

SOPHOS

Security made simple.

SafeGuard Enterprise Installation Best Practice

Product Version: 7

Document date: December 2014

Contents

- Introduction 4
- Technical prerequisites..... 5
- Installation order 6
- 1. Installing the SafeGuard Enterprise Server..... 7
 - 1.1 Quick installation reference..... 8
 - 1.2 Installing IIS services 9
 - 1.3 Installing the SafeGuard Enterprise Server package..... 13
- 2. Creating the SafeGuard Enterprise Database 15
 - 2.1 Quick installation reference..... 15
 - 2.2 Configuring a Windows user to logon to the SQL Server 15
 - 2.3 Creating the SafeGuard Database..... 17
 - 2.4 Changing access permissions for the SafeGuard Database 18
 - 2.5 Checking the SQL Server Service Settings and the Named Pipes Configuration 20
 - 2.6 Adding the SQL user to the SGNSRV-Pool and to the required Active Directory user groups including local permissions..... 21
- 3. Installing the SafeGuard Management Center 24
 - 3.1 Quick installation reference..... 24
 - 3.2 Installing the SafeGuard Management Center..... 24
 - 3.3 Running the SafeGuard Management Center Wizard 24
 - 3.4 Importing the Active Directory into SafeGuard Enterprise (optional) 29
 - 3.5 Importing the license file 32
- 4. Installing the SafeGuard Enterprise Server configuration package 34
 - 4.1 Quick installation reference..... 34
 - 4.2 Creating the SafeGuard Enterprise Server configuration package..... 34
 - 4.3 Installing the SafeGuard Enterprise Server configuration package 36
 - 4.4 Running the invoke test..... 37
- 5. Configuring the SGNSRV web page to use SSL transport encryption 39
 - 5.1 Quick installation reference..... 39
 - 5.2 Creating a self-signed certificate..... 40
 - 5.3 Configuring the SGNSRV web page to accept certificates 42
 - 5.4 Deploying the certificate to the clients 44
- 6. Installing the SafeGuard Enterprise Client on Windows 48
 - 6.1 Quick installation reference..... 48
 - 6.2 Checking the availability of the SSL certificate on the client..... 48

6.3	Preparing the client for installation	51
6.4	Installing the SGNClient_x64.msi and the SGxClientPreinstall.msi.....	52
6.5	Creating the SafeGuard Enterprise Client configuration package	53
6.6	Installing the client configuration package	54
6.7	Rebooting the machine after installation and initializing the user	54
7.	Installing the SafeGuard Enterprise Clients on Mac OS X.....	55
7.1	Quick installation reference	55
7.2	Install Fuse (only required for File Encryption)	55
7.3	Install SafeGuard Enterprise File Encryption for Mac.....	55
7.4	Install SafeGuard Enterprise Disk Encryption for Mac.....	55
7.5	Import the SSL certificate to the system keychain	55
7.6	Import the SafeGuard Enterprise configuration zip file	56
8.	Technical support	57
9.	Legal notices	58

Introduction

This document guides you through a typical SafeGuard Enterprise installation with best practice examples and recommendations.

It does NOT replace the SafeGuard Enterprise Installation Guide, but should help with first steps and simple troubleshooting hints during the installation/implementation of SafeGuard Enterprise.

Note: Some steps refer to the SafeGuard Enterprise Administrator help or to the SafeGuard Enterprise User help which can be found in your product delivery.

Please follow the steps in this guideline chapter by chapter and do not skip any – the chapter numbering follows a chronological order. This guideline is designed for system/network/database administrators installing SafeGuard Enterprise (SGN).

This document describes a set-up that is focused on a maximum of security and performance with regards to the communication between the single components. In case a different setup method can be used to install a module this will be highlighted extra.

All installation examples refer to the Windows Server 2012, IIS Server 8 and Microsoft Windows 8.1. Besides this, the document describes a domain situation in which all machines are members of the same domain. As a result of this, operating system specific tasks may differ when using other software or a workgroup environment.

Technical prerequisites

SafeGuard Enterprise supports a large variety of operating systems and hardware. The minimum hardware requirements and the supported operating systems can be found in the release notes of the product which are available in the Sophos Knowledge Database.

It is highly recommended to read the release notes prior to the installation of SafeGuard Enterprise in order to have all the latest information before starting.

Installation order

SafeGuard Enterprise consists of several different modules.

The minimum modules in order to build up a working SafeGuard Enterprise infrastructure are

- The SafeGuard Enterprise Server.
- The SafeGuard Management Center.
- The SafeGuard Database.
- The SafeGuard Client.

Even if the SafeGuard Enterprise Database is not an extra module of the SafeGuard Enterprise product, it is a vital part of the backend structure to have the product working.

Before being able to deploy any SafeGuard Client regardless of the function installed (SafeGuard Device Encryption, Data Exchange, File Share, Cloud Storage, Native Device Encryption) a working backend is required. As a result of this the installation order of SafeGuard Enterprise is like this:

1. Installing the SafeGuard Enterprise Server.
2. Creating the SafeGuard Database.
3. Installing the SafeGuard Management Center and (optionally) importing the Active Directory.
4. Installing the SafeGuard Enterprise Server Configuration package.
5. Configuring the SGNSRV web page to accept a certificate and assigning the certificate for SSL
6. Installing the SafeGuard Client.

All chapters of this document should be passed in chronological order.

1. Installing the SafeGuard Enterprise Server

On the machine that is hosting the SafeGuard Enterprise web server interface, the installation of Microsoft .Net Framework Version 4 is required (on Windows Server 2012 that is already part of the OS).

Using a dedicated server to host the SafeGuard Enterprise Server is highly recommended. It is possible to run other applications on the same machine but under heavy load from a 3rd party application, the communication between SafeGuard Clients and the SafeGuard Enterprise Server might be impacted.

From a design perspective, we recommend locating the SafeGuard Server(s) close to the Server that hosts the SafeGuard Database. The traffic caused by a communication between a SafeGuard Client and the SafeGuard Server, results in up to three times that amount between the Server and Database. Therefore, WAN connections between Client and Server are preferable to WAN connections between SGN Server(s) and the Database Server.

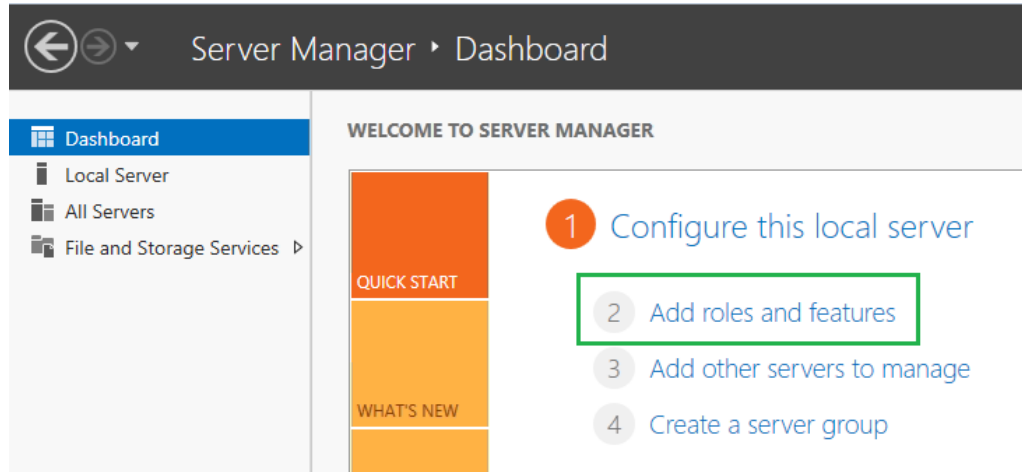
1.1 Quick installation reference

1. Install IIS Services.
2. Install the SafeGuard Enterprise Server.

1.2 Installing IIS services

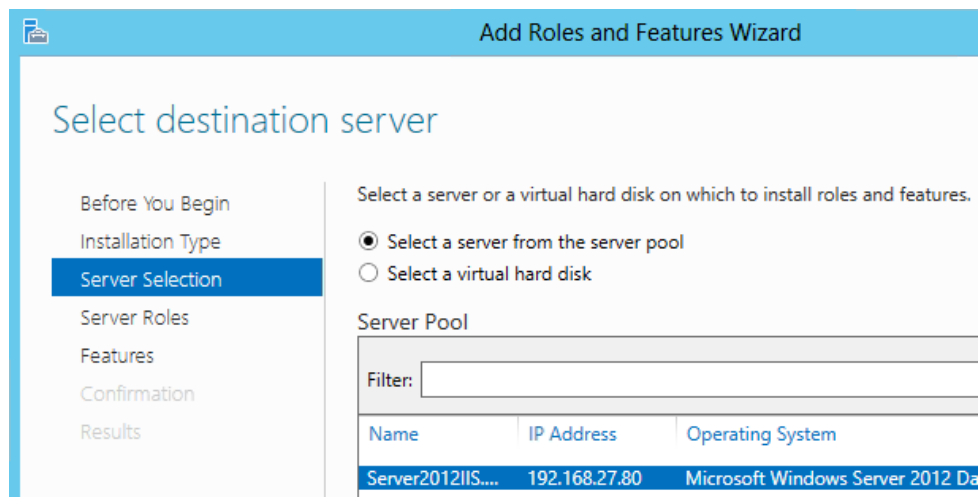
To install SafeGuard Enterprise on an IIS 8 server it is required to install the IIS services on the Windows Server 2012. Please follow these steps:

