services

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

6.2.1 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.

Hint: You will 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 website.

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 Enterprise Management Center latest version
 - Microsoft SQL Server 2005 Express
 - IIS with minimal components
- Server 2:
 - Microsoft Windows Server 2003 SP2
 - 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 will be automatically disabled,
- Client:
 - SafeGuard Enterprise Client
 - SafeGuard Management Center latest version

Installing only necessary IIS components

Ensure that only essential and necessary IIS components are installed as this will reduce the chance that the IIS server might be attacked. Disable all unnecessary settings.

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

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

Enabling only essential Web Service Extensions

Ensure that only essential Web Service Extensions are enabled as this will reduce 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**

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

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

Setting 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)

Disable Integrated Windows Authentication

It is recommended to 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, deselect the **Windows Integrated Authentication** check box.
4. Click **OK** twice.

Settings for Application Pool “DefaultAppPool”

- 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 will fail.

6.2.2 IIS rollout name

During IIS setup a standard user is created on the IIS server with standard rights. When SafeGuard Enterprise Server is installed on the IIS server a standard IIS SafeGuard user will be created with standard IIS rights and the following logon name: `IUSR_SafeGuardServerUser`. This will help to authenticate to the IIS server in case it is renamed after installation as this specific SafeGuard IIS user can always be used as a valid logon name.

6.2.3 Testing .NET Framework registration

Check whether .NET Framework Version 3.0 with Service Pack 1 is installed on the IIS server.

1. To do this, open **Control Panel** and, depending on the operating system, either select **Add/Remove Programs** or **Administrative Tools**. The program and version are shown there.
2. If necessary, install the correct version of the program.

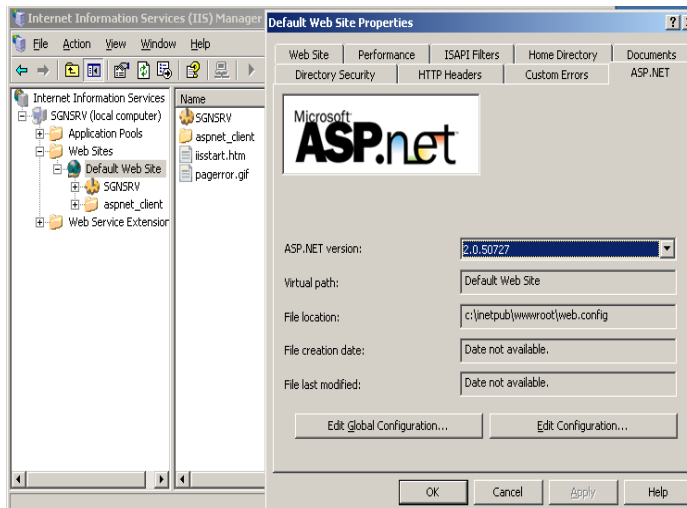
6.2.4 Checking ASP.NET registration

During SafeGuard Enterprise Server installation it is checked whether the required ASP.NET Version 2.0.50727 is set. If it is not set, the correct version will automatically be enabled during installation.

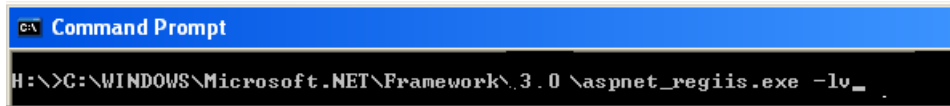
You can check the setting manually as follows:

Hint: You will find a detailed description on how to carry out this task in our knowledge database: <http://www.sophos.com/support/knowledgebase/article/107703.html>.

1. Open the **Internet Information Services Manager** on the IIS server.
2. In IIS Manager click **Server (local computer) > Web Sites**.
3. Right-click **Default Web Site > Properties > ASP.NET**. Version 2.0.50727 should show under **ASP.NET Version**. If appropriate, select this version. If this is not possible, you must re-install ASP.Net 2.050727.
4. Confirm with **Apply** and **OK**.



5. Alternatively, you can select the command `aspnet_regiis.exe -lv` to ensure that ASP Services Version 2.0 is installed.



