SOPHOS

Security made simple.

SafeGuard Enterprise

Installation guide

Product version: 7

Document date: December 2014

Contents

1 About SafeGuard Enterprise....4
1.1 SafeGuard Enterprise components....4
2 Getting started....7
2.1 What are the key steps?....7
2.2 Check the system requirements....8
2.3 Download installers....8
2.4 Language settings....8
2.5 Compatibility with other Sophos products....9
2.6 General Restrictions....10
3 Setting up SafeGuard Enterprise Server....12
3.1 Prerequisites....12
3.2 Installing and configuring Microsoft Internet Information Services (IIS)....13
3.3 Install SafeGuard Enterprise Server....15
4 Setting up SafeGuard Enterprise Database....16
4.1 Database authentication....16
4.2 Generating the SafeGuard Enterprise Database....20
4.3 Change access rights for the SafeGuard Enterprise Database 22
4.4 Check SQL Services, named pipes and TCP/IP settings....22
4.5 Create Windows Firewall rule on Windows Server 2008 (R2)....22
4.6 Configure Windows authentication for SQL Server logon....23
5 Setting up SafeGuard Management Center....25
5.1 Prerequisites....25
5.2 Install SafeGuard Management Center....25
5.3 Displaying SafeGuard Management Center help system....26
5.4 Configuring SafeGuard Management Center....26
5.5 Create further database configurations (Multi Tenancy)....31
5.6 Configure additional instances of the SafeGuard Management Center....31
5.7 Logon to SafeGuard Management Center....32
5.8 Setting up the organizational structure in the SafeGuard Management Center....33
5.9 Importing the license file....33
5.10 Restore a corrupt SafeGuard Management Center installation....34
5.11 Restore a corrupt database configuration....34

6 Testing communication....36
6.1 Prerequisites....36
6.2 Test the connection (IIS 7 on Windows Server 2008)....37
7 Securing transport connections with SSL....39
7.1 Set up SSL....39
7.2 Activate SSL encryption in SafeGuard Enterprise....40
7.3 Securing communication between server and endpoint with SSL....40
8 Registering and configuring SafeGuard Enterprise Server....44
8.1 Register and configure SafeGuard Enterprise Server for the current computer....44
8.2 Register and configure SafeGuard Enterprise Server for a different computer....44
8.3 Edit SafeGuard Enterprise Server properties....45
8.4 Register SafeGuard Enterprise Server with Sophos firewall enabled....46
9 Setting up SafeGuard Enterprise on endpoints....48
9.1 About managed and unmanaged endpoints....48
9.2 Restrictions....48
9.3 Preparing endpoints for encryption....49
9.4 Creating configuration packages....52
9.5 Installing the encryption software....54
9.6 Install the encryption software for Mac....63
9.7 FIPS-compliant installations....63
9.8 Installations on self-encrypting, Opal-compliant hard drives....64
10 Replicating the SafeGuard Enterprise Database....66
10.1 Merge replication....66
10.2 Setting up database replication....66
10.3 Install and register SafeGuard Enterprise Servers....68
10.4 Create the configuration packages for the Graz database....68
10.5 Create the configuration packages for the Linz database....69
10.6 Install the SafeGuard Enterprise Server configuration packages....69
10.7 Set up the endpoint....70
11 About uninstallation....71
11.1 Uninstallation best practice....71
11.2 Uninstalling SafeGuard Enterprise encryption software....71
12 Technical support....74
13 Legal notices....75

1 About SafeGuard Enterprise

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

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

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

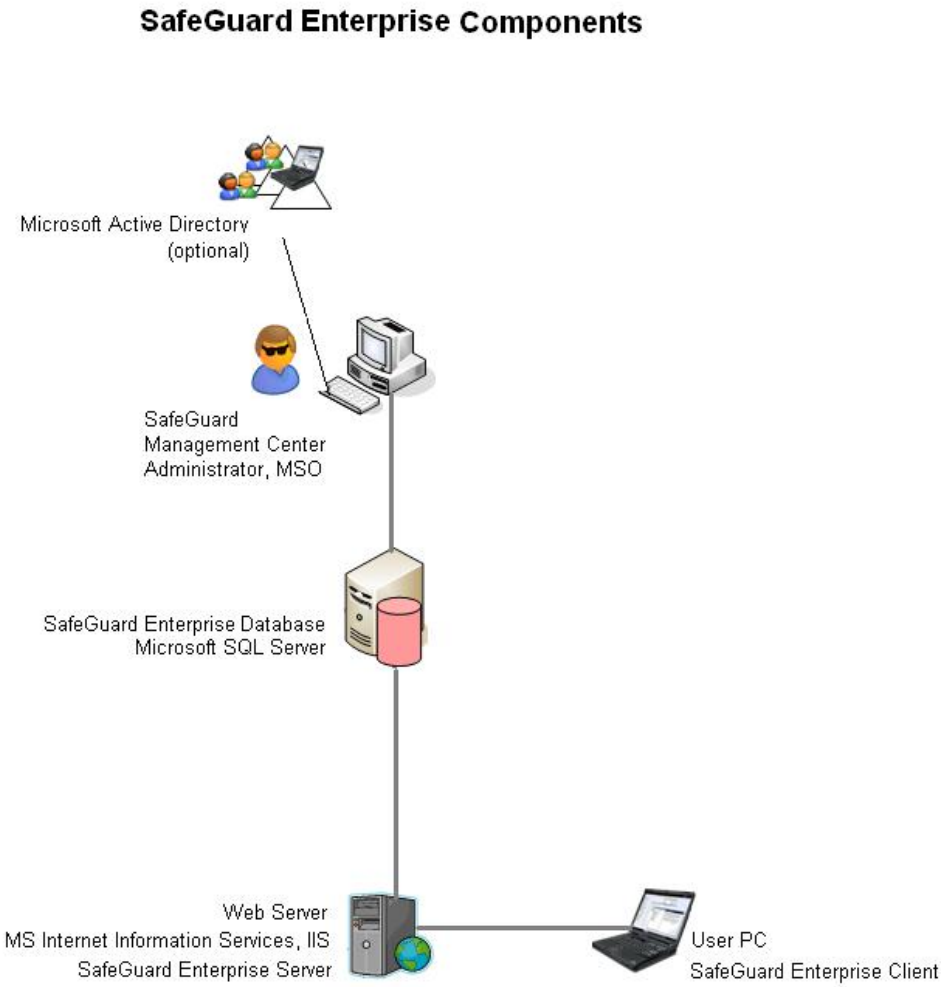
Note: Some features are not included in all licenses. For information on what is included in your license, contact your sales partner.

1.1 SafeGuard Enterprise components

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

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

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



The table below describes the individual components:

Component	Description
SafeGuard Enterprise Database(s) based on Microsoft SQL Server Database	The SafeGuard Enterprise Database(s) hold all relevant data such as keys/certificates, information about users and computers, events and policy settings. The database(s) need to be accessed by the SafeGuard Enterprise Server and by one security officer only through the SafeGuard Management Center, usually the Master Security Officer. The SafeGuard Enterprise Database(s) can be generated and configured using a wizard or scripts.
SafeGuard Enterprise Server on IIS based web server	Microsoft Internet Information Services (ISS). .NET Framework 4 and ASP.NET 4 are required. The web server used for SafeGuard Enterprise must be based on Internet Information Services (IIS). We recommend that you use a dedicated IIS for SafeGuard Enterprise Server.

Component	Description
	SafeGuard Enterprise Server interfaces between the SafeGuard Enterprise Database and the SafeGuard Enterprise endpoint. Upon request, the SafeGuard Enterprise Server sends policy settings to the endpoints. It requires access to the database. It runs as an application on a Microsoft Internet Information Services (IIS) based web server.
	Basic Authentication and ASP .NET 4.5 When choosing SSL as transport encryption method for the client server communication, the *Basic Authentication* role needs to be installed in addition to *ASP.NET 4.5*.
SafeGuard Management Center on administrator computer	Central management tool for SafeGuard Enterprise protected endpoints, managing keys and certificates, users and computers, and for creating SafeGuard Enterprise policies. The SafeGuard Management Center communicates with the SafeGuard Enterprise Database. .NET Framework 4 is required.
Directory Services (optional)	Import of an Active Directory. It holds the company's organizational structure with users and computers.
SafeGuard Enterprise encryption software on endpoints	Encryption software for secure authentication and data encryption on endpoints. SafeGuard Enterprise protected endpoints can either be connected to the SafeGuard Enterprise Server (managed) or not connected to a SafeGuard Enterprise Server at all (unmanaged). Managed endpoints receive their policies directly from the SafeGuard Enterprise Server. Unmanaged endpoints receive their policies inside configuration packages that can be deployed using third-party distribution mechanisms.

2 Getting started

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

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

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

2.1 What are the key steps?

To install SafeGuard Enterprise, follow these installation steps.

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

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

Step	Description	Package/Tool
1	Download the installers.	
2	Install .NET Framework 4 with ASP.NET 4. If you use .NET 4.5 and want to choose SSL as transport encryption method for the client server communication, install the *Basic Authentication* role in addition to ASP.NET 4.5.	
3	Set up Internet Information Services (IIS) for SafeGuard Enterprise.	
4	Install SafeGuard Enterprise Server.	SGNServer.msi
5	Configure Microsoft SQL Server database authentication for the SafeGuard Enterprise Master Security Officer.	
6	Generate the SafeGuard Enterprise Database(s) with a script.	Scripts in product delivery in Tools\Database scripts directory

Step	Description	Package/Tool
7	Install the management console SafeGuard Management Center for central management of users, computers, policies, keys and reports.	SGNManagementCenter.msi
8	Configure SafeGuard Management Center: database and database server connections, certificates, Master Security Officer credentials.	SafeGuard Management Center Configuration Wizard
9	Register and configure SafeGuard Enterprise Server: Create server configuration package and deploy it on the web server.	SafeGuard Management Center Configuration Package Tool
10	Create the organizational structure from Active Directory or manually.	SafeGuard Management Center
11	Prepare endpoints for encryption.	SGxClientPreinstall.msi
12	Create initial configuration package for endpoint configuration.	SafeGuard Management Center Configuration Package Tool
13	Install encryption software and initial configuration package on endpoints.	For available packages, see About managed and unmanaged endpoints (page 48).