1. Start the **Server Manager**
2. In the **Server Manager Dashboard** choose **Add roles and features**.

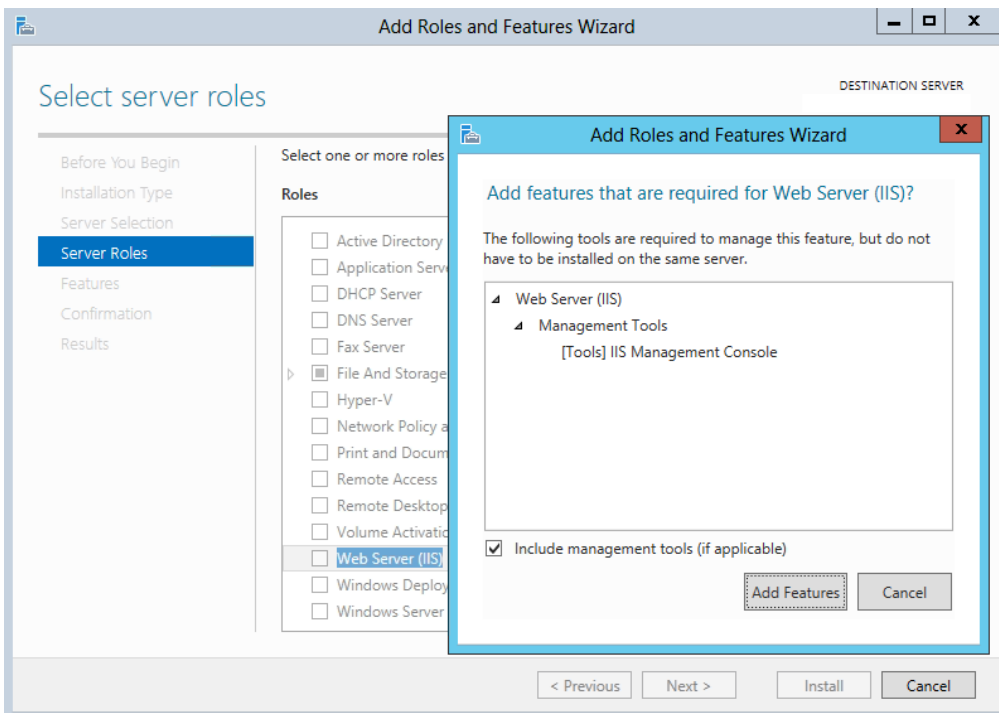


The **Add Roles and Features Wizard** starts with a *Before You Begin* page. The wizard asks for verification of the following:

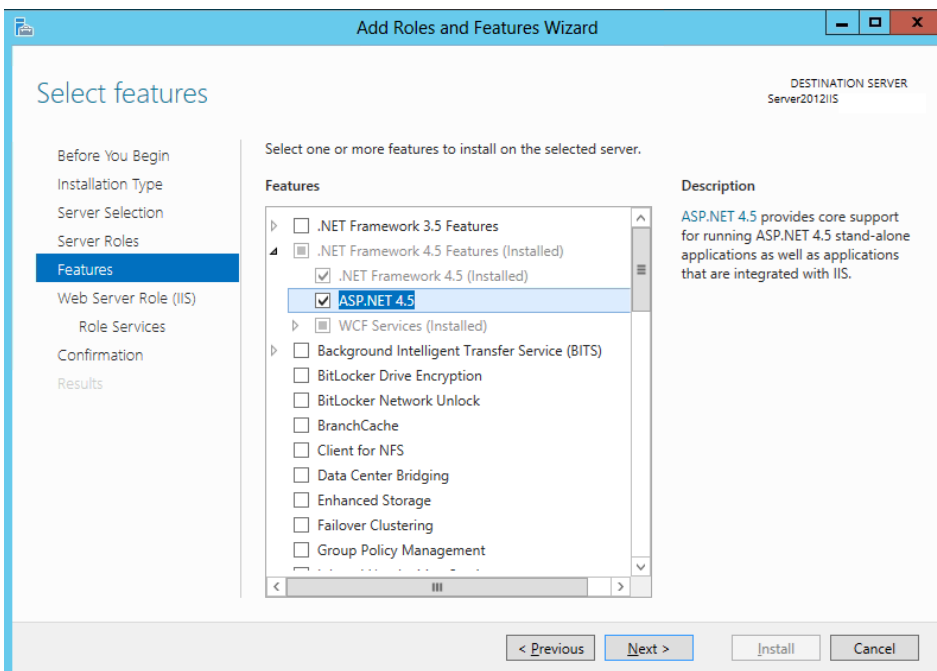
- a. The administrator account has a strong password.
 - b. The network settings, such as IP addresses, are configured.
 - c. The most security updates from Windows Update are installed.
3. On the **Installation Type** step choose *Role-based or feature-based installation* and click next
 4. Select your destination Server and click next



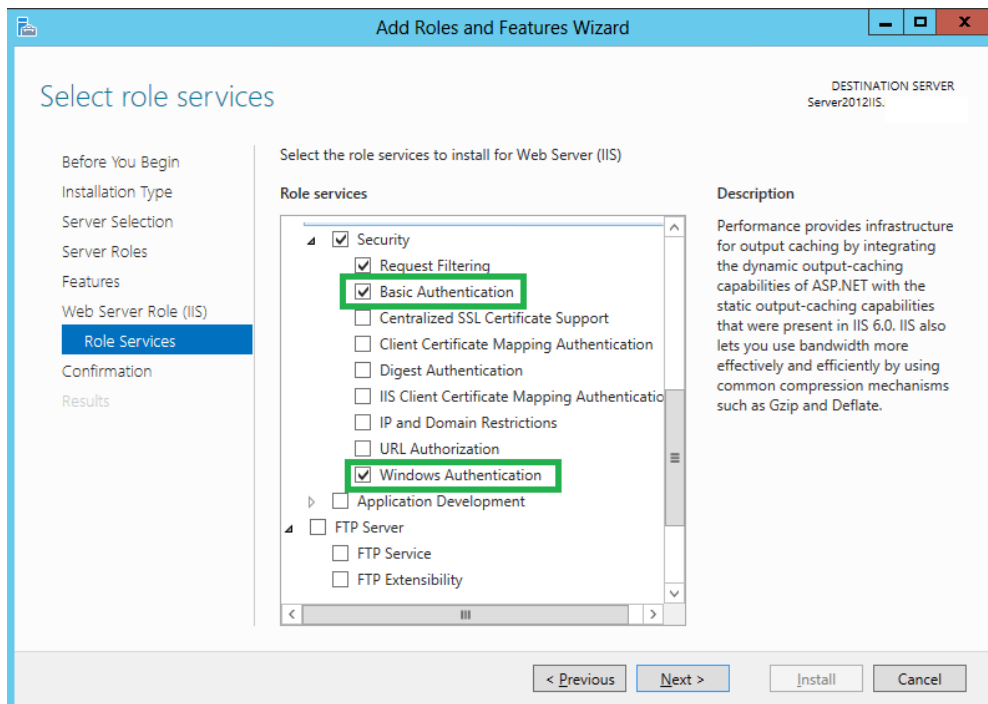
5. Select **Web Server (IIS)** on the **Select server roles** page. Include the management tools and Click on *Add Features*.



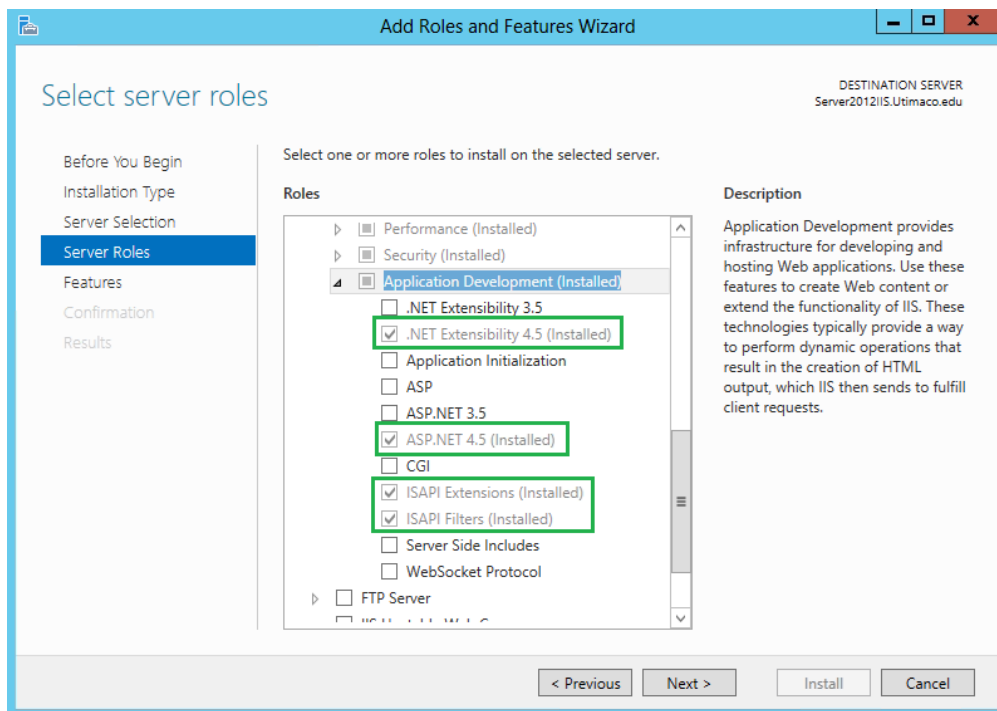
6. On **Select features** add ASP.NET 4.5 and click next



- On **Role Services** check **Basic Authentication** plus **Windows Authentication** under **Security**



- Check **.Net Extensibility 4.5**, **ASP.NET 4.5**, **ISAPI Extensions** and **ISAPI Filters** under **Application Development**



- Verify the installation selections and click **Install**

10. IIS is now installed with a default configuration for hosting ASP.NET on Windows server. Click **Close** to complete the process.
11. Confirm that the web server works using [http://\(Enter machine name without brackets\)](http://(Enter machine name without brackets)). In case that the web page is not shown properly please consider the Microsoft knowledge base (<http://support.microsoft.com>) for further information.