6.2.5 Additional IIS 6 configuration when installing SafeGuard Enterprise Server on Windows Server 2003 64 bit

When you operate IIS version 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
```

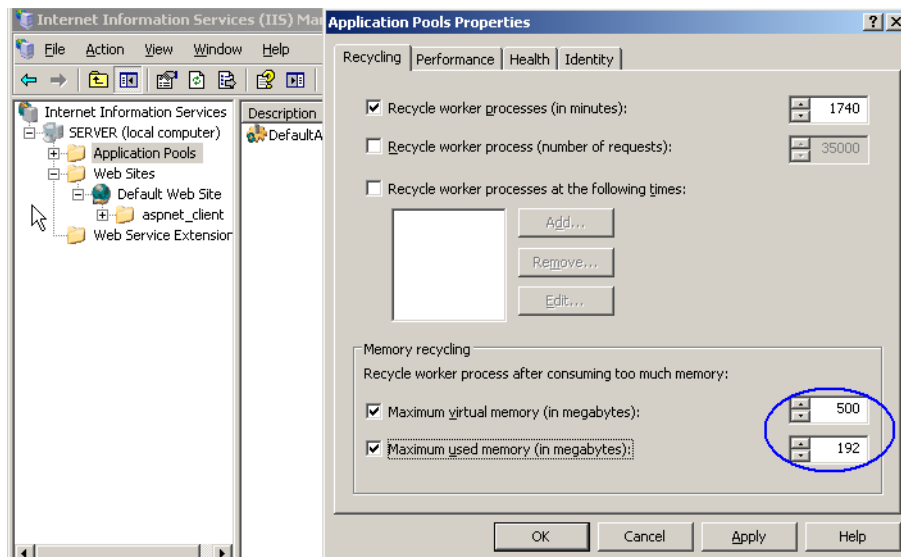
3. Activate the 32 bit version of ASP.Net 2.0.50727:

- Open the **Internet Information Services Manager** on the IIS server.
- In IIS Manager click **Server (local computer) > Web Service Extensions**.
- Right-click **ASP.NET v2.0.50727 (32 bit)**, select **Properties** and set the status to **Allowed**.
- Confirm with **Apply** and **OK**.

6.2.6 Enabling recycling for the IIS server

We recommend enabling "Recycle worker processes" for the IIS:

1. Open the **Internet Information Services Manager**.
2. In IIS Manager, click **Server (local computer)**.
3. Right-click **Application Pools > Properties**.
4. Under **Memory recycling**, set the following values:
 - Maximum virtual memory = 500 MB
 - Maximum used memory = 192 MB
5. Confirm with **Apply** and **OK**.



The IIS server is now set up for SafeGuard Enterprise.

6.3 Installing SafeGuard Enterprise Server

After the IIS is configured, you can install SafeGuard Enterprise Server on the IIS server. You will find the install package `SGNServer.msi` on the product CD.

1. Start `SGNServer.msi` from the product CD.
2. Click **Next** in the welcome window.
3. Accept the license agreement.
4. Select an installation path.
5. Confirm that the installation has completed successfully.

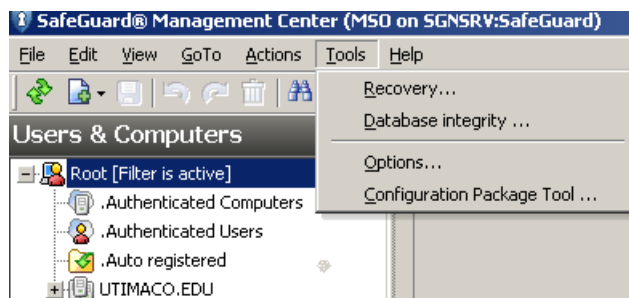
The SafeGuard Enterprise Server is installed.

Notice: To enhance performance, the concatenation of logged events is deactivated for the SafeGuard Enterprise Database by default after installation of the 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 via an integrity check. To make use of integrity protection you thus need to set the concatenation manually. For detailed information see the SafeGuard Enterprise Administrator help, chapter “Reports”.

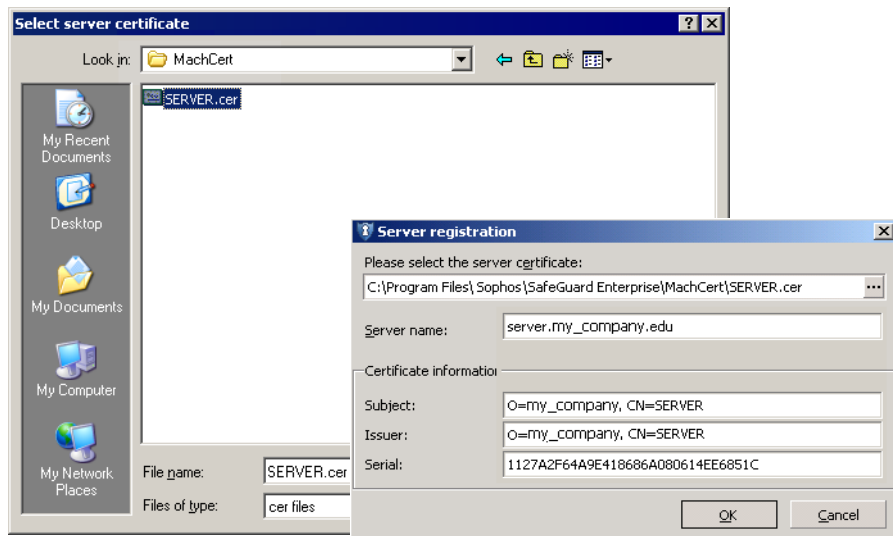
6.4 Registering and configuring SafeGuard Enterprise Server

The SafeGuard Enterprise Server still needs to be registered and configured. This is carried out with the SafeGuard Management Center Configuration Package Tool. A configuration file needs to be created for the server and deployed on it.

1. Start the Management Center and select **Tools > Configuration Package Tool**.



2. Select **Register Server** and then one of the following options:
 - **Make this computer an SGN Server:** SafeGuard Management Center and SafeGuard Enterprise Server are installed on the PC that you are currently working on. This option is not available if Multi Tenancy is enabled.
 - **Add:** The SafeGuard Enterprise Server is installed on a different PC than the SafeGuard Management Center.
 - **Add server role:** add further security officer roles for the selected server if required.
 - **Remove:** The selected SafeGuard Enterprise Server is removed from the list.
3. 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 PC than the SafeGuard Management Center, this .cer file must be accessible in the form of a copy or a network permission.



Notice: Do not select the MSO certificate!

4. Under **Server name**, enter the FQDN, e.g. server.mycompany.edu and confirm with **OK**.

Notice: 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. You have selected to **Make this computer an SGN Server:**
 - a) SafeGuard Enterprise Server Configuration Setup is automatically started.
 - b) Confirm all following dialogs.

The computer is registered as SafeGuard Enterprise Server.

6. The server and its properties are displayed in the **Register Server** tab.

You can set the following properties for the selected server:

- **Scripting allowed:** Activate to enable use of the SafeGuard Enterprise Management API.
- **Server roles:** Click to select a security officer role. Click **Add server role...** at the bottom to add further security officer roles.
- **Database connection:** Click [...] to configure a specific database connection for any registered web server, including database credentials and SSL transport encryption between the web server and the database server. The **Database Connection** dialog will be displayed.

Hint: SSL encryption requires a working SSL environment and additional configuration, see [Setting up SSL](#) on page 12.

7. In **Database Connections** configure the connection between database and server:

- a) Select the required database server the selected SafeGuard Enterprise Server is to be connected to.
- b) Activate **Use SSL** to secure the connection between this database and the selected server with SSL.
- c) In **Authentication** define the database credentials to be used for the selected database:
 - Windows authentication
 - SQL authentication

Notice: Use SQL authentication for computers that are not part of a domain, otherwise use Windows authentication. This however requires additional configuration.

If you use SQL authentication, we strongly recommend to secure the connection to the database with SSL to encrypt the transport of the SQL credentials.

- d) Check the connection to the database. Even if the check is not successful a new server configuration package can be created.

Hint: You can change the properties and settings for any registered server and its database connection at any point in time. You do not have to rerun the Management Center Configuration Wizard to update the database configuration. Simply ensure to create a new server 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.

8. You have selected **Add**:

- a) Switch to the **Create Server Configuration Package** tab.
- b) Select the server required.
- c) Specify the output path.
- d) Click **Create Configuration Package**. A server configuration file (.msi file) named `<Server>.msi` is created under the output path (in this example, `server.mycompany.edu.msi`).

You have finished registering and configuring SafeGuard Enterprise Server. Deploy the Server configuration package to the SafeGuard Enterprise Server.

Note: If you want to install a new server configuration package ensure to uninstall the “old” `ServerConfig.msi` before installing a new `ServerConfig.msi` on the server.

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 prior to the connection test:

Ports/connections

The endpoint computers must create the following connections:

Connection to	via Port
SafeGuard Enterprise Server	Port 80/TCP

The SafeGuard Management Center needs to create the following connections:

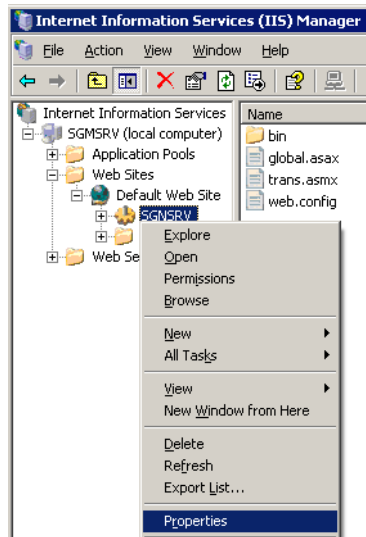
Connection to	via Port
SQL database	Port 1433/TCP and Port 1434/TCP for SQL 2005 (Express) dynamic port
Active Directory	Port 389/TCP
SLDAP	Port 636 for the Active Directory import

The SafeGuard Enterprise Server needs to create the following connections:

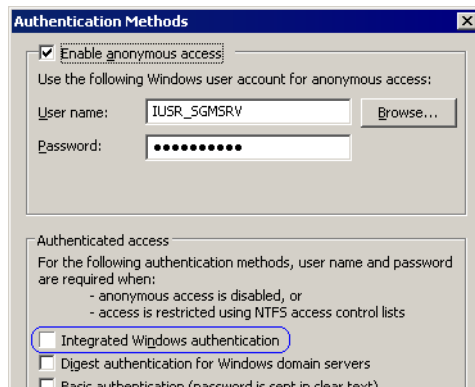
Connection to	via Port
SQL database	Port 1433/TCP and Port 1434/TCP for SQL 2005 (Express) dynamic port
Active Directory	Port 389/TCP

Authentication method

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



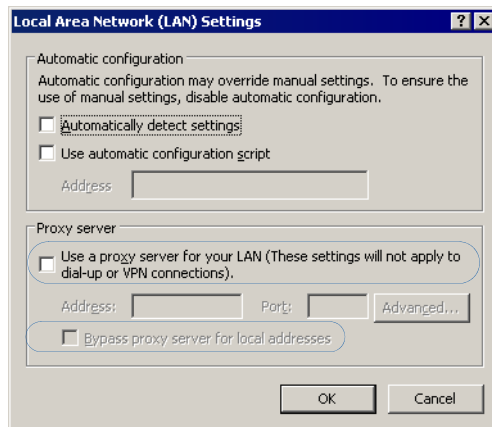
4. Select the Directory Security tab.
5. In the Authentication and Access Control box, click Edit.
Activate Enable anonymous access and deactivate Integrated Windows authentication.



Proxy server settings for web server and endpoint computer

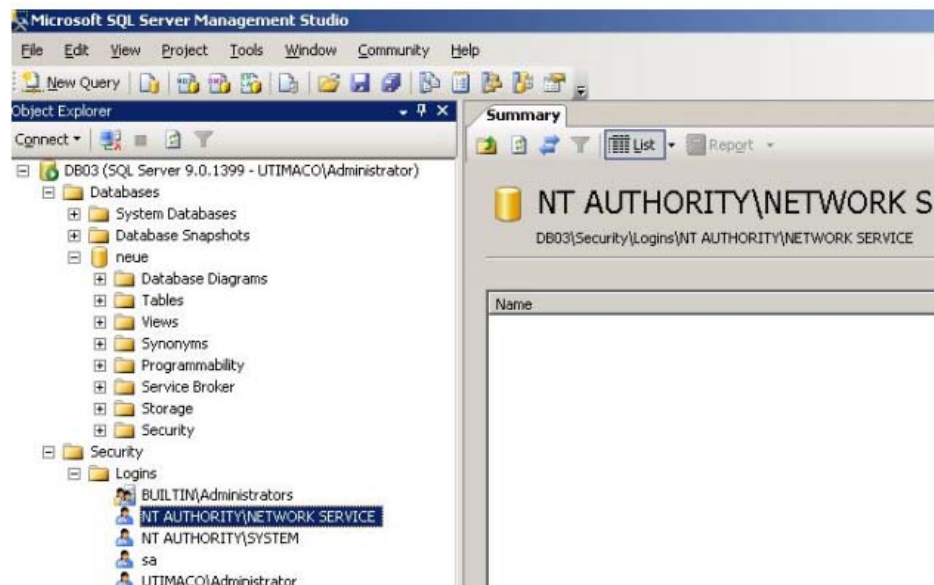
Proxy server settings should be as follows:

1. In Internet Explorer select Tools > Internet options > Connections > LAN settings.
2. Deactivate Use a proxy server for your LAN.
3. If a proxy server is required, activate Bypass proxy server for local addresses.



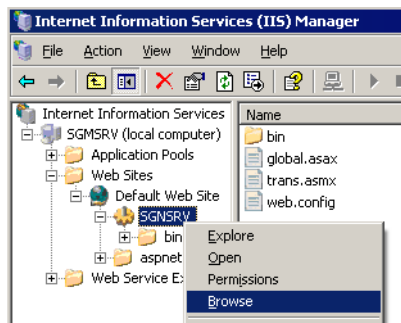
Microsoft SQL Server 2005 settings

If using Microsoft SQL Server 2005 you need to add the following users in Microsoft SQL Server Management Studio (Role "sysadmin"):

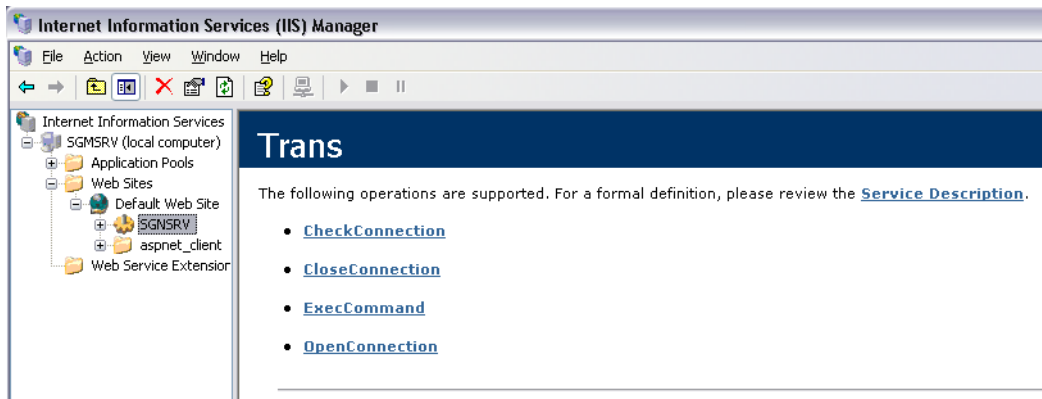


7.2 Performing connection test

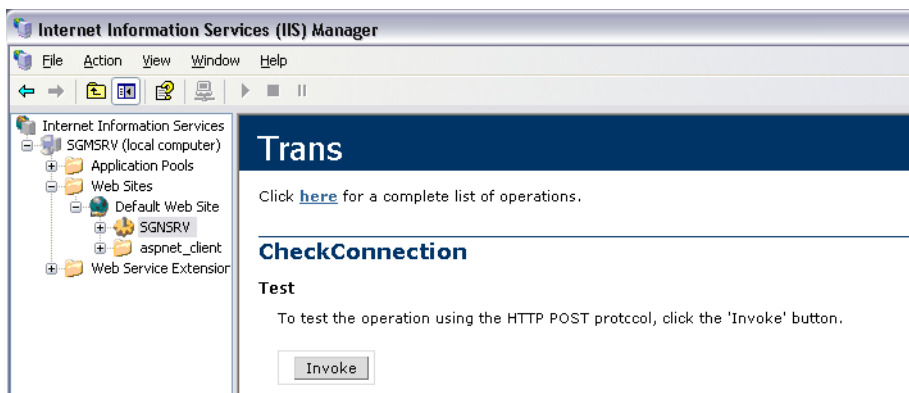
1. On the SafeGuard Enterprise Server, open the Internet Information Services (IIS) Manager.
2. In IIS Manager click Server (local computer) > Web Sites > Default Web Site.
3. Right-click the server you want and then Browse.



4. Click the Check Connection link.

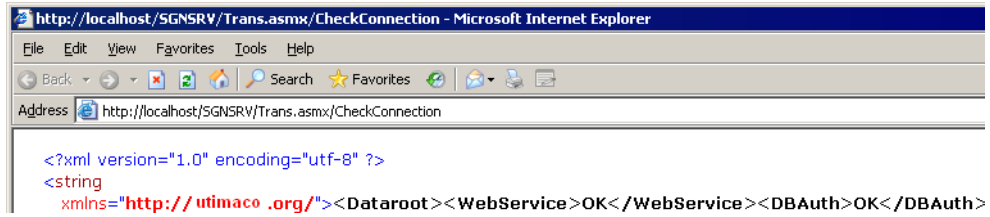


5. Test the connection by clicking Invoke.



If you receive the output below, the connection test has been successful:

- WebServices ok
- DBAuth ok



8 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.

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

8.1 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.

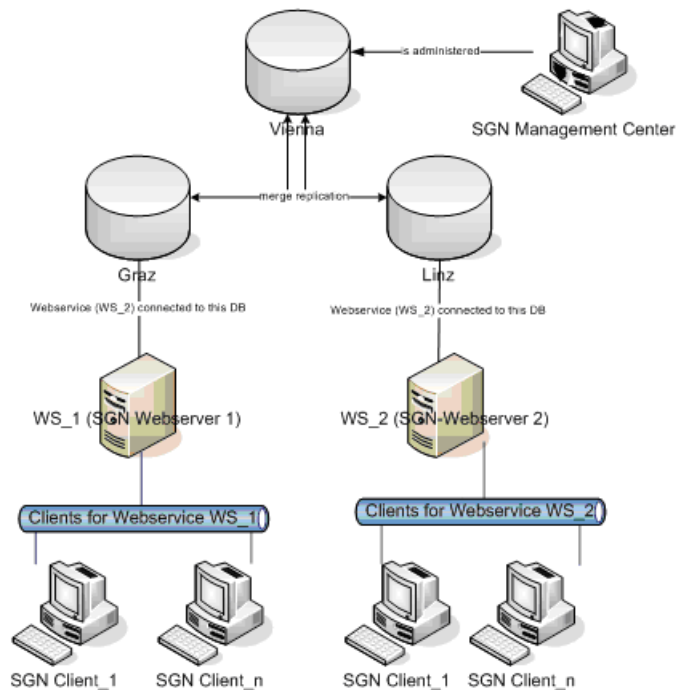
Merge replication allows various sites to work autonomously and at a later time merge updates into a single, uniform result. The initial snapshot is applied to Subscribers, and then Microsoft SQL Server tracks changes to published data at the Publisher and at the Subscribers. The data is synchronized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

8.2 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 via the web servers are also passed on to the Microsoft SQL Server 2005 by way of the replication mechanism.



8.2.1 Generating 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.

There are two ways to proceed:

- via the SafeGuard Management Center Configuration Wizard
This procedure requires that the SafeGuard Management Center is already installed, see [Installing SafeGuard Management Center](#) on page 25.
- via an SQL script you can find on the product CD.
This procedure is often preferred if extended SQL permissions during SafeGuard Management configuration is not desirable, see [Setting up SafeGuard Enterprise Database](#) on page 16.

8.2.2 Generating 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.

Hint: 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 if its data records.

To generate the replication databases proceed as follows:

1. When using distributed databases you first have to create a publication for the master database via the management console of the SQL server.
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 will 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. Proceed with installing the SafeGuard Enterprise Server.

8.3 Installing and configuring SafeGuard Enterprise Server

To install SafeGuard Enterprise Server on the web servers proceed as follows. For installation details see [Setting up SafeGuard Enterprise Server](#) on page 39.

1. Install SafeGuard Enterprise Server on server WS_1.
2. Install SafeGuard Enterprise Server on server WS_2.
3. Register the servers in the SafeGuard Management Center via **Tools > Configuration Package Tool > Register Server >Add**.