2.2 Check the system requirements

Before you deploy SafeGuard Enterprise, check the system requirements.

For hardware and software requirements, service packs and disk space required during installation as well as for effective operation, see the current release notes version on the SafeGuard release notes landing page http://www.sophos.com/en-us/support/knowledgebase/112776.aspx.

2.3 Download installers

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

2.4 Language settings

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

Wizards

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

SafeGuard Management Center

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

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

SafeGuard Enterprise on endpoints

You set the language of SafeGuard Enterprise on endpoints in a policy of the type **General Settings** in the SafeGuard Management Center, setting **Customization > Language used on client**:

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

2.5 Compatibility with other Sophos products

This section describes the compatibility of SafeGuard Enterprise 7.0 with other Sophos products.

2.5.1 Compatibility with SafeGuard LAN Crypt

SafeGuard LAN Crypt 3.7x and SafeGuard Enterprise 7.0 can coexist on one endpoint. If you want to use the feature SafeGuard Data Exchange, you must install an additional compatibility component for successful operation of these product versions on one endpoint.

Note: You will find the compatibility component in your product delivery: Install `SGFileEncCompLayer.msi` on 32 bit systems and `SGFileEncCompLayer_x64.msi` on 64 bit systems.

If SafeGuard LAN Crypt 3.7x is already installed:

1. Install the compatibility component on the endpoint.
2. Install the SafeGuard pre-installation package on the endpoint.
3. Install SafeGuard Data Exchange on the endpoint.
4. Install the SafeGuard client configuration package on the endpoint.

5. Restart the endpoint.

Note: During installation a message might be displayed informing you that the component SGLC Profile Loader is already in use. You can ignore this message. It is caused by the fact that SafeGuard LAN Crypt and SafeGuard Enterprise share common components. The affected components will be updated upon restart.

If SafeGuard Enterprise 7.0 is already installed:

1. Install SafeGuard LAN Crypt 3.7x on the endpoint.
2. Install the compatibility component on the endpoint.
3. Restart the endpoint.

Note: Previous versions of both products cannot coexist on one computer. For example, if you try to install SafeGuard LAN Crypt 3.6x on a computer with SafeGuard Enterprise 7.0 already installed, the setup is cancelled and an error message is displayed.

2.5.2 Compatibility with SafeGuard PrivateCrypto and SafeGuard PrivateDisk

SafeGuard Enterprise 7.0 and the standalone products SafeGuard PrivateCrypto (version 2.30 or above) and SafeGuard PrivateDisk (version 2.30 or above), can coexist on the same computer.

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

2.5.3 Compatibility with SafeGuard RemovableMedia

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

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

2.5.4 Compatibility with Sophos Enterprise Console

If you use Sophos Enterprise Console (SEC) to manage encryption, do not install the SafeGuard Enterprise Server or a SafeGuard Management Center on the server where the SEC management server is installed.

2.6 General Restrictions

Note the following general restrictions for SafeGuard Enterprise on endpoints:

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

- If using Intel Advanced Host Controller Interface (AHCI) on the endpoint, the boot hard disk must be in Slot 0 or Slot 1. You can insert up to 32 hard disks. SafeGuard Enterprise only runs on the first two slot numbers.
- SafeGuard volume-based encryption for volumes that are located on Dynamic Disks and on GUID Partition Table disks, (GPT), is not supported. In such cases, installations are terminated. If such disks are found on the endpoint, they are not supported.
- The SafeGuard full disk encryption (SafeGuard volume-based encryption and BitLocker support) modules do not support systems that are equipped with hard drives attached through a SCSI bus.
- **Fast User switching** is not supported.
- Operating SafeGuard Enterprise in a terminal server environment is not supported.

3 Setting up SafeGuard Enterprise Server

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

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

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

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

3.1 Prerequisites

The following prerequisites must be met:

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

  IIS is available free of charge. You find the program on your Windows DVD, for example, or on the Microsoft website.
- If you use SSL transport encryption between SafeGuard Enterprise Server and SafeGuard Enterprise Client you have to set up the IIS for it in advance, see Securing transport connections with SSL (page 39).

  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 4 and ASP.NET 4 must be installed. It is provided in the SafeGuard Enterprise product delivery.

3.2 Installing and configuring Microsoft Internet Information Services (IIS)

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

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

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

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

   IIS is installed with a default configuration for hosting ASP.NET.
9. Check that the web page is displayed properly using http://< server name>. For further information, see: http://support.microsoft.com.

3.2.1.1 Check .NET Framework registration on IIS 7

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

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

1. From the **Start** menu, select **Run...**.
2. Enter the following command: **`Appwiz.cpl`**. All programs installed on the computer are displayed.
3. Check if .NET Framework Version 4 is displayed. If it is not displayed, install this version. Follow the steps in the installation wizard and confirm all defaults.

4. To test that the installation is correctly registered, go to C:\Windows\Microsoft.NET\Framework. Each installed version must be visible as a separate folder showing the version as folder name, for example "v 4.0".

3.2.1.2 Check ASP.NET registration on IIS 7

ASP.NET Version 4 is required.

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

Version 4.0 should be displayed for ASP.NET.

3.2.2 Install and configure IIS 8 on Microsoft Windows Server 2012/2012 R2

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

1. On the **Server Manager Dashboard**, click **Manage** and select **Add Roles and Features**.
2. In the **Add Roles and Features Wizard**, on the **Before you Begin** page, verify the following:
   - The administrator account has a strong password.
   - The network settings, for example IP addresses are configured.
   - The latest security updates from Windows Update are installed.
3. Select **Server Roles** on the left hand pane and then select **Web server (IIS)**. Click **Add Features** in the displayed window. **Web Server Role (IIS)** is listed on the left hand pane of the **Add Roles and Features Wizard**.
4. In the left hand pane select **Role Services** under **Web Server Role (IIS)**. Keep the default roles services.
5. Scroll down to the **Application Development** node and check:
   - **ASP.NET 4.5**
   - **ISAPI Extensions**
   - **ISAPI Filters**

   Necessary sub-role services are selected automatically.
6. Under the **Security** node check:
   - **Basic Authentication**
   - **Windows Authentication**
7. Click **Next**, then **Install** and **Close**,

   Your IIS server service is installed with a default configuration for hosting ASP.NET.

3.3 Install SafeGuard Enterprise Server

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

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

SafeGuard Enterprise Server including Task Scheduler is installed.

Note: To enhance performance, the connection of logged events is deactivated for the SafeGuard Enterprise Database by default after installation of SafeGuard Enterprise Server. However, the connection of logged events is necessary for integrity protection of logged events. All entries in the event table are concatenated so that if an entry is removed this is evident and can be verified with an integrity check. To make use of integrity protection, you need to set the connection of logged events manually. For further information, see the *SafeGuard Enterprise administrator help*, chapter *Reports*.

4 Setting up SafeGuard Enterprise Database

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

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

You can set up the database either automatically during first-time configuration in the SafeGuard Management Center or manually using the SQL scripts provided in your product delivery. Depending on your enterprise environment, check which method to choose. For further information, see Database access rights (page 16).

To enhance performance, the SafeGuard Enterprise Database may be replicated to several SQL servers. To set up database replication, see Replicating the SafeGuard Enterprise Database (page 66).

Multiple SafeGuard Enterprise Databases can be created and maintained for different tenants such as different company locations, organizational units or domains (multi-tenancy). To configure multi-tenancy, see Multi Tenancy configurations (page 27).

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

4.1 Database authentication

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

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

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

Use SQL authentication for computers that are not part of a domain, otherwise use Windows authentication. If you use SQL authentication, we highly recommend that you secure the connection to and from the database server with SSL. For further information, see Set up SSL (page 39).

4.1.1 Database access rights

SafeGuard Enterprise is set up in such a way that, to work with the SQL database, it only needs a single user account with minimum access rights for the database. This user account is used by

the SafeGuard Management Center and is only issued to the first SafeGuard Management Center security officer. This guarantees the connection to the SafeGuard Enterprise Database. While SafeGuard Enterprise is running, a single SafeGuard Management Center security officer only needs read/write permission for the SafeGuard Management Center Database.

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

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

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

SQL Server 2012, SQL Server 2012 Express	Access Right
Create database	
Server	db_creator
Master database	None
SafeGuard Enterprise Database	db_ownerpublic (default)
Use database	
Server	None
Master database	None
SafeGuard Enterprise Database	db_datareader db_datawriter public (default)

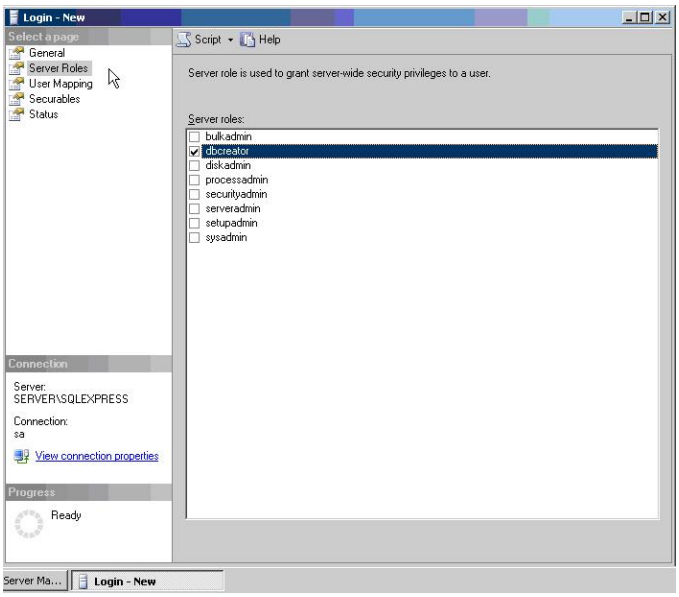
4.1.2 Configure a Windows account for SQL Server logon

The description of the individual configuration steps below is aimed at SQL administrators and relates to Microsoft Windows Server 2008 and Microsoft SQL Server 2014 Standard or Express Edition.