1.3 Installing the SafeGuard Enterprise Server package

The installation of the SafeGuard Enterprise Server is divided into two steps:

1. Installing the SafeGuard Enterprise Server package.
2. Installing the SafeGuard Enterprise Server configuration package which is described later in this document. Please proceed with the guide step by step to avoid side effects.

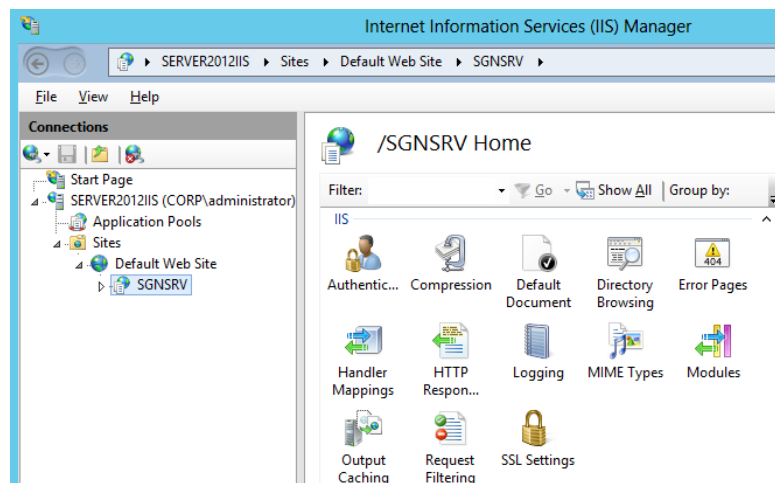
Note: This step cannot be done until the SafeGuard Management Center is installed.

The installation of the SafeGuard Enterprise Server msi package is quite easy. The detailed steps are:

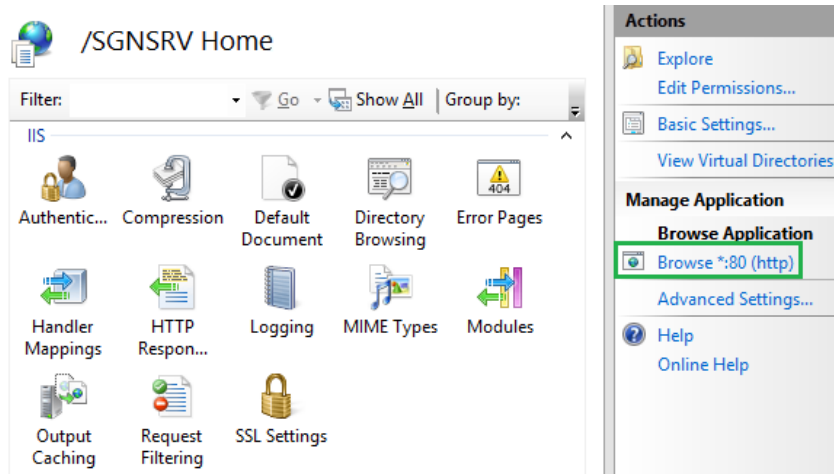
1. Copy the **SGNServer.msi** package from the installation DVD or a network location to the machine that runs the IIS Server.
2. Start the installation by double clicking the MSI package.
Please note: The installation of the SGNServer.msi on Windows Server 2012 and Windows Server 2012 R2 should be run with already elevated privileges, otherwise the installation may fail.
3. The SafeGuard Enterprise server installation wizard comes up and you can choose whether the scheduler service (required for running automated scripts e.g. for maintenance tasks) should get installed in addition to the server itself.

Note: It is not recommended to change the suggested installation path. Especially when installing other modules of SafeGuard on the same machine this could cause unwanted side effects.

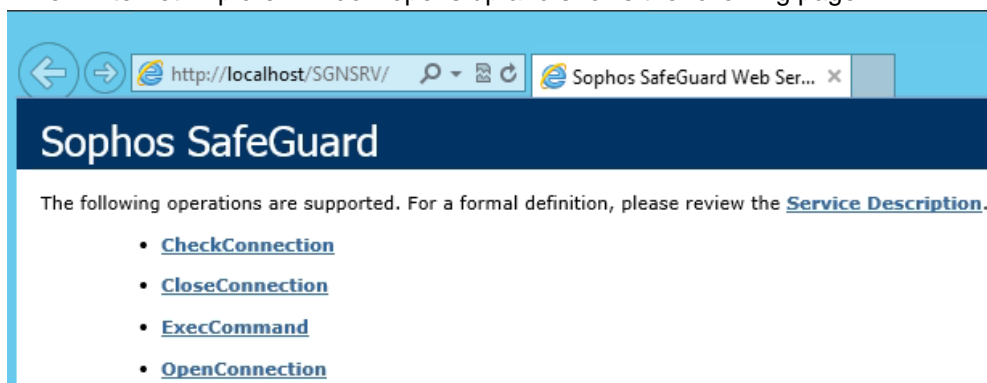
4. To ensure that the installation has completed successfully, open the **Internet Information Services Manager** (run inetmgr) and check if a web page named **SGNSRV** is now available.



To check that everything is working, click on **SGNSRV** in the left hand pane > the **/SGNSRV Home** page opens in the center pane. In the right hand pane click on **Browse *:80 (http)** in the **Manage Application** section.



5. A new Internet Explorer window opens up and shows the following page:



The first part of the SafeGuard Enterprise Server installation is completed now.

2. Creating the SafeGuard Enterprise Database

SafeGuard Enterprise stores all relevant back-end data within a database. The creation of the database can be done automatically during the SafeGuard Management Center initialization or manually using the SQL scripts which are part of the SafeGuard Enterprise product delivery.

Before setting up the database please check the release notes for a list of supported SQL server versions.

Note: When using the SQL Express Edition to host the SafeGuard Database remember the maximum file size limitation of the database given by Microsoft. In large environments, using the SQL Express Edition might be inappropriate.

This example is based on an SQL 2008 Server Standard Edition including the administrative components. The authentication is configured to mixed mode (SQL and Windows Authentication possible). All SQL services are configured to run in the **LOCALSYSTEM** context (of course this can be configured to run in a different context as well).

2.1 Quick installation reference

1. Promote a Windows user account to log on to the SQL Server.
2. Create the database using the SafeGuard Management Center configuration wizard or by running the SQL script provided on the product CD in the SQL Server Management Studio.
3. Change the SQL permissions according to your security need.
4. Check the SQL Browser Service status and the Named Pipes settings.
5. Enter the Windows/SQL user in the SGNSRV-Pool and the required Active Directory Groups including local permissions.

2.2 Configuring a Windows user to logon to the SQL Server

The logon to the SQL server can be done using either a SQL user account or using a Windows user account which has the right to authenticate at the SQL Server.

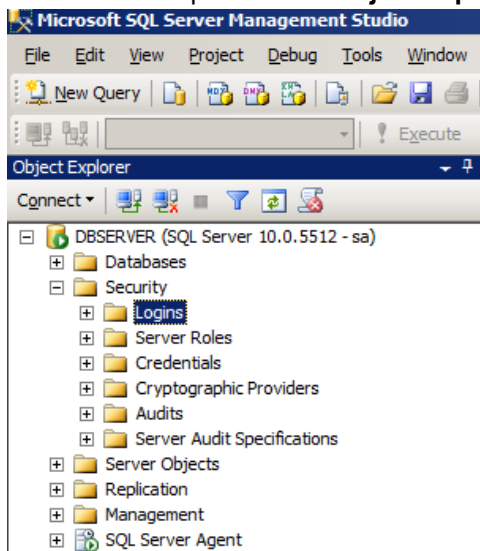
If you want to use a SQL user account to authenticate to the database this section can be skipped.

Note: Due to security reasons we recommend using Windows authentication to access the SafeGuard database.

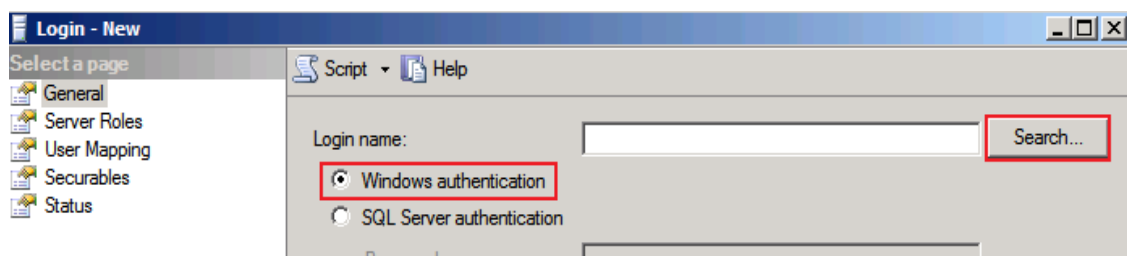
Please follow the steps below:

1. Create a new user account in Windows if no existing user should be used. In this example we are using a new user account named SGNSQL.
2. Open the **SQL Server Management Studio**.

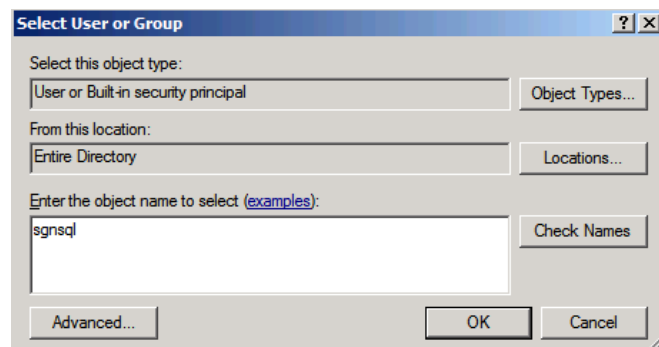
- In the left hand pane of the **Object Explorer** section browse to *Security > Logins*.