4. You are asked to add the server certificates ws_1.cer and ws_2.cer. You will find them in:
 \Program Files\Sophos\SafeGuard Enterprise\MachCert\ folder. These certificates are needed to create the appropriate server and client configuration packages.

The SafeGuard Enterprise servers are installed and registered. You now need to create the server and the client configuration packages for both of them.

8.3.1 Generating the configuration packages for the Graz database

Create the server and client configuration package for the Graz database. Start the SafeGuard Management Center and proceed as follows:

1. Link the SafeGuard Management Center with the Graz database: In **Tools > Options** select **Database Connection** and select WS_1 as **Database Server** and Graz as **Database**.
2. In **Tools > Configuration Package Tools > Create Server Configuration Package** create the Server configuration package.
3. In **Tools > Configuration Package Tools > Create Configuration Package (managed)** create the configuration package for the SafeGuard Enterprise protected endpoint computer. Make sure to select the correct server the Graz clients are to be connected to. In the example this is WS_1.

8.3.2 Generating the configuration packages for the Linz database

To create the server and client configuration package for the Linz database, start the SafeGuard Management Center and proceed as follows:

1. Link the SafeGuard Management Center with the Linz database: In **Tools > Options** select **Database Connection** and select `WS_2` as **Database Server** and `Linz` as **Database**.
2. In **Tools > Configuration Package Tools > Create Server Configuration Package** create the Server configuration package.
3. In **Tools > Configuration Package Tools > Create Configuration Package (managed)** create the configuration package for the SafeGuard Enterprise protected endpoint computers. Make sure to select the correct server the Linz clients are to be connected to. In the example this is `WS_2`.
4. Once you have created the client and server configuration packages, link the SafeGuard Management Center with the **Vienna** database again.

8.3.3 Installing the server configuration packages

To install the server configuration packages on the web servers, proceed as follows:

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 services `WS_2`, which is to communicate with the Linz database.

If communications between the SafeGuard Enterprise Server and these databases are running correctly, you can then install the SafeGuard Enterprise Clients.

8.4 Installing and configuring SafeGuard Enterprise Client software

You install the SafeGuard Enterprise Clients in the same way as for SafeGuard Enterprise without replication. For details see [Setting up endpoint computers centrally](#) on page 76 or see [Setting up endpoint computers locally](#) on page 91.

For the correct configuration make sure to install the correct client configuration package after you have installed each SafeGuard Enterprise Client. According to the example proceed as follows:

1. Install the Graz Client configuration package on the clients to be connected to the Graz server WS_1.
2. Install the Linz Client configuration package on clients to be connected to the Linz server WS_2.

For information on updating replicated SafeGuard Enterprise databases see [Updating SafeGuard Enterprise replicated databases](#) on page 106.

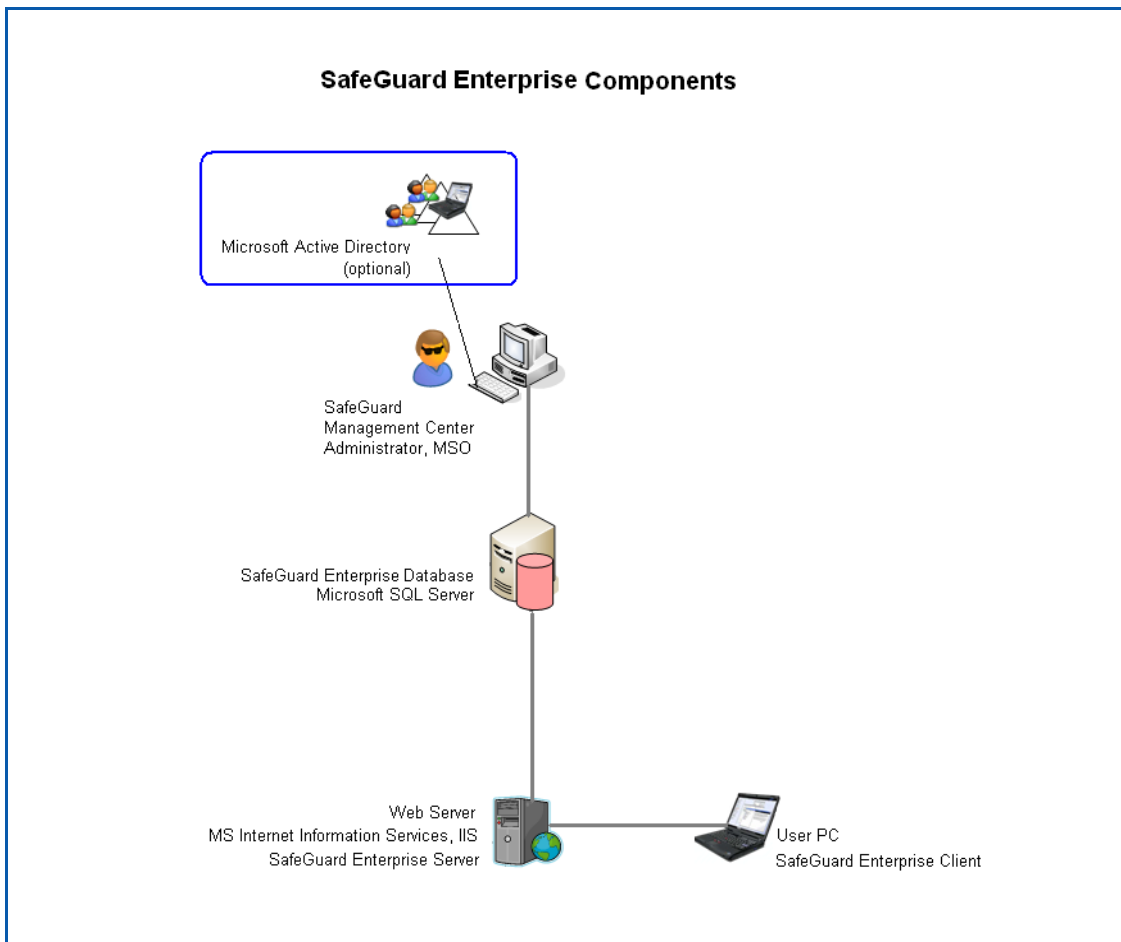
9 Setting up an organizational structure

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

- by creating the company structure manually
- by importing a directory service, e.g. an Active Directory

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. Note that in this case the organizational units created manually are not mapped in the AD.

If organizational units that you have created in SafeGuard Enterprise are also to be mapped in the AD, you must add these to the AD.



9.1 Creating an organizational structure manually

If you do not want to import your organizational structure from an Active Directory or if there is no directory service available, you can implement the organizational structure manually by creating new domains/workgroups which the user/computer can log on to.

To create a new domain, proceed as follows:

To display, open the SafeGuard Management Center and click **Users & Computers**.

1. Select **Root [filter is active]** in the navigation window on the left.
2. In the context menu, select **New > Create new domain (auto registration)**.
3. Enter the following information about the domain controller in **Common information**. All three name entries must be correct otherwise the domain will not be synchronized:
 - a) **Full name:** For example *computer name.domain.com* or the IP address of the domain controller
 - b) **Distinguished name:** DNS name, for example
`DC=computername3,DC=Domain,DC=Country`
 - c) A description for the domain (optional)
 - d) **Domain NetBios:** Name of the domain controller
 - e) The type of object is displayed under **Connection state**, in this case `Domain`.
 - f) To prevent policy inheritance, you may activate **Block Policy Inheritance**.
4. Confirm details with **OK**.

To create a new workgroup, proceed as follows:

To display, open the SafeGuard Management Center and click **Users & Computers**.

1. Select **Root [filter is active]** in the navigation window on the left.
2. In the context menu, select **New > Create new workgroup (auto registration)**.
3. Enter the following information in **Common information**:
 - a) **Full name:** a name for the workgroup
 - b) A description for the workgroup (optional)
 - c) The type of object is displayed under **Connection state**, in this case `Workgroup`.
 - d) To prevent policy inheritance, you may activate **Block Policy Inheritance**.

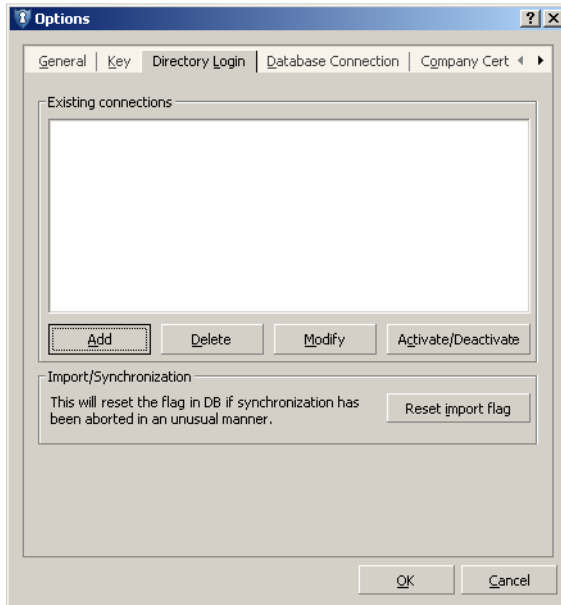
4. Confirm details with **OK**.

The new domain/workgroup has now been created. The users/computers within this domain will be automatically assigned to this domain/workgroup when they log on. Continue in the same way until your organizational structure has been created.

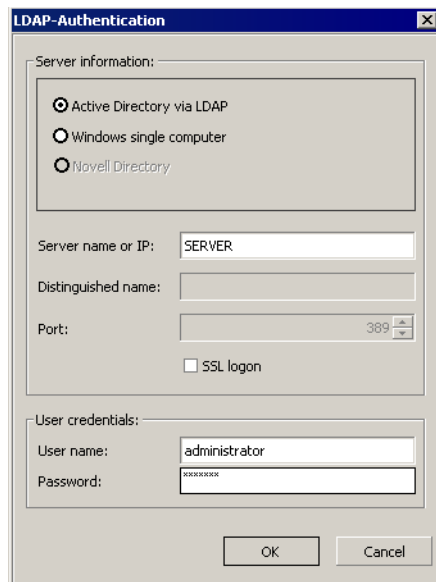
9.2 Importing an organizational structure

You have the option of importing an existing organizational structure to the SafeGuard Enterprise database, e.g. via an Active Directory.

1. Start the SafeGuard Management Center.
2. Select **Tools > Options > Directory Login** and click **Add**.



- a) LDAP Authentication appears.

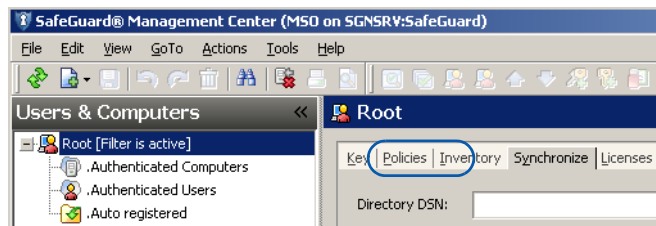


- b) For **Server name or IP**, enter the NetBIOS name of the domain controller or its IP address.
- c) For **User name and password** enter your Windows credentials.

Hint: Windows single computer: A directory must be approved on the PC to enable a connection via LDAP.

When synchronizing users and their group membership, membership to a 'primary group' will not be synchronized as it is not visible for the group.

- 3. Confirm with **OK**.
- 4. Click **Users & Computers**.
- 5. In the left-hand navigation window, click the root directory **Root [filter is active]**.
- 6. Select **Synchronize**.



- 7. Select the required directory from the DSN list. Click the magnifier icon, top right. A graphical representation of the Active Directory Structure of the organizational units (OU) in your company will appear.
- 8. You do not need to import the entire contents of the Active Directory. Highlight the organizational units (OU) to be synchronized.
- 9. Click **Synchronize**.
- 10. Confirm synchronization with **OK**.

Synchronization of the SafeGuard Management Center and Active Directory is complete. The imported objects are displayed in the **Users & Computers** area. You can view a synchronization protocol in the status bar at the left. When clicking on it, you can copy this protocol to the clipboard and paste it into an E-mail or file in case you would like to inform your users on the synchronization results.

10 SafeGuard configurations for endpoint computers

Endpoint computers can be configured as follows:

- as SafeGuard Enterprise Clients (managed) with central server-based management via the SafeGuard Management Center.

For SafeGuard Enterprise Clients (managed) a connection to the SafeGuard Enterprise Server exists. They receive their policies via 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.

- as Sophos SafeGuard Clients (standalone) with local management via the SafeGuard Management Center.

For Sophos SafeGuard Clients (standalone) no connection to the SafeGuard Enterprise Server is ever established at any point in time. They therefore receive their policies in configuration packages via third party mechanisms.

Note: Check your network and computers for outdated or unused configuration packages and, for security reasons, make sure to delete them.

10.1 Restrictions

AHCI

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.

Dynamic and GPT disks

Dynamic and GUID partition table (GPT) disks are not supported. In such cases, the installation will be terminated. If such disks can be found on the computer at a later point in time, they will not be supported.

SCSI hard disks

The SafeGuard Enterprise Device Encryption Client does not support systems that are equipped with hard disks attached via a SCSI bus.

Restrictions for initial encryption of SafeGuard Enterprise Client (managed)

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 will become immediately active on the 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 Enterprise Client, the respective configuration package has to be reassigned to the Enterprise Client's OU as well. The user-defined keys will then only be created after the 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 Sophos SafeGuard Clients (standalone)

- The following modules are not supported for Sophos SafeGuard Clients (standalone):
 - SafeGuard Enterprise BitLocker support
 - Configuration Protection

Restrictions for BitLocker support

- The following installation package is not available for SafeGuard Enterprise Clients (managed) with BitLocker support:
 - SGNClient_withoutDE.msi/SGNClient_withoutDE_x64.msi

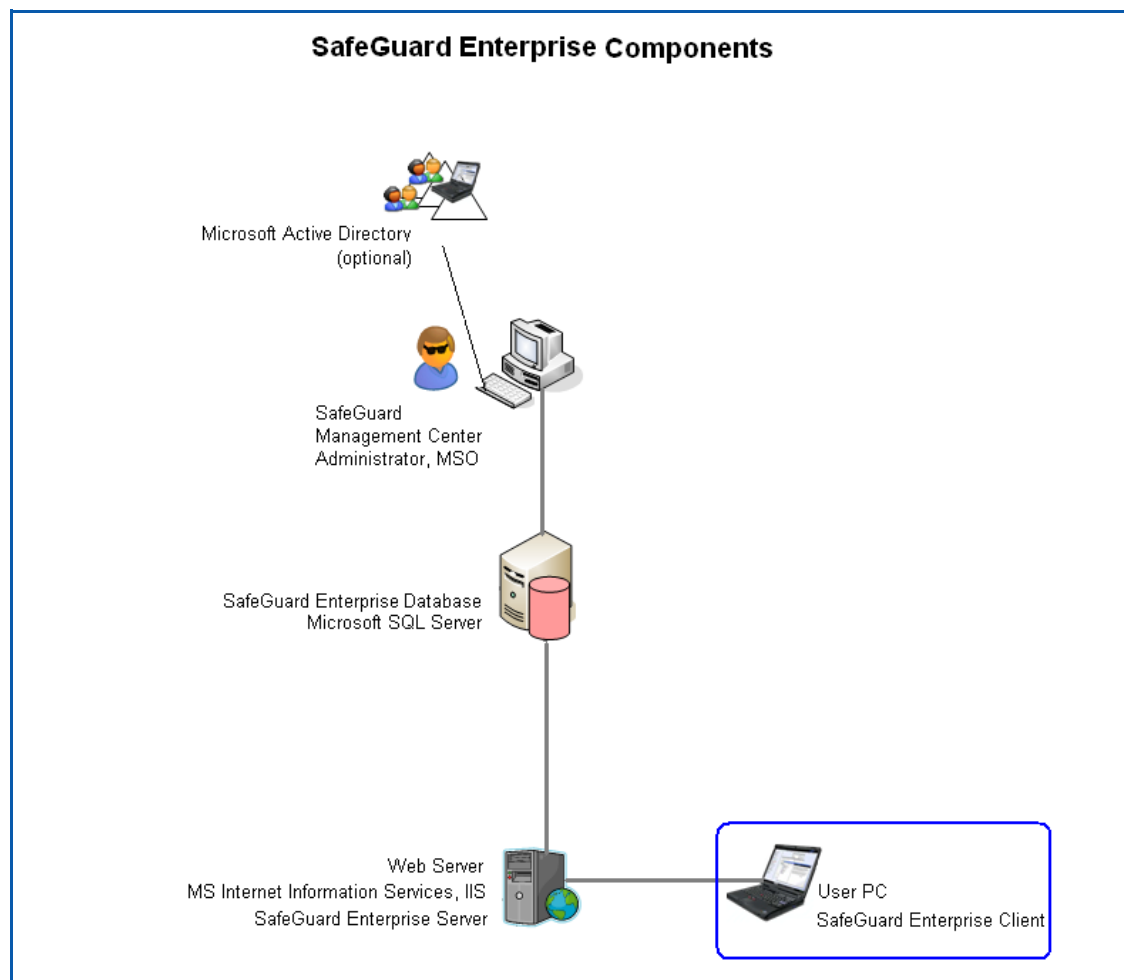
Notice: Either SafeGuard Enterprise or BitLocker volume based encryption can be used on Windows Vista/Windows 7, but not both encryption methods simultaneously. If you want to change the encryption type, you must first decrypt all the partitions, uninstall the SafeGuard Enterprise Client installation package, and then reinstall it with the features you want to use.

10.2 SafeGuard Enterprise Clients (managed)