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

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

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



4.1.3 Create an SQL account for SQL Server logon

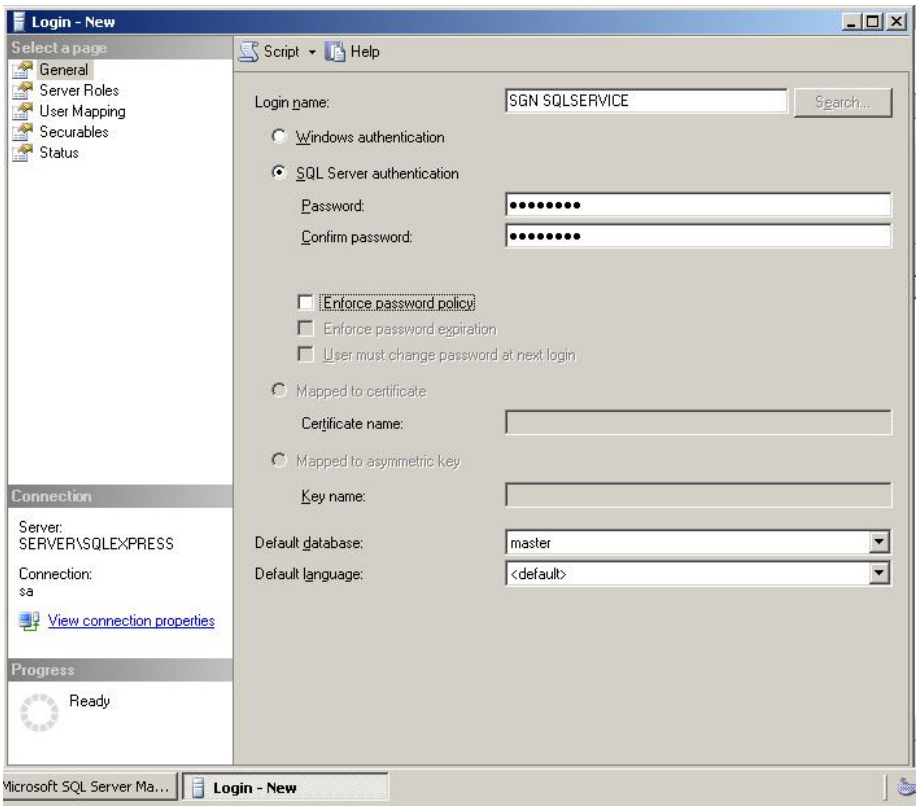
The description of the individual configuration steps below is aimed at SQL administrators. It relates to Microsoft Windows Server 2008 all editions with Microsoft SQL Server 2008 Standard Edition.

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

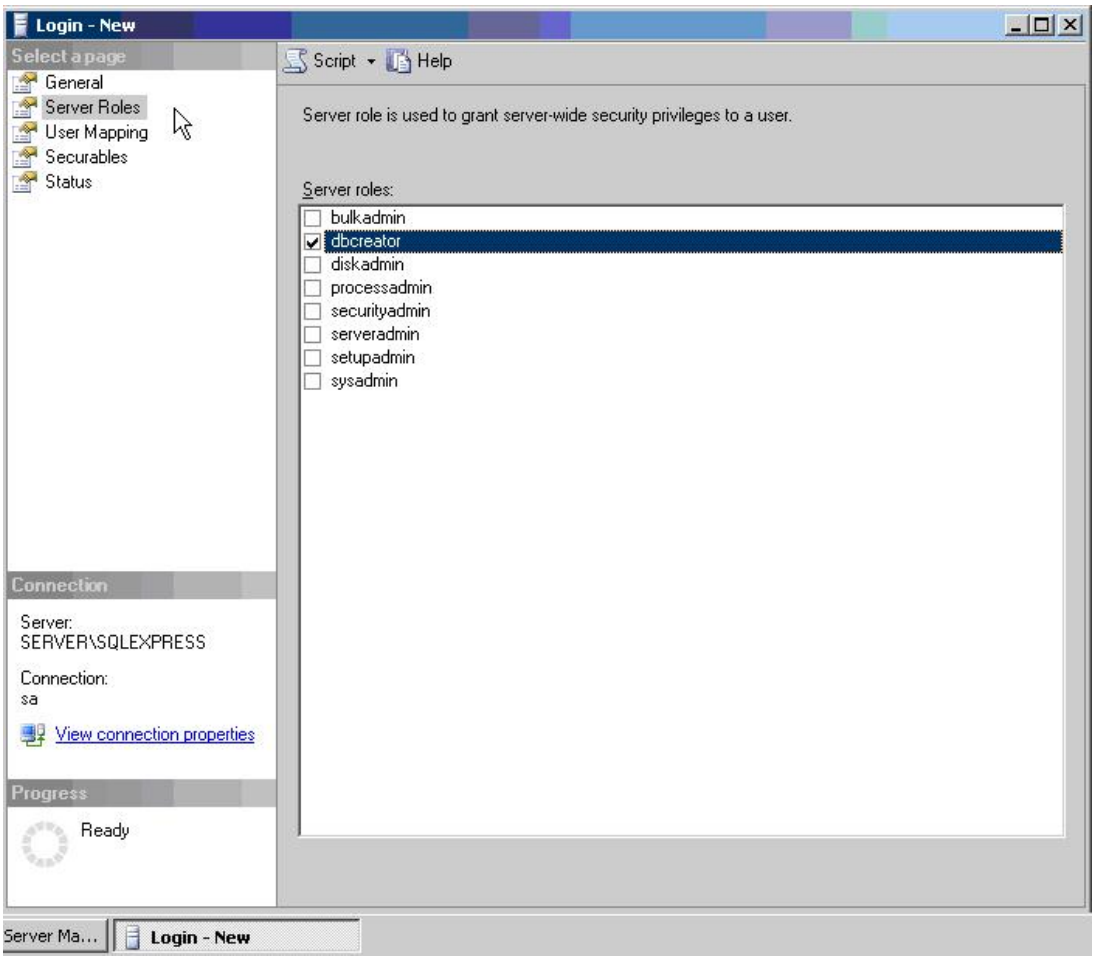
1. Open SQL Server Management Studio. Log on to the SQL Server with your credentials.
2. Open the **Object Explorer**, right-click **Security**, point to **New** and then click **Logins**.
3. In **Login - New** on the **General** page, select **SQL Server authentication**.

4. On the **General** page, in **Login name**, do the following:
   a) Enter the name of the new user, for example SGN SQLSERVICE.
   b) Enter and confirm a password for the account.
   c) Clear **Enforce password policy**.
   d) In **Default Database,** if a script has not been used to create a SafeGuard Enterprise Database yet, select **Master**. Click **OK**.

   Take a note of the authentication method and the credentials. You have to inform the SafeGuard Management Center security officer about them.



5. To create the database automatically during SafeGuard Management Center first-time configuration, you have to change the access rights as follows: In **Login - New** on the **General** page, assign the access rights/roles by clicking **Server Roles** on the left. Select **dbcreator**. Once SafeGuard Enterprise has been installed, the database role can be reset to **dbowner**.



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

4.2 Generating the SafeGuard Enterprise Database

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

- Using SafeGuard Management Center Configuration Wizard

  As a security officer, you can easily create the SafeGuard Enterprise Database during first-time configuration in the SafeGuard Management Center. The SafeGuard Management Center Configuration Wizard takes you through the basic configuration which also includes database creation. To do so, carry on with installing and configuring SafeGuard Management Center, see Setting up SafeGuard Management Center (page 25), and then continue with changing

the relevant access rights, see Change access rights for the SafeGuard Enterprise Database (page 22).

- Using SQL scripts provided in the product delivery

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

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

4.2.1 Prerequisites

The following prerequisites must be met:

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

4.2.2 Generate SafeGuard Enterprise Database with a script

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

- CreateDatabase.sql
- CreateTables.sql

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

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

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

7. At the top of the script, enter **`use SafeGuard`** to select the SafeGuard Enterprise Database in which the tables are to be created.
8. Click **Execute** from the Toolbar to generate the tables.

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

4.3 Change access rights for the SafeGuard Enterprise Database

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

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

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

The description relates to Microsoft Windows Server 2008 (R2) and Microsoft SQL Server 2012 Standard or Express Edition.

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

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

The description relates to Microsoft Windows Server 2008 (R2) with Microsoft SQL Server 2012 Standard or Express Edition. When you use this configuration, carry out the steps below to ensure

that a connection between SafeGuard Enterprise Database and SafeGuard Management Center can be established.

1. On the computer hosting the SQL Server instance, click **Start**, select **Administrative Tools** and then click **Windows Firewall with Advanced Security**.
2. From the navigation tree on the left, select **Inbound Rules**.
3. Click **Action** from the menu bar, and then click **New Rule**. The **New Inbound Rule Wizard** is launched.
4. On the **Rule Type** page, select **Custom** and click **Next**.
5. On the **Program** page, select the program and services this rule should apply to, and then click **Next**.
6. On the **Protocol and Ports** page, select **TCP** as **Protocol type**. For **Local port**, select **Specific Ports** and enter **1433**. For **Remote Port**, select **All Ports**. Click **Next**.
7. On the **Scope** page, you can specify that the rule applies only to network traffic to or from the IP addresses entered on this page. Configure as appropriate, and then click **Next**.
8. On the **Action** page, select **Allow the connection**, and click **Next**.
9. On the **Profile** page, select where to apply the rule, and click **Next**.
10. On the **Name** page, type a name and description for your rule, and click **Finish**.

4.6 Configure Windows authentication for SQL Server logon

The description relates to Microsoft Windows Server 2008 with Microsoft SQL Server 2012 Standard Edition and IIS 7.