- Right click on *Logins > New Login...*
- Select *Windows authentication* (default) and then *Search...*



- Search the user that should be used for authentication – in this case *SGNSQL > Click OK*.



- The user logon name is displayed now in the initial dialog > press **OK** to complete the user creation. Further actions are not required at this point.

Please consider:

Every user that should be able to use the SafeGuard Management Center must have a valid SQL User account when using Windows authentication to connect to the SafeGuard database.

2.3 Creating the SafeGuard Database

The creation of the SafeGuard Database can be done either by using the available SQL scripts which can be found on the product CD or by running the SafeGuard Management Center configuration wizard.

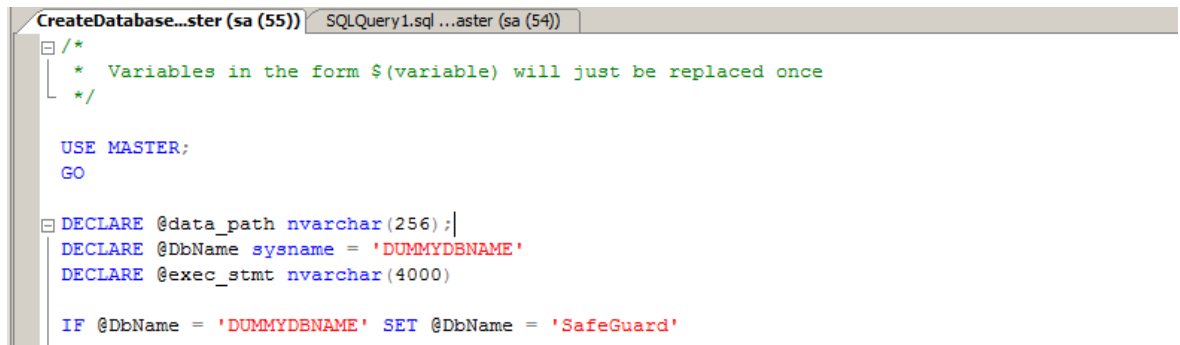
This chapter describes the creation of the database using the SQL scripts.

If you want to use the Management Center configuration wizard to create the database this step can be skipped.

The required steps to create the SafeGuard Database are:

1. Copy the script CreateDatabase.sql and CreateTables.sql from the SafeGuard Enterprise product delivery to the SQL server.
2. Double click the CreateDatabase.sql script. The **SQL Server Management Studio** will open.

Log on using a user that is allowed to create a database (the newly created user does not have the right by default! In this case do not use the SGNSQL user.)



```

CreateDatabase...ster (sa (55))  SQLQuery1.sql...aster (sa (54))
/*
 * Variables in the form $(variable) will just be replaced once
 */

USE MASTER;
GO

DECLARE @data_path nvarchar(256);
DECLARE @dbName sysname = 'DUMMYDBNAME'
DECLARE @exec_stmt nvarchar(4000)

IF @dbName = 'DUMMYDBNAME' SET @dbName = 'SafeGuard'

```

3. Execute the script either by pressing the relevant GUI button or by using the F5 hot key.
4. Another window pane below the script area opens. The screen output should be *Command(s) completed successfully.*
5. Now double click on the CreateTables.sql script.
6. Another tab opens in the **SQL Server Management Studio**.
7. Add the following line at the top of the script area:
use safeguard

```

Microsoft SQL Server Management Studio
File Edit View Query Debug Tools Window Community Help
New Query
master Execute
CreateTables.sql...ster (sa (52))* CreateDatabas...ster (sa (51))
use SafeGuard
CREATE TABLE [DBO].[POLICY] (

```

8. Execute the script.

9. Another window pane below the script area opens. The screen output should be *Command(s) completed successfully.*

The SafeGuard Enterprise Database is now created successfully. At the moment only user 'sa' and the Administrative account created during the SQL Server installation can be used to access the database.

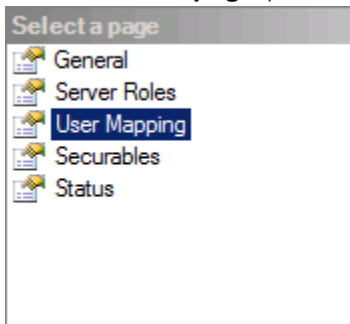
2.4 Changing access permissions for the SafeGuard Database

The last step is enabling the user account to access the SafeGuard Database. Therefore the user account must be granted access to the database. These access rights are required for all Security Officers who work with the SafeGuard Management Center when Windows NT authentication is used.

As it is possible to assign different roles and permissions to a user on a database only the minimum required ones are described.

Please follow these steps:

1. Open the **SQL Server Management Studio**.
2. In the **Object Explorer** section in the left hand pane browse *Security > Logins*.
3. Select the user that should be enabled (in this example SGNSQL).
4. Right click on the user name > *Properties*.
5. A new **Login Properties** window opens.
6. Under **Select a page** (left hand side) select *User Mapping*.



7. On the right hand side check the *Map* box for the SafeGuard database.

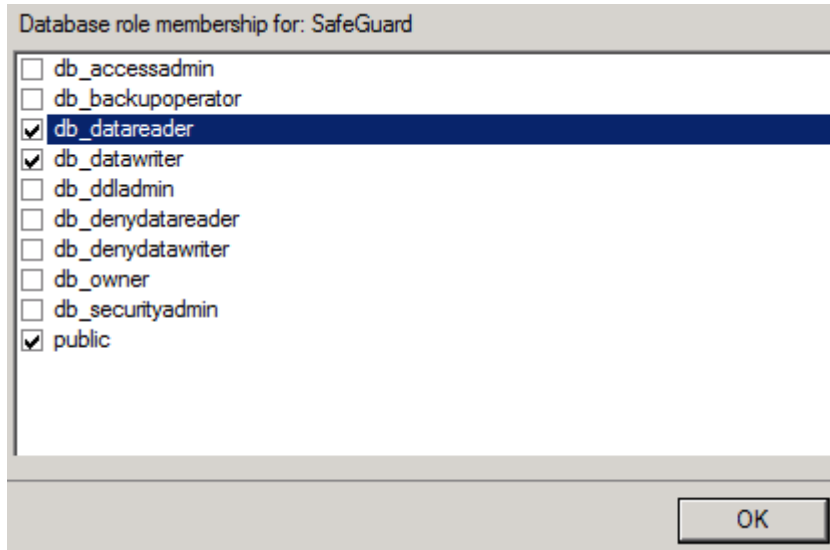
Users mapped to this login:			
Map	Database	User	Default Schema
<input type="checkbox"/>	master		
<input type="checkbox"/>	model		
<input type="checkbox"/>	msdb		
<input checked="" type="checkbox"/>	SafeGuard	TESTDOMAIN\sgnsql	
<input type="checkbox"/>	tempdb		

8. Below this the **Database role membership for:** section can now be edited. Select the following roles for the user:

db_datareader

db_datawriter

public



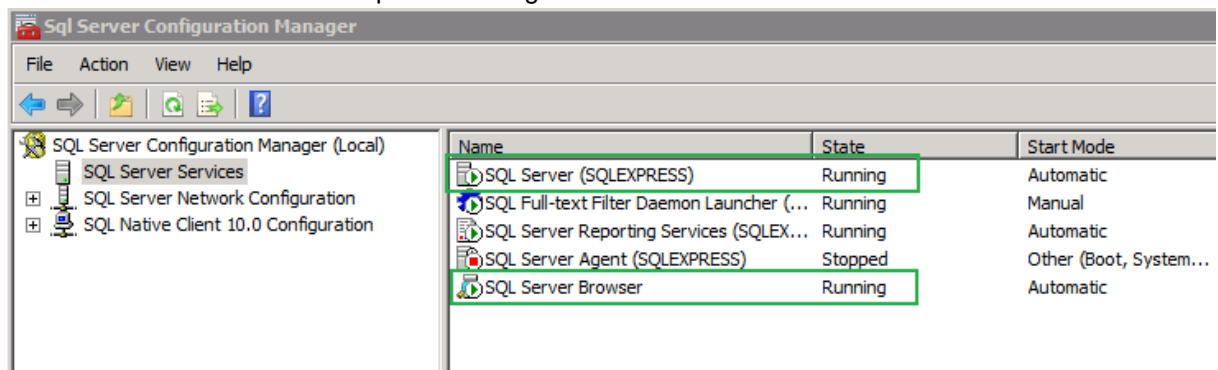
9. Confirm the configuration using the **OK** button.

2.5 Checking the SQL Server Service Settings and the Named Pipes Configuration

In order to install the SafeGuard Management Center it is required that the SQL Browser Service is running and that “Named Pipes” “TCP/IP connection” is activated. These settings are required to access the SQL server from other machines. Further information can be found in the Microsoft Knowledge Base.