SafeGuard Enterprise Clients (managed) are managed centrally in the SafeGuard Management Center.

For SafeGuard Enterprise Clients a connection to the SafeGuard Enterprise Server exists. The connection may temporarily be disabled, for example during a business trip, but even so the endpoint computer is still defined as a managed SafeGuard Enterprise Client.

The required configuration package is created in the SafeGuard Management Center.



10.2.1 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 SafeGuard Configuration Protection Client is available for Windows 7 64 bit.

The following table shows the available installation packages for the Enterprise Client and states how the configuration package needs to be created:

Package	Description
SGxClientPreinstall.msi	Must be installed on the endpoint computers prior to 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 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 (available for Windows 7 64 bit)	The 64 bit variant of this package is available for Windows 7 64 bit operating systems. For native SafeGuard Enterprise Clients and for Enterprise Clients with BitLocker Support. Configuration Protection Port protection and management of peripheral devices

Package	Description
SGNClientRuntime.msi SGNClientRuntime_x64.msi	Runtime Client enabling booting from a secondary boot volume when multiple operating systems are installed and accessing these volumes when they are encrypted by a SafeGuard Enterprise installation on the primary volume. Available for both SafeGuard Enterprise Clients and SafeGuard Standalone Clients.
Enterprise Client Configuration Package	Created in the SafeGuard Management Center Configuration Package Tool.

10.3 Sophos SafeGuard Clients (standalone)

The Sophos SafeGuard Clients (standalone) is never connected to the SafeGuard Enterprise Server at any point in time and is not connected to the central management of SafeGuard Enterprise, i.e. it operates in standalone mode.

The most significant difference to a SafeGuard Enterprise Client (managed) is that a Sophos SafeGuard Clients (standalone) only receives SafeGuard Enterprise policies via a configuration package. It never receives policies via a connection to the SafeGuard Enterprise Server.

Sophos SafeGuard Clients (standalone) are managed locally. Policy groups and configuration packages are created in the SafeGuard Management Center. The configuration packages are then distributed via company software distribution mechanisms or installed manually on the endpoint computers.

10.3.1 Restrictions

For Sophos SafeGuard Clients (standalone) the following modules are not supported:

- Configuration Protection
- BitLocker support

10.3.2 Available installation packages for Sophos SafeGuard Clients (standalone)

Note: For the Client installation packages 64 bit versions are available for Windows 7 64 bit and Windows Vista 64 bit operating systems (<package name>_x64.msi). 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.

The following table shows the available Client installation packages for this standalone scenario and states how the configuration package needs to be created:

Package	Description
SGxClientPreinstall.msi	Must be installed on the endpoint computers prior to 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 booting from a secondary boot volume when multiple operating systems are installed and accessing these volumes when they are encrypted by a SafeGuard Enterprise installation on the primary volume. Available for both SafeGuard Enterprise Clients (managed) and Sophos SafeGuard Clients (standalone).
Standalone Client Configuration Package	Created in the SafeGuard Management Center Configuration Package Tool.

11 Setting up endpoint computers centrally

This chapter describes how to set up endpoint computers centrally for multiple computers.

Installation and configuration is described for SafeGuard Enterprise Clients (managed) as well as for Sophos SafeGuard Clients (standalone).

The tasks required for an installation of users computers with Windows BitLocker are described as well.

SafeGuard Enterprise security officers may carry out the installation and initial configuration of endpoint computers as part of centralized software distribution. This ensures a standardized installation on multiple endpoint computers.

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

The behavior of the endpoint computers when first logging on after installing SafeGuard Enterprise is described in the SafeGuard Enterprise User help.

11.1 General prerequisites

The following prerequisites must be met:

- You need Windows administrator rights.
- A user account must be set up and active on the endpoint computers.
- Create a full backup of data on the endpoint computers.
- This prerequisite does only apply to SafeGuard Enterprise Clients:

Check whether there is a connection to the SafeGuard Enterprise Server. Select this web address in Internet Explorer on the endpoint computers:

<http://<ServerIPAdresse>/sgnsrv>

If the "Trans" page shows **Check Connection**, connection to SafeGuard Enterprise Server is made.

11.2 Prerequisites for BitLocker Support

If you wish to use SafeGuard Enterprise to manage BitLocker endpoint computers, you need to do the following preparation on the endpoint computer:

- Windows 7 or Windows Vista Enterprise or Ultimate 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 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. Otherwise the system may be harmed.

If you need more information, contact Microsoft Support. You will also find information on these websites:

- Information about the preparation and about 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>

11.3 Restrictions

AHCI

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.

Dynamic and GPT disks

Dynamic and GUID partition table (GPT) disks are not supported. In such cases, the installation will be terminated. If such disks can be found on the computer at a later point in time, they will not be supported.

SCSI hard disks

The SafeGuard Enterprise Device Encryption Client does not support systems that are equipped with hard disks attached via a SCSI bus.

Restrictions for initial encryption of SafeGuard Enterprise Clients (managed)

Initial configuration of SafeGuard Enterprise Clients 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 will become immediately active on the 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 Enterprise Client, the respective configuration package has to be reassigned to the Enterprise Client's OU as well. The user-defined keys will then only be created after the 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 Sophos SafeGuard Clients (standalone)

- The following modules are not supported for Sophos SafeGuard Clients (standalone):
 - SafeGuard BitLocker support
 - Configuration Protection

Restrictions for BitLocker support

The following installation package is not available for SafeGuard Enterprise Clients (managed) with BitLocker support:

- SGNClient_withoutDE.msi/SGNClient_withoutDE_x64.msi

11.4 Service accounts for post-installation tasks

To prevent that administrative operations on a SafeGuard Enterprise protected computer lead to an activation of the Power-on Authentication and the addition of rollout operators as users to the computer, SafeGuard Enterprise offers the possibility of creating service account lists for endpoint computers. The users included in these lists are thereby treated as SafeGuard Enterprise guest users.

With service accounts the scenario is as follows:

- SafeGuard Enterprise is installed on an endpoint computer.
- After rebooting the computer, a rollout operator included on a service account list logs on (Windows logon).
- According to the service account list applied to the computer the user is identified as a service account and will be treated as a guest user.
- The rollout operator will not be added to the POA and the POA will not become active. The end user can log on and activate the POA.

Note: Service Account Lists should be assigned in the first configuration package you create for the configuration of the endpoint computers. For further information see the Administrator help.

11.5 Tasks for centralized install

As a security officer, create an installation package that includes the following:

- Preparatory installation package

Use 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 will be aborted.

- SafeGuard Enterprise Client installation package

The “Client” installation packages are included on the product CD.

The installation packages are valid for Enterprise Clients (managed) and Standalone Clients alike.

For Standalone Clients, however, the Configuration Protection package may not be installed.

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 SafeGuard Configuration Protection Client is available for Windows 7 64 bit.

- Configuration package for endpoint computers

The configuration package for the endpoint computers must be generated beforehand.

Different configuration packages need to be installed for managed and standalone endpoint computers. Before installing a new configuration package on the endpoint computer ensure to uninstall any outdated ones.

- Script with commands for automatic installs

You need to distribute this installation package to the endpoint computers in the specified sequence. To do so, you can use the Windows Installer command `msiexec`. The packages are executed on the endpoint computers. The endpoint computers are then ready for use of SafeGuard Enterprise.

The User help describes the behavior of the endpoint computers when first logging on after installing SafeGuard Enterprise.

11.6 Configuring the endpoint computer

Depending on the required configuration you will create specific configuration packages for the endpoint computer in the SafeGuard Management Center.

11.6.1 Creating a SafeGuard Enterprise Client (managed) configuration package

To create a SafeGuard Enterprise Client (managed) configuration package, proceed as follows:

1. Start the SafeGuard Management Center. In the **Tools** menu, select **Configuration Package Tool**.
2. Select **Create Configuration Package (managed)**.
 - a) Click **Add Configuration Package** to create the SafeGuard Enterprise Client (managed) configuration package.
 - b) Enter a name of your choice for this package (MSI).
 - c) Assign a primary server (the secondary server is not absolutely essential).
 - d) If required, specify a policy created in the SafeGuard Management Center which is to apply to the endpoint computers, see [Restrictions for initial encryption of SafeGuard Enterprise Clients \(managed\)](#) on page 78. If you want to use service accounts for post-installation tasks on the computer ensure to include the setting in this first policy group, see [Service accounts for post-installation tasks](#) on page 79.