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

1. Select **Start** and then **Run**. Enter **dsa.msc**. Open the Active Directory Users and Computers snap-in.
2. In the navigation tree on the left, expand the domain tree and select **Builtin**.
3. Add the respective Windows user to the following groups: IIS_IUSRS, Performance Log Users, Performance Monitor Users.
4. Exit the snap-in.
5. On the local file system, in Windows Explorer, right-click the C:\Windows\Temp folder and select **Properties**. In **Properties**, select the **Security** tab.
6. In **Security**, click **Add**, and enter the respective Windows user name in the **Enter the object names to select** field. Click **OK**.
7. In **Security**, under **Permissions** click **Advanced**. In **Advanced Security Settings for Temp** dialog, on the **Permission** tab, click **Edit**. Then set the following permissions in the **Object** dialog to **Allow**: **List folders / read data**, **Create files / write data**, **Delete**.
8. Click **OK**, exit **Temp Properties** and then Windows Explorer.
9. Open **Internet Information Services Manager**.
10. In the **Connections** pane on the left, select **Application Pools** of the relevant server node.
11. From the **Application Pools** list on the right, select **SGNSRV-Pool**.
12. In the **Actions** pane on the left, select **Advanced Settings.**

13. In **Advanced Settings**, under **Process Model**, for the **Identity** property, click the **...** button.
14. In **Application Pool Identity**, select **Custom account** and click **Set**.
15. In **Set Credentials**, type the relevant Windows user name in the following form: `Domain\<Windows user name>`. Type and confirm the respective Windows password and then click **OK**.
16. In the **Connections** pane on the left, select the relevant server node and click **Restart** from the **Actions** pane.
17. In the **Connections** pane on the left, under the relevant server node, under **Sites**, **Default Web Sites**, select **SGNSRV**.
18. On the SGNSRV homepage in the middle, doubleclick **Authentication**.
19. Right-click **Anonymous authentication** and select **Edit**.
20. For **Anonymous user identity**, select **Specific user** and check that the user name is **IUSR**. Correct it, if necessary.
21. Click **OK**.

Additional configuration when using a Windows account for SQL Server logon is now completed.

5 Setting up SafeGuard Management Center

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

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

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

5.1 Prerequisites

The following prerequisites must be met:

- Make sure that you have Windows administrator rights.
- .NET Framework 4 must be installed. It is provided in the SafeGuard Enterprise product delivery.
- If you want to create a new SafeGuard Enterprise Database during SafeGuard Management Center configuration, you need the necessary SQL access rights and credentials, see Database access rights (page 16).
- If the SafeGuard Enterprise Database and SafeGuard Management Center will be installed on different computers, make sure that SQL Server 2012 Native Client and SQL Server 2014 Command Line Utilities are installed on the computer where you install the SafeGuard Management Center. These are provided in the 3rd party folder of the SafeGuard Enterprise product delivery.

5.2 Install SafeGuard Management Center

1. Start SGNManagementCenter.msi from the install folder of your product delivery. A wizard guides you through the necessary steps.
2. Accept the defaults in the subsequent dialogs except as follows: On the **Select Installation Type** page, do one of the following:
   - For SafeGuard Management Center to support one database only, select **Typical**.
   - For SafeGuard Management Center to support multiple databases **(Multi Tenancy)**, select **Complete**. For further information, see Multi Tenancy configurations (page 27).

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

5.3 Displaying SafeGuard Management Center help system

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

With Microsoft Internet Explorer, the behaviour is as follows:

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

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

5.4 Configuring SafeGuard Management Center

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

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

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

5.4.1 Prerequisites

The following prerequisites must be met:

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

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

5.4.2 Multi Tenancy configurations

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

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

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

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

5.4.3 Start initial SafeGuard Management Center configuration

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

To start the SafeGuard Management Center Configuration Wizard:

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

5.4.4 Configure the database server connection

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

1. On the **Database Server Connection** page, do the following:
   - Under **Connection settings**, select the SQL database server from the **Database Server** list. All computers on a network on which a Microsoft SQL Server is installed are listed. If you cannot select the server, enter the server name or IP address with the SQL instance name manually.
   - Select **Use SSL** to secure the connection between SafeGuard Management Center and SQL database server. We strongly recommend that you do so if you select **Use SQL Server Authentication with the following credentials** under **Authentication**, because this setting will encrypt the transport of the SQL credentials. SSL encryption requires a working SSL environment on the SQL database server which you have to set up in advance, see Securing transport connections with SSL (page 39).

2. Under **Authentication**, activate the type of authentication to be used to access the database server instance. This is needed so that the SafeGuard Management Center is able to communicate with the database:
   - Select **Use Windows NT Authentication** to use your Windows credentials.

     Note: Use this type when your computer is part of a domain. However, additional mandatory configuration is required as the user needs to be authorized to connect to the database, see Configure a Windows account for SQL Server logon (page 17) and Configure Windows authentication for SQL Server logon (page 23).
   - Select **Use SQL Server Authentication with the following credentials** to access the database with the respective SQL credentials. Enter the credentials for the SQL user account that your SQL administrator has created. Where necessary, you may obtain this information from your SQL administrator.

     Note: Use this type when your computer is not part of a domain. Make sure that you have selected **Use SSL** to secure the connection to and from the database server.
3. Click **Next**.

The connection to the database server has been established.

5.4.5 Create or select a database

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

1. Do one of the following:
   - If a database does not yet exist, select **Create a new database named**. Enter a name for the new database. To do this, you need the relevant SQL access rights, see Database access rights (page 16). SafeGuard Enterprise Database names should only consist of the following characters to prevent localization issues: characters (A-Z, a-z), numbers (0-9), underscores (_).
   - If a database has already been created or if you have already installed the SafeGuard Management Center on a different computer, select **Select an available database** and select the respective database from the list.
2. Click **Next**.

5.4.6 Create the Master Security Officer (MSO)

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

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

1. On the **Security Officer Data** page under **Master Security Officer ID**, enter a name for the Master Security Officer.

2. Under **Certificate for Master Security Officer**, do one of the following:
   - Click **Create** to create a new MSO certificate. You are prompted to enter and confirm a password each for the certificate store and for the file the certificate are to be exported to (private key file P12). The certificate is created and displayed under **Certificate for Master Security Officer**.
   - Click **Import** to use a certificate for the MSO that is already available on the network. In **Import Authentication Certificate** browse for the backed up key file. Under **Password for key file** enter the password specified for this file. Enter the password for the certificate store under **Password for certificate store** and confirm it. Click **OK**. The certificate is imported and displayed under **Certificate for Master Security Officer**.

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

   The MSO needs the private key file password for restoring a broken SafeGuard Management Center installation.
3. Click **Next**.

The Master Security Officer is created.

5.4.6.1 Create the MSO certificate

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

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

The MSO certificate is created and saved locally as a backup (<mso_name>.cer).

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

5.4.6.2 Export the MSO certificate

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

To export an MSO certificate:

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

The private key is created and the file is stored in the defined location (mso_name.p12).

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

5.4.6.3 Import the MSO certificate

If an MSO certificate is already available, you need to import it into the certificate store.

Note: A certificate cannot be imported from a Microsoft PKI. An imported certificate must have a minimum of 1024 bits and a maximum of 4096 bits.

1. In **Import Authentication Key file**, click **[...]** and select the key file.
2. Enter the password for the key file.
3. Enter the password for the certificate store.
4. Confirm the password for the certificate store.
5. Click **OK**.

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

5.4.7 Create the company certificate

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

1. On the **Company Certificate** page, select **Create a new company certificate**.
2. Enter a name of your choice.

   Note: Certificates generated by SafeGuard Enterprise, such as the company, machine, security officer and user certificates are signed with hash algorithm **SHA-256** for enhanced security in a first-time installation.

   If you still need to manage SafeGuard Enterprise 6.0 or earlier endpoints with SafeGuard Management Center 7.0, you must select **SHA-1** under **Hash algorithm for generated certificates**. For further information, see the *SafeGuard Enterprise Administrator help*, section *Change algorithm for self-signed certificates*.

   The selected algorithm is used to sign all certificates generated by SafeGuard Enterprise. These are the company and machine certificates, security officer and user certificates.

3. Click **Next**.

The newly created company certificate is stored in the database.

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

To restore a broken database configuration, see Restore a corrupt database configuration (page 34).

5.4.8 Complete initial SafeGuard Management Center configuration

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

A configuration file is created.

You have created the following:

- A connection to the SafeGuard Enterprise Server.

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

SafeGuard Management Center is launched once the configuration wizard has closed.

5.5 Create further database configurations (Multi Tenancy)

Prerequisite: The feature Multi Tenancy must have been installed with an installation of type **Complete**. SafeGuard Management initial configuration must have been carried out, see Start initial SafeGuard Management Center configuration (page 27).

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

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

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

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

Note: For further tasks concerning Multi Tenancy see the *SafeGuard Enterprise administrator help*, chapter *Working with multiple database configurations*.

5.6 Configure additional instances of the SafeGuard Management Center

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

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

1. Install SGNManagementCenter.msi on a further computer with the required features.
2. Start SafeGuard Management Center on the computer with the newly installed SafeGuard Management Center. The Configuration Wizard is launched and guides you through the necessary steps.
3. On the **Welcome** page, click **Next**.

4. On the **Database Server Connection** page, under **Database Server**, select the required SQL database instance from the list. All database servers available on your computer or network are displayed. Under **Authentication**, activate the type of authentication to be used to access this database server instance. If you select **Use SQL Server Authentication with the following credentials**, enter the SQL user account credentials that your SQL administrator has created. Click **Next**.
5. On the **Database Settings** page, click **Select an available database** and select the respective database from the list. Click **Next**.
6. In **SafeGuard Management Center Authentication**, select an authorized person from the list. If Multi Tenancy is enabled, the dialog shows to which configuration the user is going to log on. Enter and confirm the password for the certificate store.

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

7. Click **OK**.

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

8. To import the data, click **Yes**, and then click **OK**. This starts the import process.
9. In **Import authentication key file**, click **[...]** and select the key file. Enter the **password for key file**. Enter the password for the certificate store previously defined in **Cert. store password or token PIN**. Select **Import to certificate store,** or select **Copy to token** to store the certificate on a token.
10. Enter the password once more to initialize the certificate store.

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

5.7 Logon to SafeGuard Management Center

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

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

5.7.1 Log on in Single Tenancy mode

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

SafeGuard Management Center is launched.

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

5.7.2 Log on in Multi Tenancy mode

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

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

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

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

5.8 Setting up the organizational structure in the SafeGuard Management Center

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

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

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

- Creating the company structure manually.