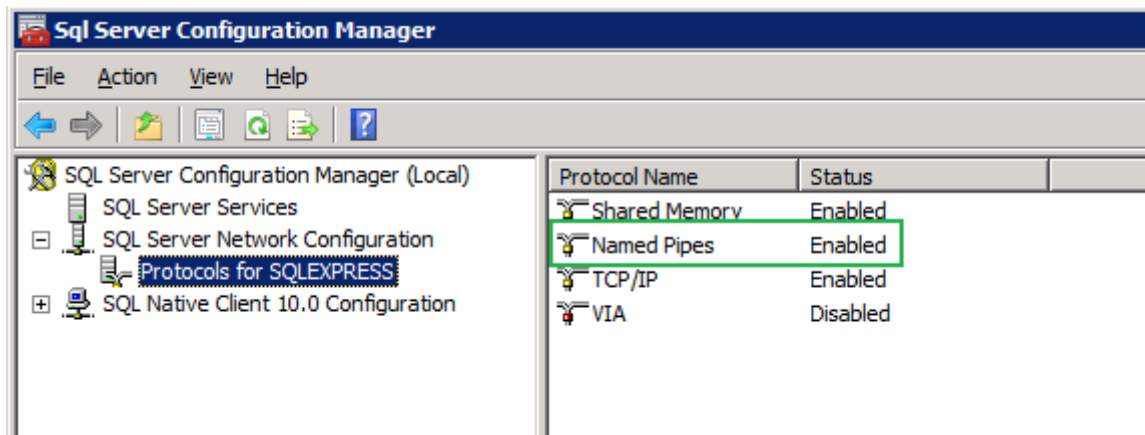
This can be checked in the **SQL Server Configuration Manager**. The check is done in two steps:

1. When opening the **SQL Server Configuration Manager** select *SQL Server Services* in the left hand pane and check in the right hand pane if the **SQL Server** and the **SQL Server Browser** service are both up and running.



Note: It might also be necessary to check the **Start Mode** of each service!

2. Expand the *SQL Server Network Configuration* node in the left hand pane and select the current instance – in this example *Protocols for SQLEXPRESS*. Verify that Named Pipes are enabled.



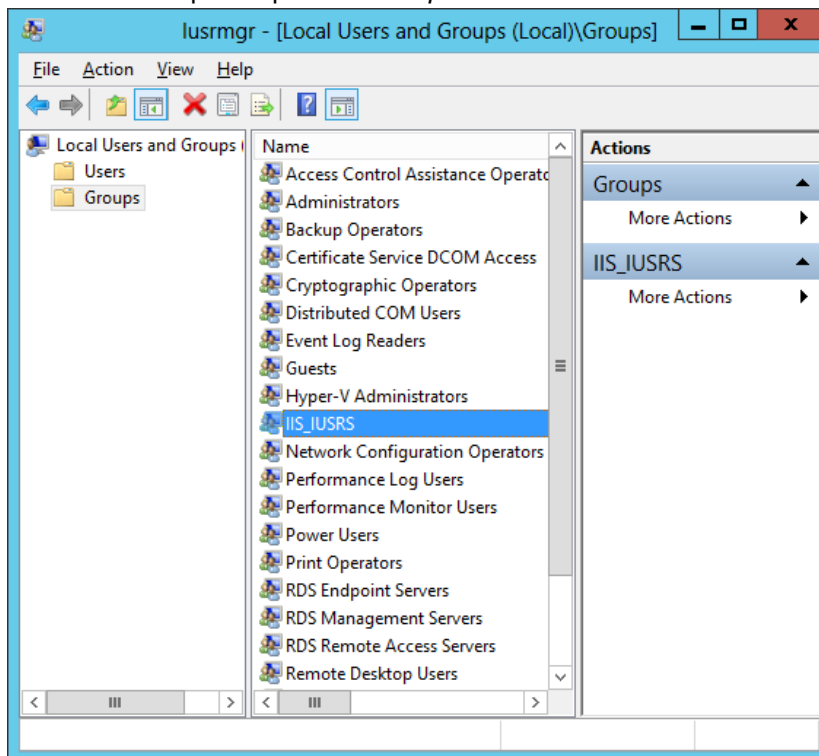
3. Restart the SQL services.

2.6 Adding the SQL user to the SGNSRV-Pool and to the required Active Directory user groups including local permissions

To allow the communication between the SafeGuard Enterprise Server and the SafeGuard Database using Windows NT authentication, additional steps are required. The SQL user account must be configured for the **Application Pool** of the IIS, local file permissions must be adjusted and the user must be made a member of certain groups on the IIS Server.

Adding the user to the required groups

1. On the IIS Server open the user/group management (**Run** > *lusrmgr.msc*).
2. In the left hand pane open the *Groups* folder.

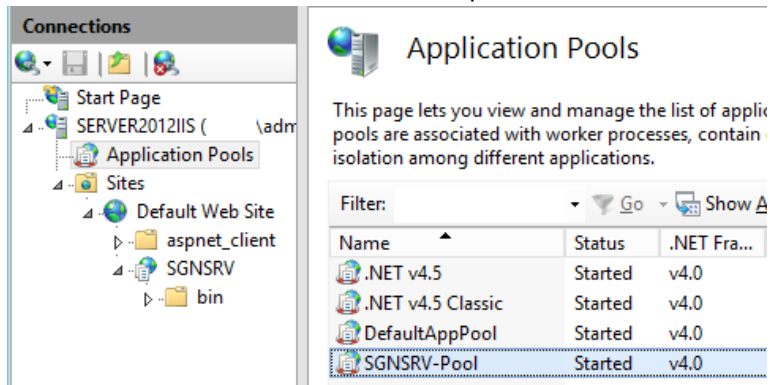


3. Add the newly created user (SGNSQL) to the following three groups:
 - a. IIS_IUSRS
 - b. Performance Log Users
 - c. Performance Monitor Users
4. Close the snap in.

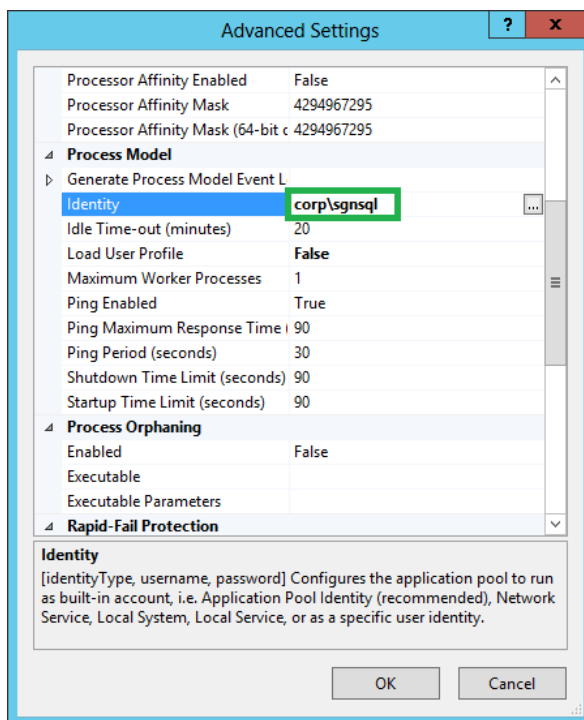
Please Note: Alternatively the user account can be added to the respective AD groups.

Adding the user to the default application pool

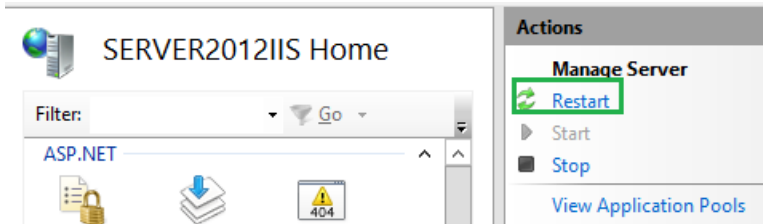
1. Open the Internet Information Service manager.
2. Browse to **Application Pools** in the left-hand pane.
3. Select the SGNSRV-Pool in the center pane window.



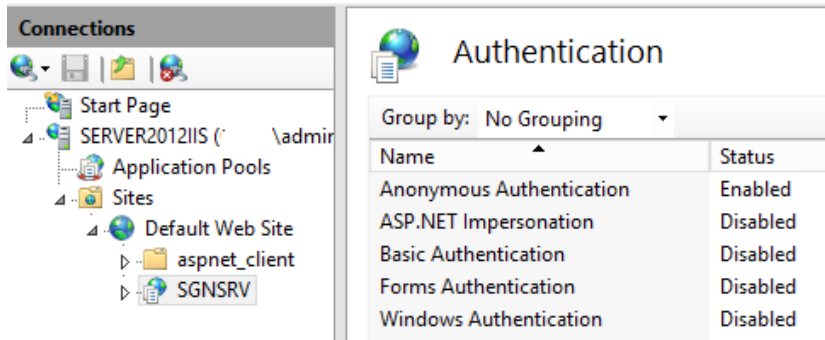
4. Click on the Right-hand pane **Actions** > **Edit Application Pool** > **Advanced Settings ...**
5. Switch to **Process Model** > **Identity** > Change the user name > *Custom Account* > *Set* > Enter the user name and the password of the SQL enabled user like Domain\User.



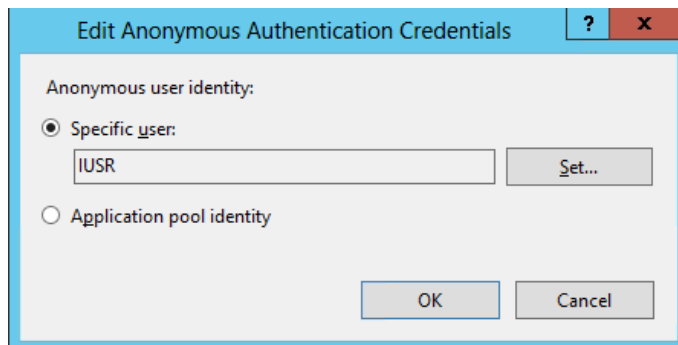
- Click on the server name in the left hand pane >in the right-hand pane under **Actions** click on **Restart**.



- In the left hand side under *Sites* select **SGNSRV**.
- In the center pane double click **Authentication**.



- Right click **Anonymous authentication** > **Edit**.
- Verify that the **Anonymous user identity:** is set to **Specific user:** and that the user name is **IUSR**.