 - e) Select the **Transport Encryption** mode defining how the connection between SafeGuard Enterprise Client and SafeGuard Enterprise Server is to be encrypted:
 - SafeGuard encryption
 - SSL 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.

Hint: If you use SSL transport encryption between server and client you have to set up the IIS for it in advance:

- 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, see [Securing transport connections with SSL](#) on page 11.

- f) Specify the output path and click **Create Configuration package**. The SGNClientConfig.msi will be created in the specified directory.

The configuration package has now been created for the SafeGuard Enterprise Client (managed). Deploy this package on the endpoint computer.

11.6.2 Creating a Sophos SafeGuard Client (standalone) configuration package

To create a Sophos SafeGuard Client (standalone) configuration package, proceed as follows:

1. In the SafeGuard Management Center, select **Tools > Configuration Package Tool** from the menu bar.
 2. Select **Create Configuration Package (standalone)** for a standalone configuration.
 - a) Click **Add Configuration Package**.
 - b) Enter a name of your choice for this package (MSI).
 - c) Specify a **Policy Group**, which must have been created beforehand in the SafeGuard Management Center, to be applied to the Standalone Clients. In contrast to Enterprise Clients, you can only apply policy groups to Standalone Clients, not individual policies. If you want to use service accounts for post-installation tasks on the computer ensure to include the setting in this first policy group, see [Service accounts for post-installation tasks](#) on page 79.
 - d) To enable recovery for Standalone Clients, the required data has to be available to the help desk.

For Standalone Clients this data is saved as a specific recovery file (.xml file). This file is created during configuration of the Standalone Client. It contains the defined machine key, the kernel key, a session key as well as a copy of the MBR.
 - e) Specify a shared network path or select it from the drop down list for storing this file (.xml file) in **Key Backup Location** so that it will be available to the help desk in case of an emergency. Enter the shared path in the following form:
\\networkcomputer\, e.g. "\\mycompany.edu\".
- If you do not specify a path here, the user will be prompted to name a storage location for this file when first logging on to the endpoint computer.

Hint: Make sure to save this .xml file at a file location accessible to the helpdesk, for example a shared network path. Alternatively the files can be provided to the helpdesk via different mechanisms.

This recovery key file (.xml file) is encrypted by the company certificate. The file can therefore be saved to any external media or to the network to provide it to the help desk in case of an emergency. It can also be sent by E-mail.

- f) 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** area of the SafeGuard Management Center. For further details, see the Administrator Help.
- g) Specify an output path for the configuration package (.msi file).
- h) Click **Create Configuration package**.

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

11.7 Command for centralized install

When centrally installing the SafeGuard Enterprise Client software on the endpoint computers, use the Windows Installer component "msiexec". "Msiexec" is already part of Windows XP, Vista, and Windows 7, and it automatically carries out a pre-configured SafeGuard Enterprise client installation. As the source and the destination for the install can also be specified, there is the option of a standard install to multiple endpoint computers.

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, e.g., log warnings and error messages to a file during the install.
- **SafeGuard Enterprise features**, which are to be installed, e.g. file based encryption.
- **SafeGuard Enterprise parameters**, e.g. to specify the install directory.

11.7.1 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.
<code>ADDLOCAL=</code>	Lists the features that are to be installed. If the option is not specified, all features intended for a standard installation are installed. When listing the features under <code>ADDLOCAL</code> note the following: <ul style="list-style-type: none"> - only separate the features by a comma, not by a space. - respect upper and lower case. - If you select a feature, you also need to add all the feature parents to the command line!
<code>ADDLOCAL=ALL</code>	Installs all the available features
<code>REBOOT=Force ReallySuppress</code>	Forces or suppresses a reboot after installation. If nothing is specified, the reboot is forced after installation.
<code>/L* <path + filename></code>	Logs all warnings and error messages in the specified log file. The parameter <code>/Le <path + filename></code> only logs error messages
<code>InstallDir= <directory></code>	Specifies the directory in which the SafeGuard Enterprise Client is to be installed. If no value is specified, the default installation directory will be <code><SYSTEM>:\PROGRAM FILES\SOPHOS</code> .

11.7.2 SafeGuard Client Features (ADDLOCAL)

For a central install, you must define in advance which SafeGuard Enterprise features are to be installed on the endpoint computers. The features are listed after stating the option `ADDLOCAL` in the command.

You should decide before the install whether you want to use SafeGuard Enterprise in association with BitLocker volume encryption or SafeGuard Enterprise encryption in its entirety.

Notice: If you wish to install SafeGuard Enterprise's volume based encryption, you should make sure that no volumes have yet been encrypted with BitLocker. Otherwise the system may be harmed.

The following table lists the SafeGuard Enterprise Client features that can be installed centrally on the endpoint computers. If you select a feature, you also need to add the feature parents to the command line!

Features for SafeGuard Device Encryption

The Features `Client` and `Authentication` must be installed by default!

Feature Parents	Feature
Client	Authentication The feature <code>Authentication</code> and its parent feature <code>Client</code> must be installed by default.
Client, Authentication	CredentialProvider For computers with Windows Vista/Windows 7 you must select this feature. It enables logon via the Credential Provider.
Client	SecureDataExchange With <code>SecureDataExchange</code> , 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 clients that do not have SafeGuard Data Exchange installed. SafeGuard Data Exchange can be installed parallel to the BitLocker Client.

Feature Parents	Feature
Client, BaseEncryption	<p>SectorBasedEncryption</p> <p>Installs SafeGuard Enterprise's volume based encryption with the following features:</p> <ul style="list-style-type: none"> ■ Any volumes, including removable media, can be encrypted with SafeGuard Enterprise's volume based encryption. ■ SafeGuard Enterprise Power-on Authentication (POA) ■ SafeGuard Enterprise Recovery with Challenge/Response <p>HINT: Either SectorBasedEncryption OR BitLockerSupport can be specified.</p>
Client, BaseEncryption	<p>BitLockerSupport</p> <p>Installs BitLocker support for SafeGuard Enterprise with the following functions:</p> <ul style="list-style-type: none"> ■ Boot volume encryption with BitLocker ■ Encryption of other volumes with BitLocker ■ BitLocker Pre-Boot Authentication ■ BitLocker Recovery <p>HINT: Either SectorBasedEncryption OR BitLockerSupport can be specified. Not available for Sophos SafeGuard Standalone Clients.</p>
Client	<p>ConfigurationProtection</p> <p>Port protection and management of peripheral devices</p> <p>To install SafeGuard Configuration Protection you need to list this feature in the msixec command for the Client installation package AND carry out additional installation steps, see Installing SafeGuard Configuration Protection on page 98. Not available for Sophos SafeGuard Standalone Clients.</p>

Features for SafeGuard Data Exchange

The Features **Client** and **Authentication** must be installed by default!

Feature Parents	Feature
Client	<p>Authentication</p> <p>The feature Authentication and its parent feature Client must be installed by default.</p>
Client	<p>SecureDataExchange</p> <p>With SecureDataExchange, SafeGuard Data Exchange with file based encryption is always installed at local level and for removable media.</p> <p>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.</p> <p>If you have installed SafeGuard Data Exchange on your computer, you can also use SafeGuard Portable. The Data Exchange package also includes SafeGuard Portable. SafeGuard Portable enables data to be securely shared with clients that do not have SafeGuard Data Exchange installed.</p> <p>SafeGuard Data Exchange can be installed parallel to the BitLocker Client.</p>
Client	<p>ConfigurationProtection</p> <p>Port protection and management of peripheral devices</p> <p>To use SafeGuard Configuration Protection you need to list this feature in the msiexec command for the Client installation package AND carry out additional installation steps, see Installing SafeGuard Configuration Protection on page 98.</p> <p>Not available for Sophos SafeGuard Standalone Clients.</p>

11.7.3 Sample command for volume and file based encryption

The command given below installs the following:

- The endpoint computers are provided with the necessary requirements for successful installation of the encryption software.
- SafeGuard Enterprise Power-on Authentication for authentication at SafeGuard Enterprise endpoint computers
- SafeGuard Data Exchange with file based encryption is installed by specifying `SecureDataExchange`.
- SafeGuard Enterprise volume based encryption is installed.
- A log file is created.
- Afterwards, the 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,SecureDataExchange,BaseEncryption,
SectorBasedEncryption

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

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

11.7.4 Sample command for Windows Vista with BitLocker support

The sample command runs the following:

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

Hint: When installing SafeGuard Enterprise with BitLocker, ensure that only BitLocker volume encryption is run. Do not add SafeGuard Enterprise's volume based encryption 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,
SecureDataExchange,BaseEncryption,BitLockerSupport