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

You can use either one of these two options or combine them. For example, you can import an Active Directory (AD) either partially or entirely, and create other organizational units (OUs) manually. Whether the organizational structure is imported or created manually, policy assignment is provided.

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

For information on how to import or create an organization structure, see the *SafeGuard Enterprise administrator help*, chapter *Creating the organizational structure*.

5.9 Importing the license file

SafeGuard Enterprise has an integrated license counter. By default, a fixed number of 5 licenses for every available SafeGuard Enterprise component is part of the installation. This enables the

evaluation of other SafeGuard Enterprise components easily without any side effects. When purchasing SafeGuard Enterprise every customer receives a personalized license file for their company which needs to be imported into the SafeGuard Management Center.

For further information, see the *SafeGuard Enterprise administrator help*, chapter *Licenses*.

5.10 Restore a corrupt SafeGuard Management Center installation

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

- The Master Security Officer certificate of the relevant database configuration must have been exported to .p12 file and must be available and valid.
- You must know the passwords for the .p12 file as well as for the certificate store.

To restore a corrupt SafeGuard Management Center installation:

1. Install the SafeGuard Management Center installation package afresh. Open the SafeGuard Management Center. The Configuration Wizard is started automatically.
2. On the **Database Connection** page, select the relevant database server and configure the connection to the database if required. Click **Next**.
3. On the **Database Settings** page, click **Select an available database** and select the relevant database from the list.
4. On the **Security Officer Data** page, do one of the following:
   - If the backed up certificate file can be found on the computer, it is displayed. Enter the password you use for authenticating at SafeGuard Management Center.
   - If the backed up certificate file cannot be found on the computer, select **Import**. Browse for the backed up certificate file and click **Open**. Enter the password for the selected certificate file. Click **Yes**. Enter and confirm the password for authenticating at the SafeGuard Management Center.
5. Click **Next**, and then **Finish** to complete SafeGuard Management Center configuration.

The corrupt SafeGuard Management Center installation is restored.

5.11 Restore a corrupt database configuration

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

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

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

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

To restore a corrupt database:

1. Install the SafeGuard Management Center installation package afresh. Open the SafeGuard Management Center. The Configuration Wizard is started automatically.
2. On the **Database Connection** page, select **Create a new database**. Under **Database settings**, configure the connection to the database. Click **Next**.
3. On the **Security Officer Data** page, select the relevant MSO and click **Import**.
4. In **Import Authentication Certificate**, browse for the backed up key file. Under **Key file password** enter and confirm the password specified for this file. Select **Store key file in certificate store** and enter the password for the store. Click **OK**.
5. The MSO certificate is imported. Click **Next**.
6. On the **Company Certificate** page, select **Restore using an existing company certificate**. Click **Import** to browse for the backed up certificate file that contains the valid company certificate. You are prompted to enter the password specified for the certificate store. Enter the password and click **OK**. Confirm the message with **Yes**. The company certificate is imported.
7. Click **Next**, then **Finish**.

The database configuration is restored.

6 Testing communication

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

6.1 Prerequisites

Make or check the following settings before the connection test.

6.1.1 Ports/connections

The endpoints must create the following connections:

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

The SafeGuard Management Center must create the following connections:

SafeGuard Management Center connection to	Port
SQL database	SQL Server 2012 dynamic port: Port 1433/TCP and Port 1434/TCP
Active Directory	Port 389/TCP
SLDAP	Port 636 for the Active Directory import

The SafeGuard Enterprise Server must create the following connections:

SafeGuard Enterprise Server connection to	Port
SQL database	Port 1433/TCP and Port 1434/TCP for SQL 2012 (Express) dynamic port

SafeGuard Enterprise Server connection to	Port
Active Directory	Port 389/TCP

6.1.2 Authentication method

1. On the computer with SafeGuard Enterprise Server installed, open **Internet Information Services (IIS) Manager**.
2. In the tree structure, click **Internet Information Services**. Click **"Servername"**, **Web Sites**, **Default Web Site**.
3. Right-click **SGNSRV** and click **Properties**.
4. Click the **Directory Security** tab.
5. Under **Authentication and access control**, click **Edit**. In **Authentication Methods**, select **Enable anonymous access**. Under **Authenticated access**, clear **Integrated Windows authentication**.

6.1.3 Proxy server settings for web server and endpoint

Set the proxy server settings as follows:

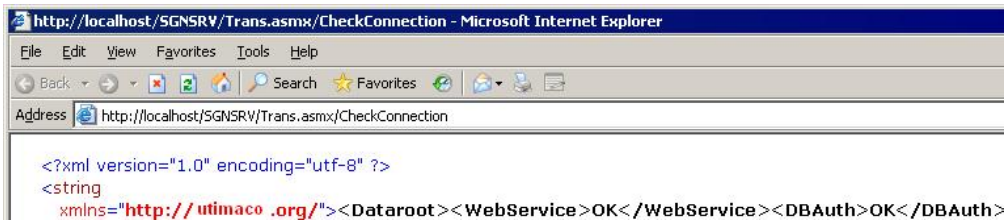
1. In Internet Explorer, on the **Tools** menu, click **Internet options**. Then click **Connections** and click **LAN settings**.
2. In **LAN Settings**, under **Proxy servers**, clear **Use a proxy server for your LAN**.

   If a proxy server is required, click **Bypass proxy server for local addresses**.

6.2 Test the connection (IIS 7 on Windows Server 2008)

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

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


http://localhost/SGNSRV/Trans.asmx/CheckConnection - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://localhost/SGNSRV/Trans.asmx/CheckConnection
<?xml version="1.0" encoding="utf-8" ?>
<string
xmlns="http://utimaco.org/"><Dataroot><WebService>OK</WebService><DBAuth>OK</DBAuth>

7 Securing transport connections with SSL

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

- The connection between the database server and the web server as well as the connection between the database server and the computer on which the SafeGuard Management Center resides may be encrypted with SSL.
- The connection between the SafeGuard Enterprise Server and the SafeGuard Enterprise managed computer may either be secured by SSL or by SafeGuard specific encryption. The advantage of SSL is that it is a standard protocol and therefore a faster connection can be achieved than by using SafeGuard transport encryption.

  Mac: For securing the connection between the SafeGuard Enterprise Server and Mac endpoints, SSL has to be used.

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

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

7.1 Set up SSL

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

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

For further information, contact our technical support or see:

- http://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

7.2 Activate SSL encryption in SafeGuard Enterprise

You may activate SSL encryption in SafeGuard Enterprise as follows:

- Connection between web server and database server:

  Activate SSL encryption when registering the SafeGuard Enterprise Server in the SafeGuard Management Center Configuration Package Tool. For further information, see Configure the database server connection (page 27) or see: http://www.sophos.com/en-us/support/knowledgebase/109012.aspx.

- Connection between the database server and SafeGuard Management Center:

  Activate SSL encryption in the SafeGuard Management Center Configuration Wizard, see Configure the database server connection (page 27).

- Connection between SafeGuard Enterprise Server and the SafeGuard Enterprise protected endpoint:

  Activate SSL encryption when creating the configuration package for the SafeGuard Enterprise managed endpoints in the SafeGuard Management Center Configuration Package Tool, see Create configuration package for managed computers (page 52). For information on how to configure the SafeGuard Enterprise Server and the SafeGuard Enterprise protected endpoint to use SSL for securing communication, see Securing communication between server and endpoint with SSL (page 40).

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

7.3 Securing communication between server and endpoint with SSL

7.3.1 Prerequisites

For securing the communication between the SafeGuard Enterprise Server and the SafeGuard Enterprise protected endpoint with SSL, a valid certificate is required. You can use the following certificate types:

- A self-signed certificate, see Using a self-signed certificate (page 41).
- A certificate issued by a PKI with a private or a public root certificate, see Using a PKI-generated certificate (page 41).

  Technically it makes no difference whether you use a certificate with a public or a private root certificate.

Note: If a certificate created by a public PKI is available but not the PKI infrastructure, you cannot use this certificate to secure communication with SSL. In this case you need to set up a PKI infrastructure or create a self-signed certificate.

7.3.2 Set up the SafeGuard Enterprise Server

To configure the SafeGuard Enterprise Server to use SSL for securing communication between the server and the SafeGuard Enterprise protected endpoint, carry out the following general tasks:

1. Install the SafeGuard Management Center, see Install SafeGuard Management Center (page 25).
2. Install the SafeGuard Enterprise Server, see Install SafeGuard Enterprise Server (page 15).
3. Check the communication between the SafeGuard Enterprise Server and the SQL database using the invoke test.

After you have completed these configuration steps successfully, you import the certificate to use for SSL communication. You can use either a self-signed certificate or an existing one. If you have a PKI infrastructure in place, you can use a PKI-generated certificate.

7.3.3 Using a self-signed certificate

To create a self-signed certificate with SafeGuard Enterprise:

1. Open the Internet Information Services (IIS) Manager on the machine that hosts the SafeGuard Enterprise Server.
2. Check the name of the server displayed at the top node.
3. On the machine with the SafeGuard Management Center installed, select **Programs** followed by **Sophos**, **SafeGuard** and **SafeGuard Certificate Manager**.

   The **SafeGuard Certificate Manager** is displayed.

4. Enter your password to open the SafeGuard certificate store.
5. Click the **Create new certificate** button.

   The **Create new certificate** dialog is displayed.

6. Create a new certificate:

   a) Enter a certificate name that corresponds to the machine identified at the top node in the Internet Information Services (IIS) Manager.

   b) Leave the key length at the default value.

   c) Enter a password.

   d) Click **OK**.

7. Save the cert and p12 files in a location that can be reached by the machine that hosts the IIS.

7.3.4 Using a PKI-generated certificate

If you want to use a PKI-generated certificate for SSL communication, create a certificate for the machine that is running the SafeGuard Enterprise Server. The following requirements apply:

- The certificate name must correspond to the machine that is shown at the top node in the Internet Information Services (IIS) Manager.

- The certificate must be issued to the machine using its FQDN name.

Note: If only a certificate created by a public PKI, but no PKI infrastructure is available, you cannot use this certificate to secure communication with SSL. In this case you need to set up a PKI infrastructure or create a self-signed certificate.