The configuration of the SafeGuard Enterprise Server is now completed. The installation of the SafeGuard Management Center can now be done.

3. Installing the SafeGuard Management Center

When the SafeGuard Enterprise Server is installed and the SafeGuard Database is configured, the next step is installing the SafeGuard Management Center. The SafeGuard Management Center can be installed on different Client and Server operating systems. A list of the currently supported operating systems can be found in the release notes.

This document describes the installation of the SafeGuard Management Center on Server 2012.

3.1 Quick installation reference

1. Install the SafeGuard Management Center.
2. Run the SafeGuard Management Center configuration wizard.
3. Create a directory connection and import the Active Directory.
4. Import the license file.

3.2 Installing the SafeGuard Management Center

In order to install the SafeGuard Management Center please follow these steps

1. Copy the **SGNManagementCenter.msi** from the product CD or any network location to the machine that should run the Management Center.
2. In addition, the installation requires that the Microsoft SQL Server 2012 Native Client (**sqlncli.msi**) and the Microsoft SQL Server 2012 Command Line Utilities (**SqlCmdLnUtils.msi**) which are available in the 3rd party folder of the product delivery are installed.
3. Run the msi package as Administrator.
4. Proceed with the installation wizard.
 - a. Accept the legal disclaimer.
 - b. Select the modules to be installed > if the "multi tenancy" mode (required to manage more than one SafeGuard Database) is not required, select *Typical* as installation type.

3.3 Running the SafeGuard Management Center Wizard

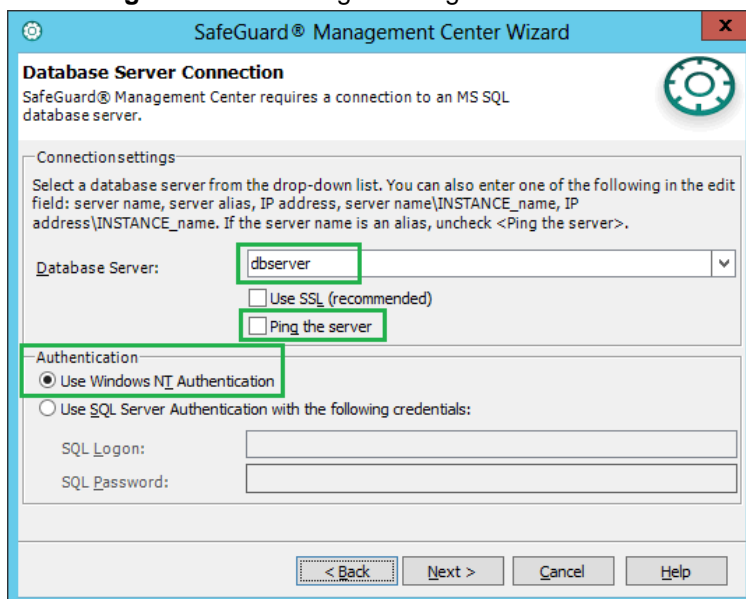
To complete the installation, the next step is to run the **SafeGuard Management Center Wizard**. The wizard is used to configure the connection to the SafeGuard Database and to create the company certificate and MSO.

The required configuration steps are:

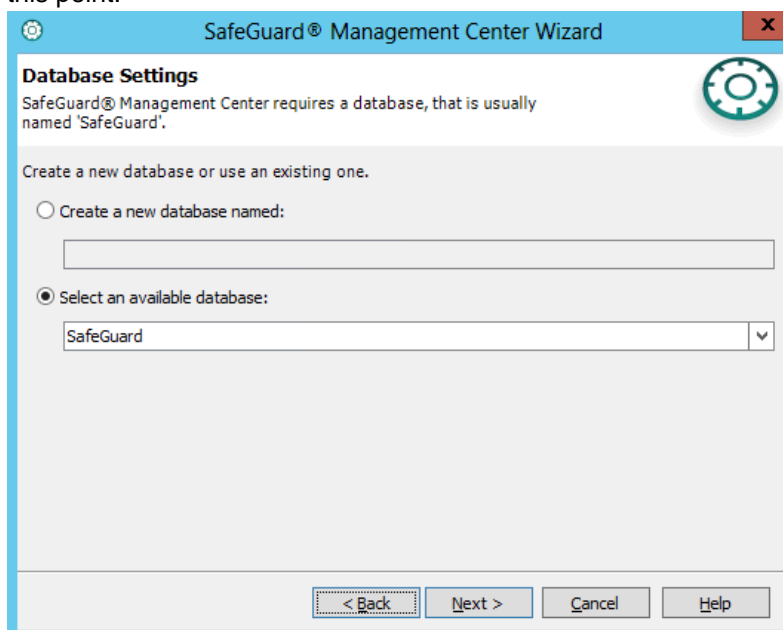
1. Open **SafeGuard Management Center**
2. The SafeGuard Management Center Wizard starts.
Note: After completing the wizard this link will start the **SafeGuard Management Center**. The wizard will not come up again as soon as the configuration is completed.

3. On the Database Server Connection page connect to the database server. These settings will be used in the SafeGuard Management Center afterwards.
 - a. Uncheck the **Ping Server** box.
 - b. Under **Authentication > Use Windows NT Authentication**.
 - c. Select the SQL server instance using the drop down field. When using SQL Express the instance name would be `SQLEXPRESS`.

Note: In case the drop down field is empty enter the server name manually like `Machine Name\Instance Name`. This information is available in the **SQL Server Management Studio** logon dialog under **Server name:** when starting the application.

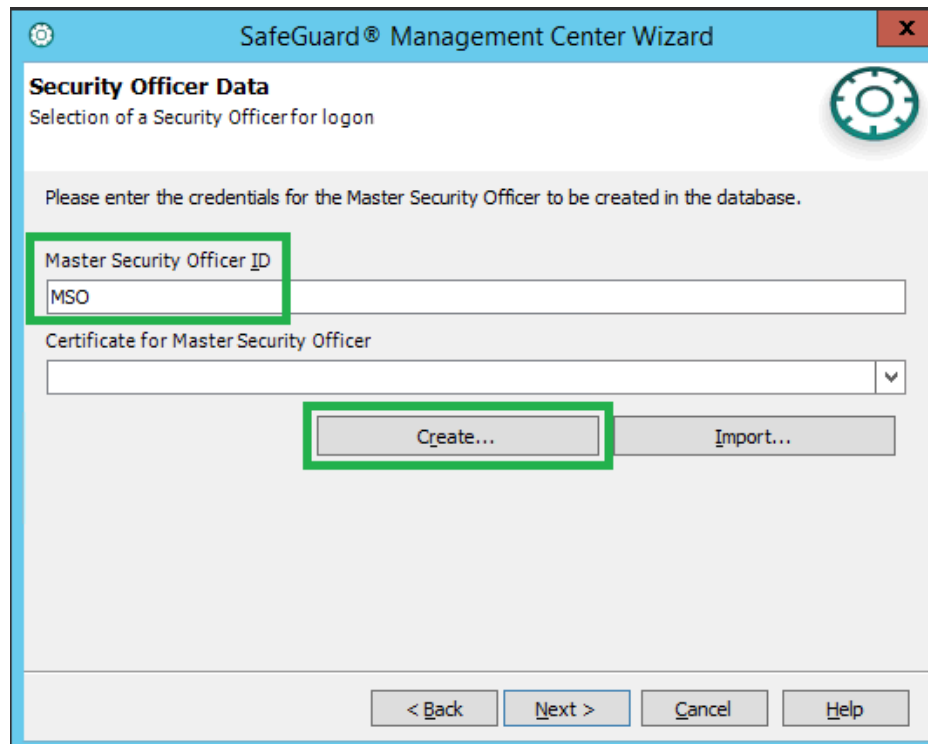


4. On the Database Settings page it is possible to either create a new database or using an existing one. Since the database was pre-created using the SQL scripts, the wizard will automatically select the already existing database. No further configuration is required at this point.



Note: If the database was not created beforehand, select **Create a new database named:** to create a new database using this wizard. In this case the user that was used to log on to the database on the page before must have the right to create a new database on the SQL server! This step is not required when following this document!

5. The next step is the creation of a Master Security Officer and a personal SafeGuard Enterprise certificate store for the Windows user. This is done in multiple steps:
 - a. Define the ID of the Master Security Officer. The ID can be chosen as desired – a possible name would be *MSO* since this is common terminology when talking about SafeGuard Enterprise master security officers.
 - b. After that select the token logon mode – we recommend **not** selecting **Mandatory**.
 - c. Complete this step by clicking **Create...**



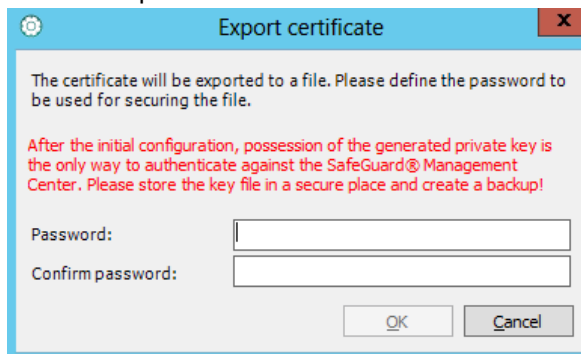
- d. Then create the password for the personal certificate store. The SafeGuard Enterprise Certificate store is a virtual store to store SafeGuard Enterprise certificates. This store is not related to Microsoft functionality!

Please note:

The password which is defined in this step is the password that is used to log on to the Management Center afterwards. This is not the password to import the MSO certificate in case of restoring the SafeGuard Management Center again! This example uses 123456 as password.