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

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

11.8 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 algorithms for encryption. As to AES algorithms, a new implementation is installed by default 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 SafeGuard Enterprise Client.

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.

12 Setting up endpoint computers locally

This chapter describes how to set up the encryption software locally at the endpoint computer. Steps required for SafeGuard Enterprise Clients with Windows Vista BitLocker are described as well.

For information on the different Client installation and configuration packages see [SafeGuard configurations for endpoint computers](#) on page 68.

You should decide before the install whether you want to use SafeGuard Enterprise in combination with BitLocker volume encryption or SafeGuard Enterprise encryption.

Notice: If you wish to install SafeGuard Enterprise volume based encryption, you should make sure that no volumes have already been encrypted with BitLocker. Otherwise the system may be harmed.

12.1 Prerequisites

For general prerequisites see [General prerequisites](#) on page 76 and for special prerequisites for Windows Vista BitLocker support see [Prerequisites for BitLocker Support](#) on page 77.

12.2 Installing the encryption software on the endpoint computers

This chapter is both valid for SafeGuard Enterprise Clients (managed) and Sophos SafeGuard Clients (standalone). The installation procedure is identical except that you create a different configuration package for each of them. Before installation, decide which SafeGuard Enterprise features you want to use.

12.2.1 Carrying out installation

1. Start the preparatory installation package SGxClientPreinstall.msi from the product CD to provides endpoint computers with necessary requirements for successful installation of the encryption software, for example the relevant DLLs.

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.

2. Start the relevant Client installation package from the product CD.
3. Accept the default on the next dialogs.

4. If required, select the install type and activate the features to your needs, see [Selecting features](#) on page 92.
5. Select an installation path. The default installation path is:
`C:\Program Files\Sophos\SafeGuard Enterprise`
6. Confirm that the installation has completed successfully.

12.2.2 Creating the configuration package

1. Configure the endpoint computer by creating a configuration package in the SafeGuard Management Center.
 - For creating a SafeGuard Enterprise Client (managed) configuration, see [Creating a SafeGuard Enterprise Client \(managed\) configuration package](#) on page 81.
 - For creating an Sophos SafeGuard Client (standalone) configuration, see [Creating a Sophos SafeGuard Client \(standalone\) configuration package](#) on page 82.
2. Distribute the configuration package to the endpoint computers.
3. Install the configuration package on the endpoint computer.

The Client software has now been completely installed.

The User help describes how the computers behave when first logging on after installing SafeGuard Enterprise.

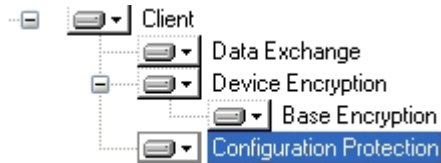
12.3 Selecting features

While SafeGuard Enterprise is being installed on the computer, you are offered optional features, depending on the operating system and installation package. Further details about the features see [SafeGuard Client Features \(ADDLOCAL\)](#) on page 85.

1. Click the features to select them.
2. Disable the features you do not want to install.
3. Continue the installation.

12.3.1 Client features for Windows XP

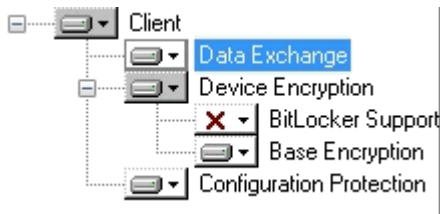
The picture shows the selection of features for of the SGNClient.msi installation package.



- SafeGuard Data Exchange with file based encryption: **Data Exchange** activated.
- Volume based encryption: **Device Encryption > Base Encryption** activated.
- Configuration protection: **Configuration Protection** activated. Further steps are required for installing this module, see [Installing SafeGuard Configuration Protection](#) on page 98. This feature cannot be installed for Sophos SafeGuard Standalone Clients.

12.3.2 Client features for Windows Vista without BitLocker support

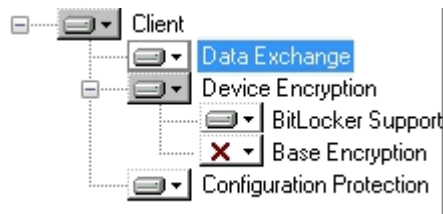
The picture shows the selection of features for the SGNClient.msi installation package.



- SafeGuard Data Exchange with file based encryption: **Data Exchange** activated.
- Volume based encryption based on SafeGuard Enterprise:
 - **Device Encryption > Base Encryption** activated.
 - **Device Encryption > BitLocker Support** deactivated.
- Configuration protection: **Configuration Protection** activated. Further steps are required for installing this module, see [Installing SafeGuard Configuration Protection](#) on page 98. This feature cannot be installed for Sophos SafeGuard Standalone Clients.

12.3.3 Client features for Windows Vista with BitLocker support

The picture shows the selection of features for the SGNClient.msi installation package. For Sophos SafeGuard Standalone Clients BitLocker support and Configuration Protection cannot be installed.



- SafeGuard Data Exchange with file based encryption: **Data Exchange** activated.
- Volume based encryption based on BitLocker:
 - **Device Encryption > BitLocker Support** activated.
 - **Device Encryption > Base Encryption** deactivated.
- Configuration protection: **Configuration Protection** activated. Further steps are required for installing this module, see [Installing SafeGuard Configuration Protection](#) on page 98.

13 Installing the SafeGuard Enterprise Client software on computers with multiple operating systems

The SafeGuard Enterprise Client 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 Client enables the following when it is installed on volumes with an additional Windows installation:

- The Windows installation residing on these volumes may successfully be booted 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.

13.1 Requirements and restrictions

Note the following:

- SafeGuard Enterprise Runtime Client does not provide any SafeGuard Enterprise Client specific features or functionality.
- SafeGuard Enterprise Runtime Client only supports those operating systems that are also supported for SafeGuard Enterprise Client.
- Successful 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 to use Microsoft boot managers.
- The SafeGuard Enterprise Runtime Client cannot be updated to a full SafeGuard Enterprise Client.
- This scenario is valid for SafeGuard Enterprise Clients as well as Sophos SafeGuard Standalone Clients.
- 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 may be accessed.

13.2 Preparations

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

1. Ensure that those volumes on which SafeGuard Enterprise Runtime is to run are visible at the time of installation and may be addressed by their Windows name (e.g. C:).
2. Decide on which volume(s) of the hard disk the **SafeGuard Enterprise Runtime Client** is to be installed. In terms of SafeGuard Enterprise, these volumes are defined as "secondary" Windows installations. There can be several secondary Windows installations.

You may install the following package from the product CD:

- SGNClientRuntime.msi/SGNClientRuntime_x64.msi

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.

You may install the following packages from the product CD:

- SGNClient.msi,/SGNClient_x64.msi
- additionally SGN_CP_Clien.msi/ SGN_CP_Client_x64.msi (available for Windows 7 64 bit operating systems).

13.3 Setting up SafeGuard Enterprise Runtime Client

Proceed as follows:

1. Select the required secondary volume(s) of the hard disk, you want to install SafeGuard Enterprise Runtime Client on.
2. Boot the secondary Windows installation on the selected volume.
3. Install the Client Runtime installation package on the selected volume.
4. Confirm the defaults in the next dialog of the installer. No special feature selection is necessary.
5. Select an installation folder for the runtime installation.
6. Confirm to finish the runtime installation.
7. Select the primary volume of the hard disk, you want to install SafeGuard Enterprise Client on.
8. Boot the primary Windows installation on the selected volume.

9. Start the preparatory installation package SGxClientPreinstall.msi to provides endpoint computers with necessary requirements for successful installation of the encryption software, for example the relevant DLLs.
10. Install the required SafeGuard Enterprise Client installation package on the selected volume.
11. Create the configuration packages for the SafeGuard Enterprise Client (managed) or Sophos SafeGuard Client (standalone) as required and deploy it on the endpoint computer.
12. Encrypt both volumes with the defined machine key.

13.4 Booting from a secondary volume via 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 boot volume.
4. Reboot the computer from this volume.

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

14 Installing SafeGuard Configuration Protection

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

14.1 Prerequisites and Restrictions

- 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.

14.2 Workflow

To install SafeGuard Configuration Protection on the endpoint computers you need to run a separate installation package, after having installed the SafeGuard Enterprise Client installation package. You will find the required installation packages on your product CD.

Note: 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.

1. Install the preparatory installation package SGxPreinstall.msi.
2. Install one of the following SafeGuard Enterprise Client installation packages:
 - SGNClient.msi/SGNClient_x64.msi
 - SGNClient_withoutDE.msi/SGNClient_withoutDE_x64.msi
3. Install SafeGuard Configuration Protection:
 - SGN_CP_Client.msi/SGN_CP_Client_x64.msi
4. Generate and install the SafeGuard Enterprise Client configuration package.

14.3 Command for central installation

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

Command line syntax

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

14.4 Sample command for SafeGuard Configuration Protection with SafeGuard Device Encryption

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 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 msiexec command.
- A log file is created.
- Finally, the Client configuration package SGNEnterpriseClientConfig.msi 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,Co  
nfigurationProtection  
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
```