7.3.5 Configure the SGNSRV web page to accept a certificate

Prerequisite: A valid certificate for using SSL is available.

Note: The following description refers to Microsoft Windows Server 2012.

1. Open **Internet Information Services (IIS) Manager**.
2. In the navigation pane select the server that hosts the SGNSRV web page.
3. In the right hand pane select **Server certificates** from the **IIS** section.
4. On the **Server Certificates** page click **Import** in the **Actions** pane.
5. Select the certificate to be used for securing the SSL connection. Enter the password and click **OK**.
6. In the navigation pane right-click **Default Web Site**, and then click **Edit bindings**.
7. Click **Add** in the **Site Bindings** dialog.
8. Under **Type:** select **https** and under **SSL certificate:** select the certificate to be used for securing the SSL connection.
9. Click **OK** and close the **Site Bindings** dialog box.
10. In the navigation pane select the server and click **Restart** in the **Actions** pane.

7.3.6 Configure the endpoint to use SSL

To use SSL on the SafeGuard Enterprise protected endpoint, carry out the following steps:

1. Assign the certificate to the client.
2. Create a client configuration package that includes SSL, see Create configuration package for managed computers (page 52).

7.3.6.1 Assign a certificate

There are several ways for assigning a certificate to an endpoint. One way is assigning it by using a Microsoft Group Policy, which is described in this section. If you want to use a different method, make sure that the certificate is stored in the local machine certificate store.

To assign a certificate by using Group Policy:

1. Open **Group Policy Management** console.
2. Find an existing or create a new GPO to contain the certificate settings. Ensure that the GPO is associated with the domain, site, or organizational unit whose users you want to manage with the policy.
3. Right-click the GPO, and then select **Edit**.

   Group Policy Management Editor opens, and displays the current contents of the policy object.

4. In the navigation pane, open **Computer Configuration** > **Windows Settings** > **Security Settings** > **Public Key Policies** > **Trusted Publishers**.
5. Click the **Action** menu, and then click **Import**.
6. Follow the instructions in the **Certificate Import Wizard** to find and import the certificate.
7. If the certificate is self-signed, and cannot be traced back to a certificate that is in the **Trusted Root Certification Authorities** certificate store, then you must also copy the certificate to that store. In the navigation pane, click **Trusted Root Certification Authorities**, and then repeat steps 5 and 6 to install a copy of the certificate to that store.

8 Registering and configuring SafeGuard Enterprise Server

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

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

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

8.1 Register and configure SafeGuard Enterprise Server for the current computer

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

Note: This option is not available if Multi Tenancy is installed.

1. Start SafeGuard Management Center.
2. On the **Tools** menu, click **Configuration Package Tool**.
3. Select the **Servers** tab and then select **Make this computer an SGN Server**.

   SafeGuard Enterprise Server Configuration setup is automatically started.

4. Accept the defaults in all subsequent dialogs.

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

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

8.2 Register and configure SafeGuard Enterprise Server for a different computer

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

1. Start SafeGuard Management Center.

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

   Do not select the MSO certificate.

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

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

5. Click **OK**.

   The server information is displayed in the **Servers** tab.

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

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

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

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

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

8.3 Edit SafeGuard Enterprise Server properties

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

1. On the **Tools** menu, click **Configuration Package Tool**.
2. Select **Servers** tab and then select the required server.

3. Carry out any of the following:

Element	Description
Scripting allowed	Click to enable use of the SafeGuard Enterprise Management API. This allows for scripting administrative tasks.
Win. Auth. WHD	Click to enable Windows Authentication for Web Helpdesk. By default, the option is disabled.
Server roles	Click to select/deselect an available security officer role for the selected server.
Add server role...	Click to add further specific security officer roles for the selected server if required. You are prompted to select the server certificate. The security officer role is added and can be displayed under **Server roles**.
Database connection	Click **[...]** to configure a specific database connection for any registered web server, including database credentials and transport encryption between the web server and the database server. For further information, see Configure the database server connection (page 27). Even if the database connection check has not been successful, a new server configuration package can be created. **Note:** You do not have to rerun the SafeGuard Management Center Configuration Wizard to update the database configuration. Simply make sure that you create a new server configuration package afterwards and distribute it to the respective server. When the updated server package is installed on the server, the new database connection can be used.

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

The new server configuration becomes active.

8.4 Register SafeGuard Enterprise Server with Sophos firewall enabled

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

1. As a workaround, do one of the following:
   - Unblock NetBIOS connections in the firewall.

- Include the fully qualified name of the SafeGuard Enterprise Server in the server configuration package. For further information, see Register and configure SafeGuard Enterprise Server for a different computer (page 44).

9 Setting up SafeGuard Enterprise on endpoints

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

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

9.1 About managed and unmanaged endpoints

Endpoints can be configured as follows:

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

  Central server-based management in SafeGuard Management Center.

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

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

  Local management through configuration packages created in SafeGuard Management Center.

  Unmanaged endpoints are not connected to the SafeGuard Enterprise Server at all and they are not connected to the central management of SafeGuard Enterprise. They operate in standalone mode.

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

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

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

9.2 Restrictions

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

9.2.1 Restrictions for managed endpoints

Note the following restrictions for managed endpoints.

- **Restrictions for initial encryption:**

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

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

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

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

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

- **Restrictions for BitLocker Drive Encryption support:**

  Either SafeGuard Enterprise volume-based encryption or BitLocker Drive Encryption can be used, but not both simultaneously. If you want to change the encryption type, you must first decrypt all encrypted drives, uninstall the SafeGuard Enterprise encryption software and then reinstall it with the features you want to use. The installer prevents the deployment of both features at the same time. Uninstallation and reinstallation is necessary even if no configuration package intended to trigger encryption has been installed.

9.2.2 Restrictions for unmanaged endpoints

File Encryption is not supported for unmanaged endpoints - Sophos SafeGuard Clients (standalone).

9.3 Preparing endpoints for encryption

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

- A user account must be set up and active on the endpoints.
- Ensure that you have Windows administrator rights.
- Create a full backup of the data on the endpoint.
- Drives to be encrypted must be completely formatted and have a drive letter assigned to them.
- Sophos provides a hardware configuration file to minimize the risk of conflicts between the POA and your endpoint hardware. The file is contained in the encryption software package.

We recommend that you install an updated version of this file before any significant deployment of SafeGuard Enterprise. The file is updated on a monthly basis and made available to download from: http://www.sophos.com/en-us/support/knowledgebase/65700.aspx

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

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

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

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

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

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

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

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

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

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

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

9.3.1 Prepare for Cloud Storage

The SafeGuard Enterprise module Cloud Storage offers file-based encryption of data stored in the cloud.

Cloud Storage makes sure that local copies of cloud data are encrypted transparently and remain encrypted when stored in the cloud.

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

To prepare endpoints for Cloud Storage:

- The cloud storage software provided by the vendor must be installed on the endpoints where you want to install Cloud Storage.
- The cloud storage software provided by the vendor must have an application or system service stored on the local file system that synchronizes data between the cloud and the local system.
- The cloud storage software provided by the vendor must store the synchronized data on the local file system.

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

9.3.2 Prepare for BitLocker Drive Encryption support

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

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

- Windows 7 or Windows 8 must be installed on the endpoint.
- BitLocker Drive Encryption must be installed and activated.
- If TPM is to be used for authentication, TPM must be initialized, owned and activated.
- If you wish to install SafeGuard Enterprise volume-based encryption, you should make sure that no volumes have yet been encrypted with BitLocker Drive Encryption. Otherwise the system may be harmed.
- To install BitLocker Drive Encryption support, either deactivate User Access Control (UAC) or log on with the built-in Administrator account.

9.3.3 Prepare for a "Modify" installation

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

This behavior applies to installation in attended and unattended mode.

9.4 Creating configuration packages

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

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

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

9.4.1 Create configuration package for managed computers

1. In the SafeGuard Management Center, on the **Tools** menu, click **Configuration Package Tool**.
2. Select **Managed client packages**.
3. Click **Add Configuration Package**.
4. Enter a name of your choice for the configuration package.
5. Assign a primary SafeGuard Enterprise Server (the secondary server is not necessary).
6. If required, specify a policy group which must have been created beforehand in the SafeGuard Management Center to be applied to the computers. If you want to use service accounts for post-installation tasks on the computer, make sure that you include the respective policy setting in this first policy group, see Service accounts for post-installation tasks (page 54).
7. Select the **Transport Encryption** mode defining how the connection between SafeGuard Enterprise Client and SafeGuard Enterprise Server is to be encrypted, either SafeGuard transport encryption or SSL encryption.

   The advantage of SSL is that it is a standard protocol and that a faster connection can be achieved than when using SafeGuard transport encryption. SSL encryption is selected by default. For further information, see Securing transport connections with SSL (page 39).

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

   If you have selected SSL encryption as the **Transport Encryption** mode, the server connection is validated. If the connection fails, a warning message is displayed.

The configuration package (MSI) has now been created in the specified directory. You now need to distribute and deploy this package to the endpoints.

9.4.2 Create configuration package for unmanaged computers

1. In the SafeGuard Management Center, on the **Tools** menu, click **Configuration Package Tool**.
2. Select **Standalone client packages**.

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

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

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

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

The configuration package (MSI) has now been created in the specified directory. You now need to distribute and deploy this package to the endpoints.

9.4.3 Create configuration package for Macs

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

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

   The server connection for the SSL **Transport Encryption** mode is validated. If the connection fails, a warning message is displayed.

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

9.4.4 Service accounts for post-installation tasks

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

With service accounts the workflow is as follows:

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

Note: You need to create service account lists in a policy and assign it to the first policy group of the first configuration package you install on the endpoint after the encryption software is installed. For further information, see the *SafeGuard Enterprise administrator help*.

9.5 Installing the encryption software

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

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

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

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

9.5.1 Installation packages and features

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

Note: When the operating system of the endpoint is Windows 64-bit, install the 64-bit variant of the installation packages (<package name>_x64.msi).