- e. As soon as the password for the certificate store is defined, a new dialog is displayed to define the certificate password. This is the password which is required to import the certificate again in case the SafeGuard Management Center has to be restored, the SafeGuard Database has to be restored or the MSO should be used on a second Management Center on a different machine. This example uses 654321 as password.



Note:

A **Save As...** dialog box is displayed. Save the .cer and the .p12 file at a secure place where it cannot be deleted. In case the .cer and the .p12 file are not available a recovery of the SafeGuard Database will not be possible!

- As soon as the security officer certificate is exported, the certificate store and the security officer are created the wizard proceeds with the creation of the company certificate. At this point it is possible to either import an existing company certificate from an already existing SafeGuard Enterprise installation or to create a new company certificate. Since this is a fresh installation select **Create a new company certificate** and enter the company name into the field. In this example the name would be *My company Ltd.*

Company Certificate
Create or restore the global certificate for your company

Create a new company certificate
Please enter the name of your company. The company name will be used as the applicant for the company certificate. The name is also used to distinguish between several SafeGuard(r) Enterprise installations.

My company Ltd.

Restore using an existing company certificate

Subject:

Serial number:

Expiry date: Import...

Hash algorithm (for generated user and company certificates): SHA-256

Use SHA-1 for SafeGuard Enterprise clients on Windows XP, Vista or Windows 7 (without SP1).

< Back Next > Cancel Help

Important hint (regarding Hash algorithm):

Because of the now (as of version 6.10) used SHA-256 algorithm for certificate signing, introduced to increase the level of security, you have to consider the interoperability with older SGN Clients:

When only new SGN 6.10 or 7.0 clients will be used, you can leave the default value "SHA-256". If you need to use older SGN clients, e.g. because of running clients with Windows XP/Vista or the SafeGuard Configuration Protection Module, you have to create the company certificate by changing the Hash algorithm setting to SHA-1. It is not possible to switch from SHA-256 to SHA-1 after the creation of the company certificate.

This completes the configuration of the **SafeGuard Management Center**. Exiting the wizard will automatically start the **SafeGuard Management Center**.

3.4 Importing the Active Directory into SafeGuard Enterprise (optional)

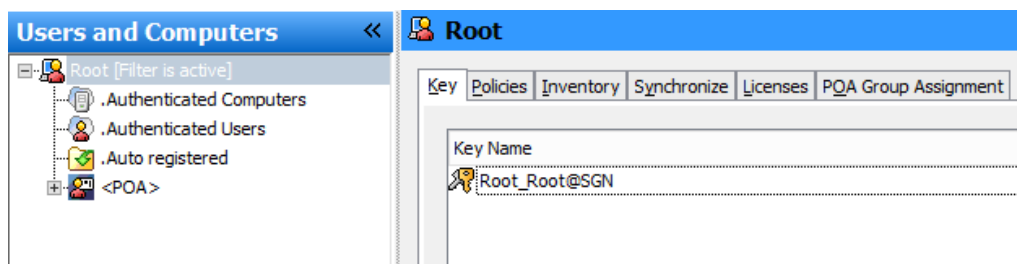
SafeGuard Enterprise offers the possibility to import the Active Directory structure into the SafeGuard Management Center. During the synchronization with the Active Directory objects such as computers, users and groups are imported to the SafeGuard Management Center. All data is stored within the SafeGuard Database.

If you do not have an Active Directory or the directory should not be imported it is also possible to use the **Autoregistration** feature of SafeGuard Enterprise. Please read the SafeGuard Enterprise Administrator Help for further information.

In this example we import the AD structure which is the most common scenario.

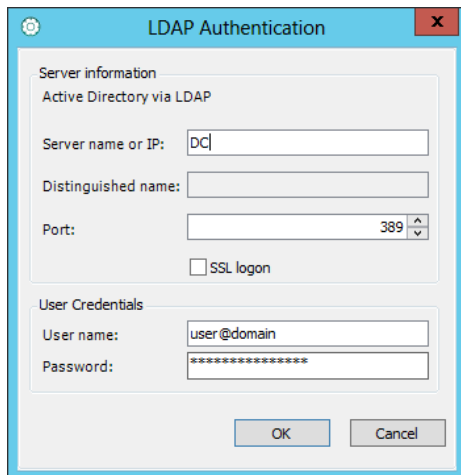
The Active Directory import can be configured as follows:

1. Open the **SafeGuard Management Center**.
2. Authenticate using the password which was defined for the certificate store (in this example 123456).
3. The SafeGuard Management Center opens.
4. In the lower left-hand pane select **Users and Computers**. After that select **Root [Filter is active]** in the top left window.



5. In the right hand pane select the **Synchronize** tab.

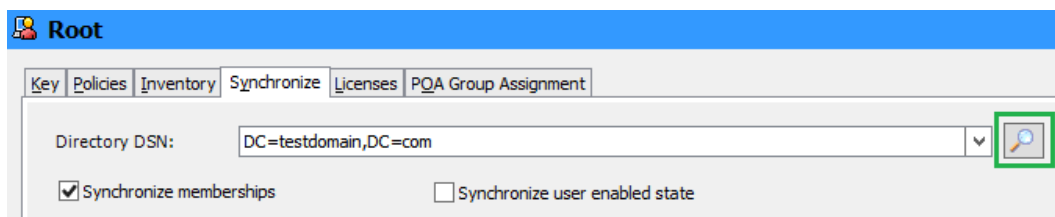
- The **LDAP Authentication** wizard starts automatically. Within this wizard the communication details to import the Active Directory into SafeGuard Enterprise are defined. Enter the logon credentials which should be used to synchronize the Active Directory and specify the server name or the IP address of the **Domain controller!** **Important:** The user name should be in the format User@Domain to avoid issues resolving the domain Netbios name.



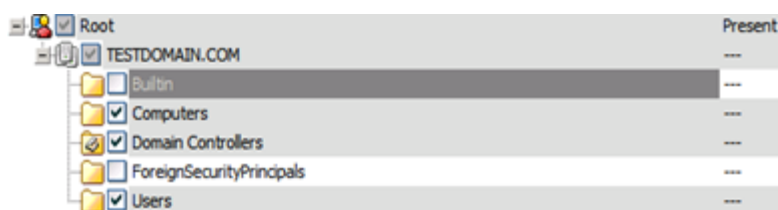
Note: The synchronization will be done in the context of the user defined in this wizard! Therefore, it is required that the user has sufficient rights on the Active Directory objects that should be imported. However, the user can be a normal AD user and does not have to be member of the administrative group. The SafeGuard Enterprise synchronization will only read information and not modify the Active Directory at any time!

After submitting the data by clicking OK a positive result should be displayed on the screen.

- As soon as the directory connection is successfully established the **Directory DSN** field shows the domain information. Click the magnifier symbol in order to list the Active Directory – depending on the number of objects the reading of the Active Directory information might take a while.



As soon as the reading process has completed, the domain structure is displayed in the center pane. Select the organizational units that should be imported into SafeGuard Enterprise by clicking the referencing check boxes. It is not possible to select single machines, groups or user objects only. However, it is possible to select organizational units only.



Now decide if Active Directory group memberships should be synchronized with the SafeGuard Management Center. The import of group memberships can be skipped by unchecking the **Synchronize memberships** box. Not importing and synchronizing group memberships has a positive impact on the performance of the Management Center (especially in large AD structures).

Note: By default SafeGuard Enterprise creates a key for every Container, Organizational Unit (OU) and domain object that is imported. The creation of keys can be quite time consuming and resource allocating. As a result of this we recommend (especially when importing large environments) not to enable the key creation for groups if not required.

8. Start the synchronization by clicking **Synchronize**. The detailed information from the Active Directory will now be read.
9. At the end of the synchronization a summary with all changes is shown.

By clicking **OK** all changes are written into the SafeGuard Enterprise Database.
10. As soon as this is completed the domain structure is displayed in the left-hand pane.
11. The import of the Active Directory in the SafeGuard Management Center is now completed.

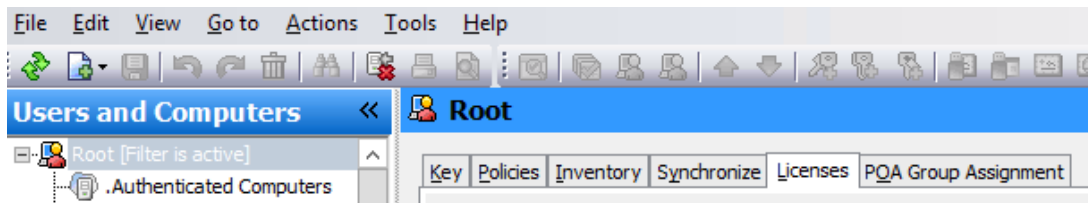
3.5 Importing the license file

SafeGuard Enterprise has an integrated license counter. By default a fixed number of 5 licenses for every available module is part of the installation. This allows the evaluation of other SafeGuard modules easily without any side effects. However, when purchasing SafeGuard Enterprise you receive a personalized license file for your company which needs to be imported into the SafeGuard Management Center.

Note: Further information regarding the licensing model of SafeGuard Enterprise can be found in the SafeGuard Enterprise Administrator Help or via the sales department.

Importing the license file is very easy. The required steps are:

1. Save the license file (the XML file) on a local hard drive so that it can be reached from a machine that has the SafeGuard Management Center installed.
2. In the SafeGuard Management Center click on **Root** in the left hand pane and then on the **Licenses** tab on the right hand side.



3. The license overview will be displayed showing 5 licenses for every module. In the lower left corner of the center pane press the **Import license file...** button.