14.5 Sample command for SafeGuard Configuration Protection with SafeGuard Data Exchange

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 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 msixec command.
- A log file is created.
- Finally, the configuration package SGNEnterpriseClientConfig.msi is run.

EXAMPLE:

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

msiexec /i F:\Software\SGNClient_withoutDE.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
```

14.6 Local installation

To successfully install SafeGuard Configuration Protection, please stick to the following installation sequence:

1. Start the preparatory installation package SGxClientPreinstall.msi from the product CD to provides endpoint computers with necessary requirements for successful installation of the encryption software.
2. Install one of the following SafeGuard Enterprise Client installation packages 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.
 - SGNClient.msi /SGNClient_x64.msi
 - SGNClient_withoutDE.msi/SGNClient_withoutDE_x64.msi
3. When you are prompted to select the required features, make sure to activate the feature Configuration Protection.
4. Then, install the SafeGuard Configuration Protection installation package:
 - SGN_CP_Client.msi / SGN_CP_Client_x64.msi (avaialble for Windows 7 64 bit operating systems)

Notice: To ensure that the Configuration Protection module is installed in the SafeGuard Enterprise directory, you need to change it to

C:\Program Files\Sophos\SafeGuard Enterprise\

5. We recommend restarting the endpoint computer. However, if the Client configuration package is directly installed afterwards, the restart can be postponed.
6. Generate and install the SafeGuard Enterprise Client (managed) configuration package SGNEnterpriseClientConfig.msi.
7. Restart the computer.

SafeGuard Configuration Protection is installed on the endpoint computer.

14.7 Uninstalling SafeGuard Configuration Protection

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

1. Uninstall the respective Client configuration package.
2. Run the SafeGuard Enterprise Client installation package on the computer, either SGNClient.msi or SGNClient_withoutDE.msi or the respective 64 bit variant.
3. Select the option **Modify** in the installation wizard.
4. Deactivate the feature **Configuration Protection**.
5. When the uninstall is finished, do not restart the computer!
6. Uninstall SGN_CP_Client.msi/SGN_CP_Client_x64.msi.
7. Restart the computer.

SafeGuard Configuration Protection has been removed from the endpoint computer.

14.8 Updating SafeGuard Configuration Protection

To update SafeGuard Configuration Protection to the latest version, carry out the tasks in the order mentioned:

1. Start the preparatory installation package SGxClientPreinstall.msi from the product CD to provides endpoint computers with necessary requirements for successful installation of the encryption software.
2. Update the SafeGuard Enterprise Client installation package on the computer to the current version, see [Updating SafeGuard Enterprise protected endpoint computers](#) on page 108.

Note: Do not reboot the computer afterwards.

3. Uninstall the currently installed SafeGuard Configuration Protection client module, see [Uninstalling SafeGuard Configuration Protection](#) on page 102.
4. Install the latest SafeGuard Configuration Protection Client module afresh, see [Local installation](#) on page 101.

15 Preventing uninstallation from the endpoint computer

To provide extra protection for endpoint computers you can prevent local uninstallation of SafeGuard Enterprise via a central machine policy. If this kind of policy is applied to the endpoint computer, SafeGuard Enterprise can only be uninstalled when the appropriate policy is assigned. Otherwise uninstallation will be cancelled and the unauthorized attempt will be logged. See the SafeGuard Enterprise Administrator help for further details about policies.

Hint: If you work with a demo version, you should not activate this policy setting or in any case deactivate it prior to expiry of the demo version to ensure easy uninstallation.

16 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 5.50 is supported for SafeGuard Enterprise version 5.35 onwards. When updating from older versions, you first need to update to SafeGuard Enterprise 5.40.

Apart from the SafeGuard Enterprise database, the SafeGuard Enterprise Server, Management Center, and the endpoint computer updates 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, the policy transport will be blocked after the update of the backend. Please contact your sales partner in advance to request a license file.

Hint: It is essential that you update the components in the order outlined below. Any update from an earlier version to the current version of SafeGuard Enterprise will only succeed if you follow this sequence. Updating the SafeGuard Enterprise components is supported for SafeGuard Enterprise version 5.30 or above.

SafeGuard Enterprise

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

16.1 Updating SafeGuard Enterprise Database

On the product CD several SQL scripts are provided for updating the SafeGuard Enterprise database.

Prerequisites

- There must be a SafeGuard Enterprise database version 5.20 or higher installed.
- The SQL scripts that are to be run must be present on the database computer.
- You need Windows administrator rights for the database server.
- Backup the SafeGuard Enterprise Database before starting the update.

Updating the database

1. Take all SafeGuard Enterprise Servers (IIS servers) connected to the relevant SafeGuard Enterprise database offline.
2. Close all open SafeGuard Management Centers connected to the relevant SafeGuard Enterprise database.
3. Set the SafeGuard Enterprise database to SINGLE_USER mode for running the SQL scripts so that you have exclusive access. to the database.
4. The database must be migrated 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`.
Note: 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) 5.30 > 5.40: Run `MigrateSGN530_SGN540.sql`
 - d) 5.35 > 5.40: Run `MigrateSGN535_SGN540.sql`
 - e) 5.40 > 5.50: Run `MigrateSGN540_SGN550.sql`
5. Set the SafeGuard Enterprise database to MULTI_USER mode again.

After updating the database the cryptographic check sums of some tables might no longer be correct. When starting the SafeGuard Management Center warning messages will be displayed accordingly. You can repair the tables in the relevant dialog. The latest version of the SafeGuard Enterprise database is then ready for use.

16.2 Updating 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 conflict with replicated databases.

1. Uninstall the replicated databases.
2. Run the SQL migration scripts on the master database. You can find it in the Tools folder of the product CD (see [Updating SafeGuard Enterprise Database](#) on page 105).
3. Set up the replication databases anew.

16.3 Updating SafeGuard Enterprise Server

Prerequisites

- The SafeGuard Enterprise database has already been updated to the latest version.
- There must be a SafeGuard Enterprise Server 5.35 or higher installed. Versions below 5.35 must be updated to SafeGuard Enterprise Server 5.40 first of all.
- You need Windows administrator rights.
- ASP.NET must be upgraded to version 2.0.

Carrying out the update

Reinstall the server, see [Installing SafeGuard Enterprise Server](#) on page 48. After successful updating, the server is automatically restarted and is ready to operate again.

16.4 Updating SafeGuard Management Center

Prerequisites

- SafeGuard Management Center 5.35 or higher must be installed. Versions below 5.35 must be updated to SafeGuard Management Center 5.40 first of all.
- The SafeGuard Enterprise database and SafeGuard Enterprise Server have already been updated to the latest version.
- NET Framework 3.0 Service Pack 1 must be installed for successfully updating to the latest version.
- ASP.NET must be converted to version 2.0.

- You need Windows administrator rights.
- You need a valid licence file. Please contact your sales partner in advance to request it.

Carrying out the update

1. Reinstall the Management Center, see [Setting up SafeGuard Management Center](#) on page 24 with the required features.
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 whether the feature Multi Tenancy has been installed with the update.
 - Multi Tenancy has not been installed: You are prompted to enter the security officer credentials.
 - Multi Tenancy has been installed: The SafeGuard Management Center Configuration Wizard will be started and prompt you to select which database is to be used. The wizard will already preselect a previously used database. Select the required database and finish the Wizard.

Notice:

- The default configuration file for the SafeGuard Management Center has been moved and renamed. You may find it in the following location:
 - **Windows XP:** <CSIDL_LOCAL_APPDATA>\Sophos\SafeGuard Enterprise\Configuration\<hash>.xml
 - **Windows Vista:** C:\Users\<user name>\AppData\Local\Sophos\SafeGuard Enterprise\Configuration\FE2E60C269D115B176D195AB3ABF8324.xml
- **Scripting API:** Due to the renaming and new storage location of the default configuration file, ensure that the path and filename is changed to the new location when using the following method with parameter "confFilePathName":