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

Package	Content	Available for managed endpoints	Available for unmanaged endpoints
SGxClientPreinstall.msi	**Pre-installation package** The package must be installed before installing any encryption installation package. Provides endpoints with necessary requirements for successful installation of the current encryption software.	 mandatory	 mandatory
SGNClient.msi SGNClient_x64.msi	**SafeGuard client installation package** Provides endpoints with necessary requirements for successful installation of the current encryption software. For full disk encryption for internal and external hard disks, SafeGuard Enterprise offers the alternatives **SafeGuard volume-based encryption** or **BitLocker**.		
	SafeGuard volume-based encryption (only Windows 7 BIOS) SafeGuard full disk encryption. Includes SafeGuard Power-on Authentication. Select installation type **Complete**, **Typical**, **Custom**.		
	BitLocker or **BitLocker C/R** SafeGuard Enterprise manages the Microsoft BitLocker encryption engine. On UEFI platforms, BitLocker pre-boot authentication comes with a SafeGuard Challenge / Response mechanism whereas the BIOS version allows the retrieval of the recovery key from the SafeGuard Management Center. Select installation type **Custom**.		
	Data Exchange SafeGuard Data Exchange: file-based encryption of data on removable media on all platforms without re-encryption.		

Package	Content	Available for managed endpoints	Available for unmanaged endpoints
	Select installation type **Complete** or **Custom**.		
	File Encryption File-based encryption of data on local hard disks and network shares, especially for workgroups. Select installation type **Complete** or **Custom**.		
	Cloud Storage File-based encryption of data stored in the cloud. Local copies of data stored in the cloud are always encrypted transparently. To send data to or receive data from the cloud, vendor-specific software must be used. Select installation type **Complete** or **Custom**.		

9.5.2 Install the encryption software locally

Prerequisites:

- Endpoints must have been prepared for encryption, see Preparing endpoints for encryption (page 49).
- Decide which encryption package and features you need to install.

To install the encryption software locally:

1. Log on to the endpoint as an administrator.
2. If you have SafeGuard LAN Crypt 3.7 x installed on the endpoint and want to install SafeGuard Data Exchange, first install the compatibility component `SGFileEncCompLayer.msi` or `SGFileEncCompLayer_x64.msi`. You find it in your product delivery. For further information, see Compatibility with SafeGuard LAN Crypt (page 9).
3. Install the latest pre-installation package **`SGxClientPreinstall.msi`** that provides the endpoint with the necessary requirements for a successful installation of the current encryption software.

   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 **`MSVCR100.dll`** is present in the Windows\WinSxS folder on the computer.

4. Double-click the relevant encryption software package (MSI). A wizard guides you through the necessary steps.
5. In the wizard, accept the defaults on all subsequent dialogs.

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

   SafeGuard Enterprise is installed on the endpoint.

6. Go to the location where you saved the relevant configuration package (MSI) created beforehand in SafeGuard Management Center. Specific configuration packages need to be installed for managed and unmanaged endpoints, see Creating configuration packages (page 52).
7. Install the relevant configuration package (MSI) on the computer.
8. After installation, make sure that endpoints are restarted twice to activate Power-on-Authentication. The computer must be restarted for a third time to perform a backup of the kernel data on every Windows boot.

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

SafeGuard Enterprise is set up on the endpoint. For more information on the computer's logon behavior after SafeGuard Enterprise installation, see the *SafeGuard Enterprise user help*.

9.5.3 Installing the encryption software centrally

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

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

For a central installation, do the following:

- Check the available encryption packages and features for managed and unmanaged endpoints, see Installation packages and features (page 54).
- Check the command-line options.
- Check the list of feature parameters for the ADDLOCAL command-line option.
- Check the sample commands.
- Prepare the installation script.

9.5.3.1 Installing the encryption software centrally through Active Directory

Make sure that you do the following when installing the encryption software centrally using group policy objects (GPO) in an Active Directory:

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

- Use a separate group policy object (GPO) for each installation package and sort them in the following order:

  compatibility component

pre-installation package
encryption software package
endpoint configuration package

For further information on the packages, see Prepare the installation script (page 58).

- When the endpoint language is not set to German, additionally do the following: in the Group Policy Editor, select the respective group object and then **Computer Configuration > Software Settings> Advanced**. In the **Advanced Deployment Options** dialog, select **Ignore language when deploying this package** and click **OK**.

9.5.3.2 Prepare the installation script

Prerequisites:

- Endpoints must have been prepared for encryption.
- Decide which encryption package and features you want to install.

To install the encryption software centrally:

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

Package	Description
Pre-installation package **`SGxClientPreinstall.msi`**	The mandatory package provides the endpoints with the necessary requirements for a successful installation of the current encryption software, for example the required DLL **`MSVCR100.dll`**. **Note:** If this package is not installed, installation of the encryption software is aborted.
Encryption software package	For a list of available packages see Installation packages and features (page 54).
Configuration package for endpoints	Use the configuration packages created before in SafeGuard Management Center. Different configuration packages need to be installed for managed and unmanaged endpoints, see Creating configuration packages (page 52). Make sure that you delete any old ones first.

3. Create a script with the commands for the pre-configured installation. The script must list which features of the encryption software you want to install, see Feature parameters for ADDLOCAL option (page 60). Open a command prompt, and then type the scripting commands. For the command-line syntax, see Command line options for central installation (page 59).

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

   The installation is executed on the endpoints. The endpoints are then ready to be used with SafeGuard Enterprise.

5. After installation, make sure that endpoints are restarted twice to activate Power-on Authentication. They must be restarted for a third time to perform a backup of the kernel data on every Windows boot.

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

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

http://www.sophos.com/en-us/support/knowledgebase/107781.aspx

http://www.sophos.com/en-us/support/knowledgebase/107785.aspx

9.5.3.3 Command line options for central installation

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

Command line syntax

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

The command line syntax consists of:

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

Command line options

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

Option	Description
/i	Specifies the fact that this is an installation.
/qn	Installs with no user interaction and does not display a user interface.
ADDLOCAL=	Lists the SafeGuard Enterprise features that are to be installed. If the option is not specified, all features intended for a standard installation are installed. For a list of SafeGuard Enterprise features in each installation package and availability according to endpoint configuration, see Installation packages and features (page 54). For list of feature parameters for the ADDLOCAL option, see Feature parameters for ADDLOCAL option (page 60).
ADDLOCAL=ALL	Under Windows 7 (BIOS) **ADDLOCAL=ALL** installs the SafeGuard volume-based encryption and all other available features. Under Windows 8 **ADDLOCAL=ALL** installs BitLocker support and all other available features.
REBOOT=Force | NoRestart	Forces or suppresses a restart after installation. If nothing is specified, the restart is forced after installation.
/L* <path + filename>	Logs all warnings and error messages in the specified log file. The parameter **/Le <path + filename>** only logs error messages.
Installdir= <directory>	Specifies the directory in which the SafeGuard Enterprise encryption software is to be installed. If no value is specified, the default installation directory is <SYSTEM>:\PROGRAM FILES\SOPHOS.

9.5.3.4 Feature parameters for ADDLOCAL option

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

- Separate the features by comma, not by space.
- Observe upper and lower case.
- If you select a feature, you also need to add all feature parents to the command line.
- Please note that the names of the features may differ from the corresponding module names. You find them in the table below in parenthesis.
- You must list the features **Client** and **CredentialProvider** by default.

The following tables list the features that can be installed on the endpoints. For further information, see: Installation packages and features (page 54).

Feature Parents	Feature
Client	**CredentialProvider** Mandatory. The feature enables logon with the Credential Provider.
Client, **BaseEncryption**	**SectorBasedEncryption** (SafeGuard volume-based encryption)
	Note: SectorBasedEncryption OR **BitLockerSupport** can be specified.
Client, **BaseEncryption**	**BitLockerSupport** (BitLocker)
Client, **BaseEncryption**, **BitLockerSupport**	**BitLockerSupportCR** (BitLocker C/R)
Client	**SecureDataExchange** (Data Exchange)
Client	**FileShare** (File Encryption)
Client	**CloudStorage** (Cloud Storage)

9.5.3.5 Sample command: SafeGuard volume-based encryption with File Encryption

The command installs the following:

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

Sample command:

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

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

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

9.5.3.6 Sample command: SafeGuard BitLocker Support with Challenge/Response

The command installs the following:

- The endpoints are provided with the necessary requirements for successful installation of the current encryption software.
- Logon to endpoints with Windows Credential Provider.
- SafeGuard BitLocker Support.
- SafeGuard Challenge/Response for BitLocker recovery.
- Configuration package that configures the endpoint as a managed endpoint and enables connection to the SafeGuard Enterprise Server.
- Log files are created.

Sample command:

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

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

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

9.5.3.7 Sample command: SafeGuard BitLocker Support with Challenge/Response and File Encryption

The command installs the following:

- The endpoints are provided with the necessary requirements for successful installation of the current encryption software.
- Logon to endpoints with Windows Credential Provider.
- SafeGuard BitLocker Support.
- SafeGuard Challenge/Response for BitLocker recovery.
- SafeGuard File Encryption with file-based encryption of data on local hard disk and network shares.
- Configuration package that configures the endpoint as a managed endpoint and enables connection to the SafeGuard Enterprise Server.
- Log files are created.

Sample command:

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

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

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

9.6 Install the encryption software for Mac

For information on the installation of the encryption software on Mac OS X clients please refer to the *Sophos SafeGuard File Encryption for Mac Administrator help* and the *Sophos SafeGuard Native Device Encryption for Mac Administrator help*.

9.7 FIPS-compliant installations

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

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

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

You can do so by adding the property to the command line script:

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

Note: This only applies to SafeGuard Enterprise Device Encryption and Windows 7.

Note: If you want to upgrade an FIPS-compliant installation, please note that the new versions will be installed in FIPS-compliant mode as well, independently from the setting you select.

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

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

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

- **Functional checks**

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

- **Security checks**

  Security checks ensure that only SafeGuard Enterprise users are registered on the drive and that only SafeGuard Enterprise users own the keys used to software-encrypt non-self-encrypting drives. If other users are found to be registered at installation, SafeGuard Enterprise automatically tries to disable these users. This is a functionality required by the Opal standard with the exception of a few default "authorities" which are required to run an Opal system.