```
AuthenticateOfficer (string OfficerName, string PinOrPassword, string confFilePathName).
```
- If Multi Tenancy is installed with the update, the SafeGuard Management Configuration Wizard will be started after the first update. The wizard will already preselect the previously used database configuration.
- If Multi Tenancy is uninstalled, the last used configuration will be used in the SafeGuard Management Center. After reinstallation of the Multi Tenancy feature this configuration will be preselected.
- Please note that existing SafeGuard Enterprise policies might have been modified as the policy structure has changed from SafeGuard Enterprise version 5.30 upwards.

16.5 Updating SafeGuard Enterprise protected endpoint computers

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

SafeGuard Enterprise Server and SafeGuard Management Center version 5.50 will be able to manage SafeGuard Enterprise Clients (managed and standalone) version 5.35 or higher.

Prerequisites

- There must be a SafeGuard Enterprise Client software version 5.35 or higher installed. Versions below 5.35 must be updated to SafeGuard Enterprise Client 5.40 first of all.
- The SafeGuard Enterprise database, the SafeGuard Enterprise Server and the SafeGuard Management Center have already been updated to the latest version.
- You need Windows administrator rights.

Note:

- Check your network and computers for outdated or unused Client configuration packages and, for security reasons, make sure to delete them.

Carrying out the update

You need to update the SafeGuard Enterprise Client version by version until version 5.50 is reached.

1. Start the preparatory installation package SGxClientPreinstall.msi from the folder of your software delivery to provide endpoint computers with necessary requirements for successful installation of the encryption software.
2. Install the respective Client installation package afresh, see [Setting up endpoint computers centrally](#) on page 76 or see [Setting up endpoint computers locally](#) on page 91.

Windows Installer recognizes the modules that are already installed and only installs these modules afresh. If Power-on Authentication is installed, an updated POA kernel will also be available after a successful update (policies, keys etc.). The SafeGuard Enterprise Client will be automatically restarted.

Note: If the Client configuration has not changed, you do not need to create and install a new Client configuration package. For security reasons however, we recommend that you delete all outdated or unused Client configuration packages.

You only need to create and reinstall a new Client configuration package if there have been changes to the configuration. If you do create a new Client configuration package ensure to delete the outdated one.

If you try to install an older Client configuration package over a newer one, the installation is aborted and a warning message is displayed.

16.5.1 Upgrading Sophos SafeGuard Clients (standalone) with volume based encryption

If you want to enhance a standalone endpoint computer (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 ensure 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 Sophos SafeGuard Client (standalone) configuration package.
3. Install the Client installation package with volume based encryption (SGNClient.msi/SGNClient_x64.msi) selecting the features Device Encryption and Data Exchange.
4. Generate and install a new Sophos SafeGuard Client (standalone) configuration package.

The recovery key file as well as the local keys created during the installation of the Data Exchange package will not be deleted but will still be available.

16.6 Upgrading standalone computers to managed computers

You can upgrade endpoint computers with a Sophos SafeGuard Client (standalone) configuration to a computers with 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.

Notice: The reverse procedure, i.e. migrating a SafeGuard Enterprise Client configuration to a Standalone Client configuration, is not advisable. To do this, you have to completely reinstall SafeGuard Enterprise with the Standalone configuration on to the endpoint computer.

Prerequisites

- SafeGuard Policy Editor has been upgraded to SafeGuard Management Center.
- The Client installation package does not have to be uninstalled.
- Ensure to backup the endpoint computer before starting the upgrade.
- You need Windows administrator rights.

Carrying out the upgrade

For upgrading, you only have to create the respective configuration package required for managed computers and assign it to the endpoint computers:

1. Create the configuration package for the SafeGuard Enterprise Client (managed) in the SafeGuard Management Center via **Tools > Configuration Package Tool > Create Configuration Package (managed)**.
2. Assign this package to the endpoint computer, via a group policy.

Notice: During the upgrade all users and certificates will be deleted and the Power-on Authentication will be disabled as the user-computer assignment is not upgraded. After upgrading, the endpoint computers are therefore unprotected!

3. Reboot twice after the upgrade: The first logon is still done via Autologon. New keys and certificates are assigned to the user. Thus users can only log on at the Power-on Authentication when rebooting for the second time. Only after the second reboot, the endpoint computers are protected again.

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

16.7 Updating SafeGuard Configuration Protection

To update the SafeGuard Configuration Protection Client module, see [Updating SafeGuard Configuration Protection](#) on page 102.

17 Upgrading Sophos SafeGuard 5.5x to SafeGuard Enterprise

Sophos SafeGuard 5.5x comprises the following products:

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

You can easily upgrade these products to the SafeGuard Enterprise suite with central management to make use of the full functionality of SafeGuard Enterprise. For this purpose, the following steps must be taken:

- The SafeGuard Policy Editor must be upgraded to the SafeGuard Management Center.
- The Sophos SafeGuard Clients (standalone) must be upgraded to SafeGuard Enterprise Clients (managed).

You can upgrade the SafeGuard Policy Editor to the SafeGuard Management Center to use comprehensive management features, e.g. user and computer management, as well as logging.

17.1 Prerequisites

- You do not have to uninstall SafeGuard Policy Editor.
- Set up the SafeGuard Enterprise Server prior to migration, see [Setting up SafeGuard Enterprise Server](#) on page 39.

17.2 Upgrading SafeGuard Policy Editor

For the upgrade, simply install the SGNManagementCenter.msi package on the computer, on which the SafeGuard Policy Editor has been set up.

1. Start SGNManagementCenter.msi from the product CD.
2. Click Next in the welcome window.
3. Accept the license agreement.
4. Select an installation path.
5. Confirm that the installation has completed successfully.
6. If necessary, restart your computer.

7. Configure the SafeGuard Management Center, see [Configuring SafeGuard Management Center](#) on page 26.

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

17.3 Upgrading Sophos SafeGuard Clients (standalone)

You can upgrade computers with a Sophos SafeGuard 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.

17.3.1 Prerequisites

- SafeGuard Policy Editor has been migrated to SafeGuard Management Center.
- The Client encryption software does not have to be uninstalled.
- Ensure to backup the endpoint computer before starting the upgrade.
- You need Windows administrator rights.

17.3.2 Carrying out the upgrade

For the upgrade, you only have to create the respective configuration package and assign it to the computer:

1. Create the configuration package for the SafeGuard Enterprise Client (managed) in the SafeGuard Management Center via **Tools > Configuration Package Tool > Create Configuration Package (managed)**.
2. Assign this package to the relevant computers, via a group policy.

Notice: During the upgrade, all users and certificates will be deleted and the Power-on Authentication will be disabled as the user-computer assignment is not upgraded. After the upgrade the endpoint computers are therefore unprotected!

3. Reboot twice after upgrading: The first logon is still done via Autologon. New keys and certificates are assigned to the user. Thus, users can only log on at the Power-on Authentication when rebooting for the second time. Only after the second reboot, the endpoint computers are protected again.

The unmanaged standalone computer is now a computer that can be centrally managed via SafeGuard Enterprise.

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

SafeGuard Easy 4.5x as well as Sophos SafeGuard Disk Encryption 4.60 can be directly upgraded to SafeGuard Enterprise 5.50 by simply installing the SafeGuard Enterprise Client installation package on the computer.

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

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

18.1 Prerequisites

The following prerequisites must be met:

- 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 for versions older than 4.3x is not supported, they must be updated to SafeGuard Easy 4.50 beforehand.
- Direct upgrade is supported for Sophos SafeGuard Disk Encryption version 4.60.
- Windows Installer Version 3.01 or higher has to be installed.
- SafeGuard Easy/Sophos SafeGuard Disk Encryption must be running on one of the following operating systems:
 - Windows XP Professional Workstation Service Pack 2, 3
- The hardware and specific software (for example token or Lenovo middleware) must meet the system requirements for SafeGuard Enterprise.
- Upgrading may only take place if the hard disks are encrypted with the following algorithms: AES128, AES256, 3DES, IDEA.

18.2 Limitations

The upgrade is subject to the following limitations:

- Only the SafeGuard Device Encryption Client installation package (SGNClient.msi) with the standard feature set can be installed. If SafeGuard Configuration Protection or SafeGuard Data Exchange are to be installed in addition, this has to be done in a separate step.
- The installation package without volume based encryption (SGNClient_withoutDE.msi) is not supported for upgrading to SafeGuard Enterprise.

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

Note: If you start an upgrade with the following installations, an error message will be displayed (error number 5006).

- Twin Boot installations
- Installations with active Compaq Switch
- Lenovo Computrace installations
- Hard disks that are partially encrypted, e.g. only have boot sector encryption
- Hard disks with hidden partitions
- Hard disks that have been encrypted with one of the following algorithms: XOR, STEALTH, DES, RIJANDAEL, 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 XOR, STEALTH, DES, RIJANDAEL, Blowfish-8, Blowfish-16 cannot be upgraded.

Notice: There is a risk of data being lost if a removable device has been encrypted with one of the algorithms XOR, STEALTH, DES, RIJANDAEL, Blowfish-8, Blowfish-16 in SafeGuard Easy. The data on the removable medium cannot be accessed with SafeGuard Enterprise after the 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.
- Removable media with Super Floppy volumes cannot be converted after migration.

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 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 (not applicable to Sophos SafeGuard Disk Encryption)	Yes	Encrypted data media, e.g. USB memory sticks, can be converted to a SafeGuard Enterprise compatible format. Note: After conversion, an encrypted data medium can only be read with SafeGuard Enterprise and only at the one endpoint computer where it was converted. The conversion needs to be confirmed in each case. About exceptions, see Limitations on page 114.
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. About non-migratable algorithms, see Limitations on page 114.
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.

SafeGuard Easy/ Sophos SafeGuard Disk Encryption	Upgrade	SafeGuard Enterprise
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 will therefore not be upgraded.
Policies, settings (e.g. 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 SafeGuard Enterprise Power-on Authentication (POA).
Installations without GINA	Yes	Installations without GINA are upgraded to SafeGuard Enterprise with SGNGINA installed.
Token/Smartcards (not applicable to Sophos SafeGuard Disk Encryption)	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 used token/smartcard middleware 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 refer to the user help.

18.4 Preparing for upgrade

The following measures should be taken before starting the installation of SafeGuard Enterprise:

- Before upgrading the endpoint computers, prepare a SafeGuard Enterprise configuration package using SafeGuard Management Center. After the SafeGuard Enterprise encryption software has been installed on the endpoint computers, deploy the configuration package to them. 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 with the upgrade, all drives that were encrypted with SafeGuard Easy/Sophos SafeGuard Disk Encryption will stay encrypted.

- For security purposes, create a full backup of the computers that are to be upgraded.
- Perform the steps that are recommended prior to the installation of SafeGuard Enterprise, e.g. use “chkdsk” and “defrag”.

For further information on e.g. “chkdsk” and “defrag” see our knowledgebase:

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

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

- Create a valid kernel backup and save this backup in a location that can always be accessed, e.g. a network path. For further information see your SafeGuard Easy 4.5x/Sophos SafeGuard Disk Encryption 4.60 manuals/help, chapter *Saving the system kernel and creating emergency media*.
- For security purposes, 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 migration. This can happen if users have previously logged on to the Pre-Boot Authentication and have later been logged on via Windows Secure Autologon (SAL). So users never used their Windows credentials.

Notice: Users need to know their password for Windows logon before upgrading. This is essential as a Windows password cannot be subsequently 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 will not be able to 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 Starting the upgrade

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 package (SGNClient.msi) from the product folder with the standard feature set. The client package SGNClient_withoutDE.msi cannot be used.

Note: For a successful upgrade the installation should best be performed centrally in unattended mode. Installation via the setup folder is not recommended!

Do the following:

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 will start the Migration Wizard.
2. In the Migration Wizard, enter the SYSTEM password and confirm with **Next**. In **Destination folder**, confirm the default with **Next** and click **Finish** to complete the action. A migration configuration file `SGEMIG.cfg` will be created.
3. In the Windows Explorer, rename this file from `SGEMIG.cfg` to `SGE2SGN.cfg`. Store it in a location the computer can access during the upgrade.

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 will be displayed.

4. Enter the “msiexec” command at the command prompt to install the SafeGuard Enterprise preinstallation package as well as the Client installation package on the SafeGuard Easy/Sophos SafeGuard Disk Encryption endpoint computer. 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\%Computename%.log"
MIGFILE=\\Distributionserver\Software\Sophos\SafeGuard\SGE2SGN.cfg
```

If the upgrade is successful, SafeGuard Enterprise can be used 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 Configuring the upgraded endpoint computers

The endpoint computers are initially configured by configuration packages which, among other aspects, define whether the computer is standalone or centrally managed and which activate the Power-on Authentication.

Therefore, during the upgrade, first the preinstallation package and SGNClient.msi should be installed. Only after the POA has been activated and the user has logged on successfully to Windows, endpoint computer configuration should take place.

1. Create the initial configuration package in the SafeGuard Management Center via **Tools > Configuration Package Tool** with the required policy settings.
2. Install the configuration package on the endpoint computers.

Note: The policies transferred with the first SafeGuard Enterprise configuration package have to correspond to the previous configuration of the SafeGuard Easy/Sophos SafeGuard Disk Encryption computer.

18.7 After the upgrade

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

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

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

Notice: To be able to decrypt the hard disk or add and remove keys for hard disk encryption the user first needs to restart the computer.

Policies have to be reset the SafeGuard Management Center to correspond to the previous configuration of the SafeGuard Easy/Sophos SafeGuard Disk Encryption computer.

Removable media migration

Notice: Removable media migration is not applicable to Sophos SafeGuard Disk Encryption.

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!

To be able to decrypt removable media or add and remove keys for removable media encryption the user first needs to detach the media from the computer and reinsert it again.

When accessing removable media after migration, the user needs to actively confirm the transformation of the encryption keys into a SafeGuard Enterprise compatible format. The appropriate policy for volume based encryption has to be present on the endpoint computer before conversion. Otherwise the keys will not be converted.

The user is prompted to confirm the conversion for any removable media. An appropriate message is displayed.

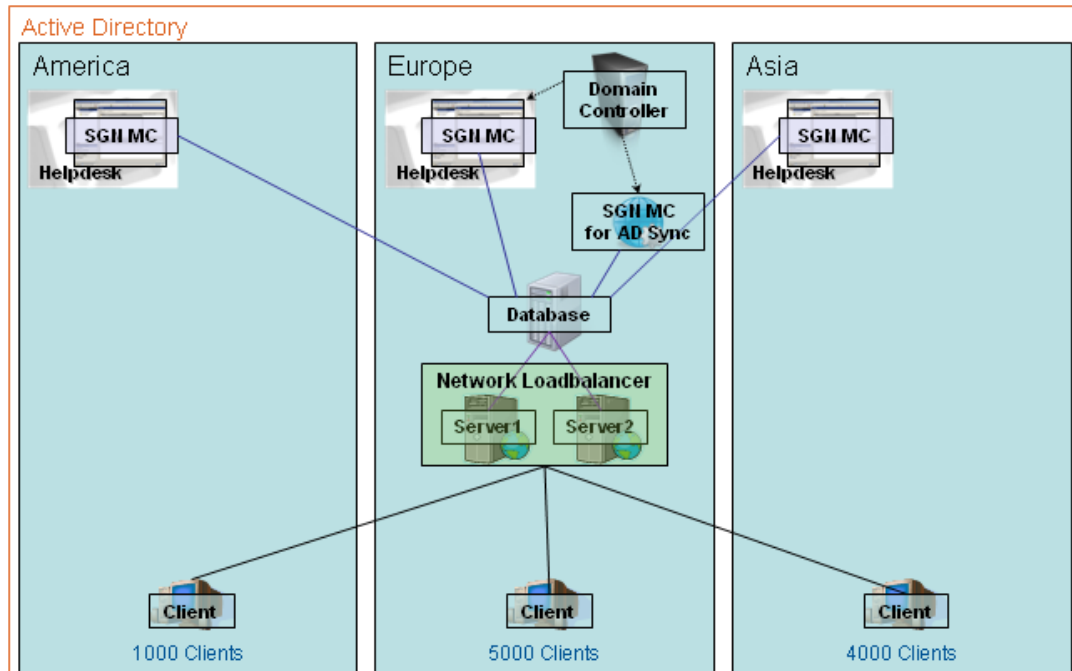
- If the user confirms the conversion, full access to the migrated data is possible.
- If the user rejects the conversion, the migrated data can still be opened for reading and writing.

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

19 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 may, 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 instance you cannot migrate from Windows XP to Windows Vista with SafeGuard Enterprise installed.

20 Annex - Best practice scenario



In this scenario, Europe is the ideal location for the SafeGuard Enterprise database. The reasons are:

- The Active Directory is located in Europe and thus permits rapid synchronization.
- Central management using the SafeGuard Management Center is done in Europe.
- The IIS server is located in Europe.
- Most users reside in Europe.

21 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.

22 Copyright

Copyright © 1996 - 2010 Sophos Group and Utimaco Safeware AG. All rights reserved.

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

Sophos is a registered trademark of Sophos Plc and the Sophos Group. SafeGuard is a registered trademark of Utimaco Safeware AG - a member of the Sophos Group. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

All SafeGuard products are copyright of Utimaco Safeware AG - a member of the Sophos Group, or, as applicable, its licensors. All other Sophos products are copyright of Sophos plc., or, as applicable, its licensors.

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