  Note: The security checks are repeated when an encryption policy for the drive is applied after successful Opal-mode installation. If they fail, drive management must have been manipulated outside of SafeGuard Enterprise since the first check at installation. In this case, SafeGuard Enterprise does not lock the Opal hard drive. A corresponding message will be displayed.

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

From SafeGuard Enterprise version 7 onwards, no Opal checks are performed by default. This means that, although an Opal drive is present, SafeGuard Enterprise will encrypt volumes on this drive using software-based encryption.

If you want to force Opal checks, use the following command line syntax:

```
MSIEXEC /i <name_of_selected_client_msi>.msi OPALMODE=0
```

Note: An upgrade from SafeGuard Enterprise 6.x to SafeGuard Enterprise 7.0 on a system with an Opal HDD used in Opal HW-encryption mode will preserve the Opal HW-encryption mode.

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

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

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

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

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

10 Replicating the SafeGuard Enterprise Database

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

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

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

Important:

The proposed solution does not describe database replication for the purposes of redundant failover, but for improving performance in multi-site scenarios.

10.1 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.

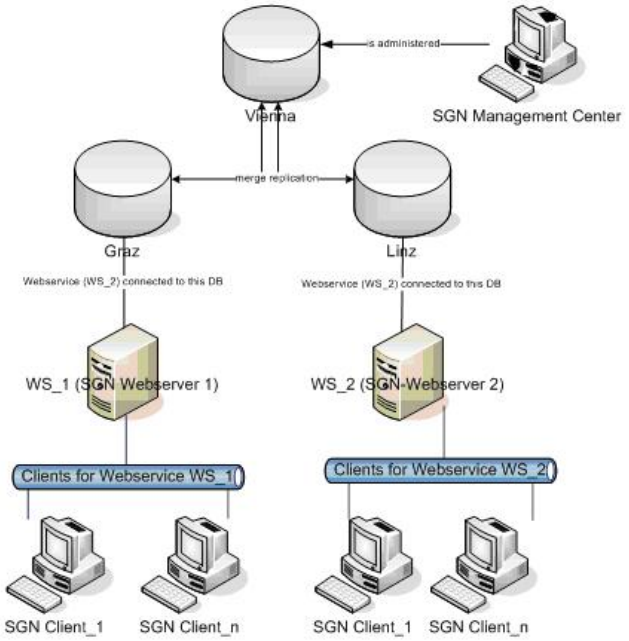
Merge replication allows various sites to work autonomously and at a later time merge updates into a single, uniform result. The initial snapshot is applied to Subscribers, and then Microsoft SQL Server tracks changes to published data at the Publisher and at the Subscribers. The data is synchronized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

10.2 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.

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. Changes reported by the client computers through the web servers are also passed on to the Microsoft SQL Server by way of the replication mechanism.



10.2.1 Generate the master database

Set up the SafeGuard Enterprise master database first. In the example, this is the VIENNA database.

The procedure for generating the master database is the same as for a SafeGuard Enterprise installation without replication.

- Generate the master database in the SafeGuard Management Center Configuration Wizard.

  This procedure requires that the SafeGuard Management Center is already installed. For further information, see Start initial SafeGuard Management Center configuration (page 27).

- Generate the master database with an SQL script. You find them in your product delivery.

  This procedure is often preferred if extended SQL permissions during SafeGuard Management configuration is not desirable. For further information, see Generate SafeGuard Enterprise Database with a script (page 21).

10.2.2 Generate the replication databases Graz and Linz

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

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

To generate the replication databases:

1. Create a publication for the master database in the Management Console of the SQL Server.

   A publication defines the set of data that is to be replicated.

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

The replication databases Graz and Linz have been created.

10.3 Install and register SafeGuard Enterprise Servers

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

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

The SafeGuard Enterprise Servers are installed and registered.

10.4 Create the configuration packages for the Graz database

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

1. In the SafeGuard Management Center, on the **Tools** menu, click **Options**, and then click **Database**.
2. Under **Connection settings**, select **`WS_1`** as **Database Server** and Graz as **Database on Server**. Click **OK**.
3. On the **Tools** menu, click **Configuration Package Tool,** and then click **Server Packages**. Select the **`WS_1`** server, select the output path and click **Create Configuration Package.**
4. Switch to the **Managed client packages** tab. Click **Add Configuration Package** and enter a name for the package. Under **Primary Server** select the correct server the SafeGuard Enterprise Clients Graz are to be connected to: **`WS_1`** . Select the output path and click **Create Configuration Package.**

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

10.5 Create the configuration packages for the Linz database

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

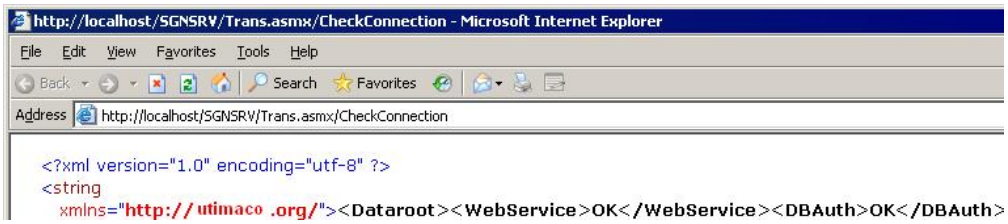
1. In the SafeGuard Management Center, on the **Tools** menu, click **Options**, then click **Database**.
2. Under **Connection settings**, select **`WS_2`** as **Database Server** and Linz as **Database on Server**. Click **OK**.
3. On the **Tools** menu, click **Configuration Package Tools** and then click **Server Packages**. Select the **`WS_2`** server, select the output path and click **Create Configuration Package**.
4. Switch to the **Managed client packages** tab. Click **Add Configuration Package** and enter a name for the package. Under **Primary Server** select the correct server the SafeGuard Enterprise Clients Linz are to be connected to: **`WS_2`**. Select the output path and click **Create Configuration Package**. Click **Close**.
5. Link the SafeGuard Management Center to the Vienna database again: On the **Tools** menu, click **Options**, then click **Database**.

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

10.6 Install the SafeGuard Enterprise Server configuration packages

1. Install the server configuration package **`ws_1.msi`** on web service WS_1 which is to communicate with the Graz database.
2. Install the server configuration package **`ws_2.msi`** on web service WS_2 which is to communicate with the Linz database.
3. Test the communication between the SafeGuard Enterprise Servers and these databases:
   a) On the computer with SafeGuard Enterprise Server installed, open **Internet Information Services (IIS) Manager**.
   b) In the tree structure, click **Internet Information Services**. Click **"Servername"**, **Web Sites**, **Default Web Site**. Check that the web page **SGNSRV** is available in the **Default Web Site** folder.
   c) Right-click **SGNSRV** and click **Browse**. A list of possible actions is displayed on the right-hand side of the window.
   d) From this list, select **CheckConnection**. The possible action is displayed on the right-hand side of the window.
   e) To test the connection, click **Invoke**.

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



10.7 Set up the endpoint

To install the encryption software on endpoints, see Installing the encryption software centrally (page 57) .

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

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

For information on updating replicated SafeGuard Enterprise Databases, see the *SafeGuard Enterprise Upgrade guide*.

11 About uninstallation

This section covers the following topics:

- Uninstallation best practices
- Uninstalling SafeGuard Enterprise encryption software
- Preventing uninstallation of SafeGuard Enterprise encryption software on endpoints

11.1 Uninstallation best practice

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

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

11.2 Uninstalling SafeGuard Enterprise encryption software

Uninstalling the SafeGuard Enterprise encryption software from endpoints involves the following steps:

- Decrypt encrypted data.
- Uninstall the encryption software.

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

11.2.1 Preventing uninstallation on the endpoints

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

11.2.2 Decrypt encrypted data

The following prerequisite must be met:

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

1. In SafeGuard Management Center, edit the current policy of the type **Device Protection** that is assigned to the computers you want to decrypt. Select the targets and set **User may decrypt volume** to **Yes**. Assign the policy to the respective endpoints.
2. Create a decryption policy of the type **Device Protection**, select the targets that are to be decrypted and set the **Media encryption mode** to **No encryption**.
3. In **Users and Computers**, create a group for the computers you want to decrypt: Right-click the domain node where you want to create the group. Then select **New > Create new group**.
4. Select the domain node of this group and assign the decryption policy to it by dragging the policy from the **Available Policies** list into the **Policies** tab. Activate the policy by dragging the group from the **Available Groups** list into the **Activation** area. In the **Policies** tab of the domain node, check that **Priority** is set to 1 and that **No Override** is activated. In the **Activation** area of the domain node, make sure that only members of the group are affected by this policy.
5. In the **Users and Computers** navigation area, select the group, right-click in the **Members** tab shown in the action area and click **Add** to add the computers you want to decrypt to the group.
6. On the endpoint that is to be decrypted, synchronize with the SafeGuard Enterprise Server to make sure that the policy update has been received and is active.
7. Open Windows Explorer. Right-click the volume that should be decrypted and click **Encryption > Decryption**.

   Make sure that the decryption is completed successfully.

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

11.2.3 Start uninstallation

The following prerequisites must be met:

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

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

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

1. In SafeGuard Management Center, edit the policy of the type **Specific Machine Settings**. Set **Uninstallation allowed** to **Yes**.
2. In **Users and Computers**, create a group for the computers you want to decrypt: Right-click the domain node where you want to create the group. Then select **New > Create new group**.

3. Select the domain node of this group and assign the uninstallation policy to it by dragging the policy from the **Available Policies** list into the **Policies** tab. Activate the policy by dragging the group from the **Available Groups** list into the **Activation** area. In the **Policies** tab of the domain node, check that **Priority** is set to 1 and that **No Override** is activated. In the **Activation** area of the domain node, make sure that only members of the group are affected by this policy.
4. Add the endpoints you want to uninstall to the group.
5. To start uninstallation, use one of the following methods:
   - To uninstall locally on the endpoint, synchronize with the SafeGuard Enterprise Server to make sure that the policy update has been received and is active. Then select **Start > Control Panel > Add or Remove Programs > Sophos SafeGuard Client > Remove**.
   - To uninstall centrally use the software distribution mechanism of your choice. Make sure that all required data has been decrypted properly before uninstallation starts.

12 Technical support

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

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

13 Legal notices