License issued to: **Sophos SafeGuard® Evaluation License**
 Issued on: **8/19/2013**

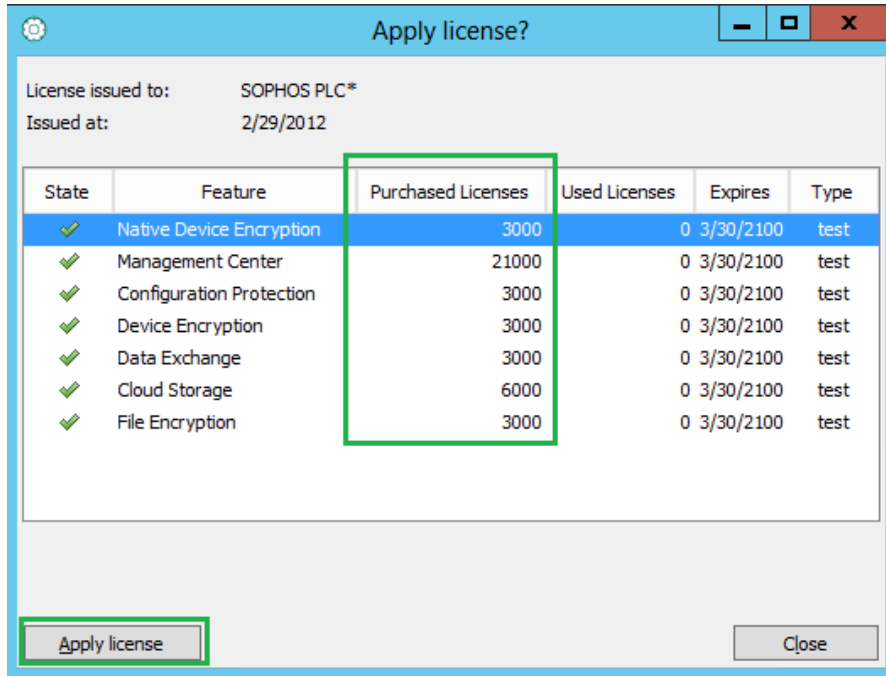
State	Feature	Purchased Licenses	Used Licenses	Expires	Type
✓	Data Exchange	5	0	3/31/2016	regular
✓	Native Device Encryption	5	0	3/31/2016	regular
✓	Configuration Protection	5	0	3/31/2016	regular
✓	Device Encryption	5	0	3/31/2016	regular
✓	File Encryption	5	0	3/31/2016	regular
✓	Management Center	5	0	3/31/2016	regular
✓	Cloud Storage	5	0	3/31/2016	regular

Licensed token modules: AET SafeSign Identity Client, Charismathics Smart Security Interface, ActivIdentity ActivClient, ActivIdentity ActivClient (PIV), Aladdin eToken PKI Client, a.sign Client, Estonian ID-Card, Gemalto Access Client, Gemalto Classic ClientSiemens, Gemalto .NET Card, IT Solution trustWare CSP+, RSA Authentication Client, RSA Smart Card Middleware 3.x, Siemens CardOS API, T-Systems NetKey 3.0, Unizeto proCertum

Your license is valid.

Import license file... Recount used licenses

4. An open file dialog is displayed. Browse to the license xml file and click **Open**.
5. The **Apply license?** dialog is displayed. Validate that the number of licenses matches the purchase order and check that the company name is ok. To complete this step, click **Apply license**.



6. After that, the center frame should show the correct license information.

The installation of the SafeGuard Management Center is now completed. The next step is to complete the installation of the SafeGuard Enterprise Server.

4. Installing the SafeGuard Enterprise Server configuration package

At the moment the SafeGuard Enterprise server is installed. However, no communication information to connect to the SafeGuard database is available.

Communication information (between the IIS server, the database, the SafeGuard client and the IIS server) gets configured by installing the so-called configuration packages. These configuration packages are created in the SafeGuard Management Center.

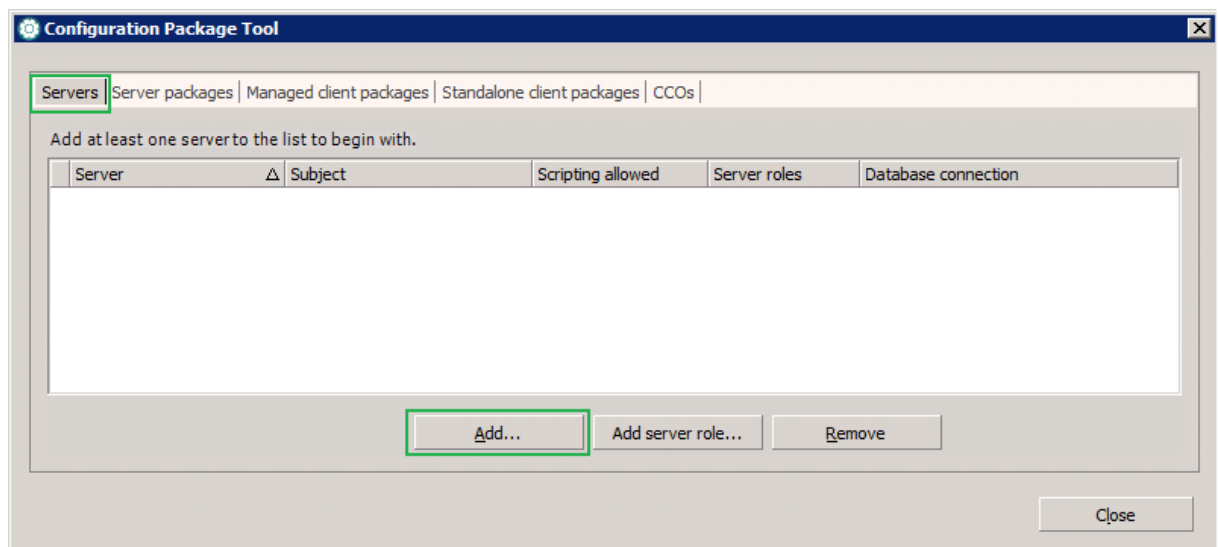
4.1 Quick installation reference

1. Create the server configuration package.
2. Install the server configuration package on the SafeGuard Enterprise Server.
3. Run the invoke test.

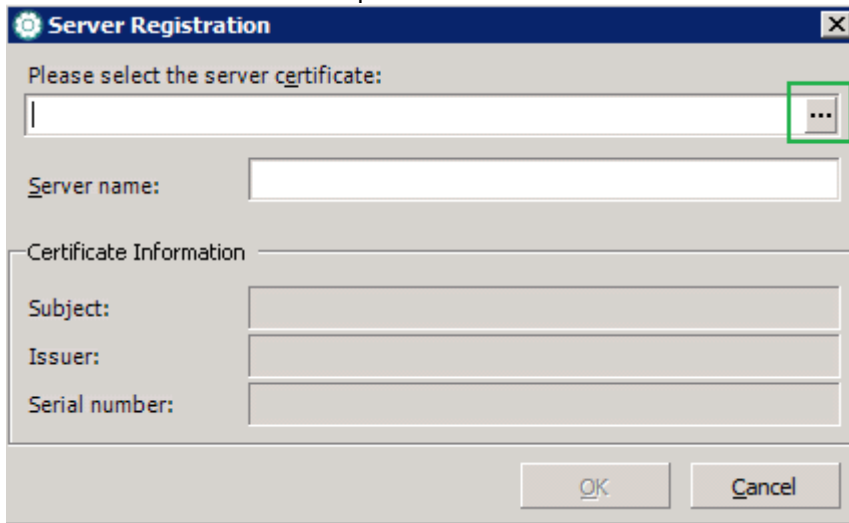
4.2 Creating the SafeGuard Enterprise Server configuration package

To complete the installation of the SafeGuard Enterprise Server it is necessary to create a new **server configuration package**. In order to create this file, follow these steps in the SafeGuard Management Center:

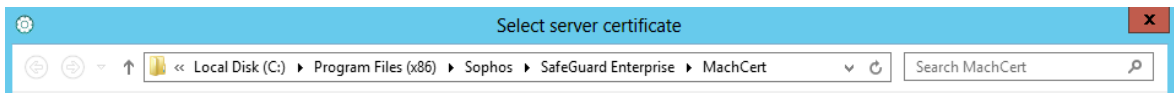
1. Open **SafeGuard Management Center**.
2. **Tools > Configuration Package Tool > Servers** tab.
3. Click **Add...**



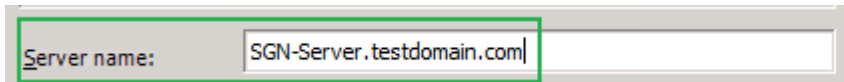
- In the next window browse the SafeGuard Enterprise server certificate which can be found under *C:\Program Files (x86)\Sophos\SafeGuard Enterprise\MachCert* on the **IIS server** that runs the SafeGuard Enterprise Server.



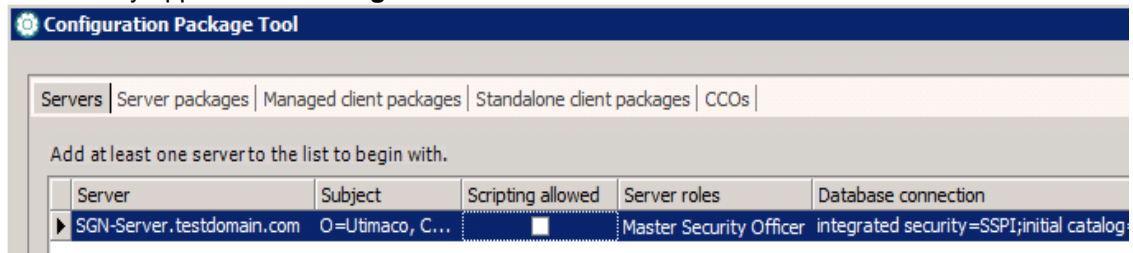
Path of the Server Certificate:



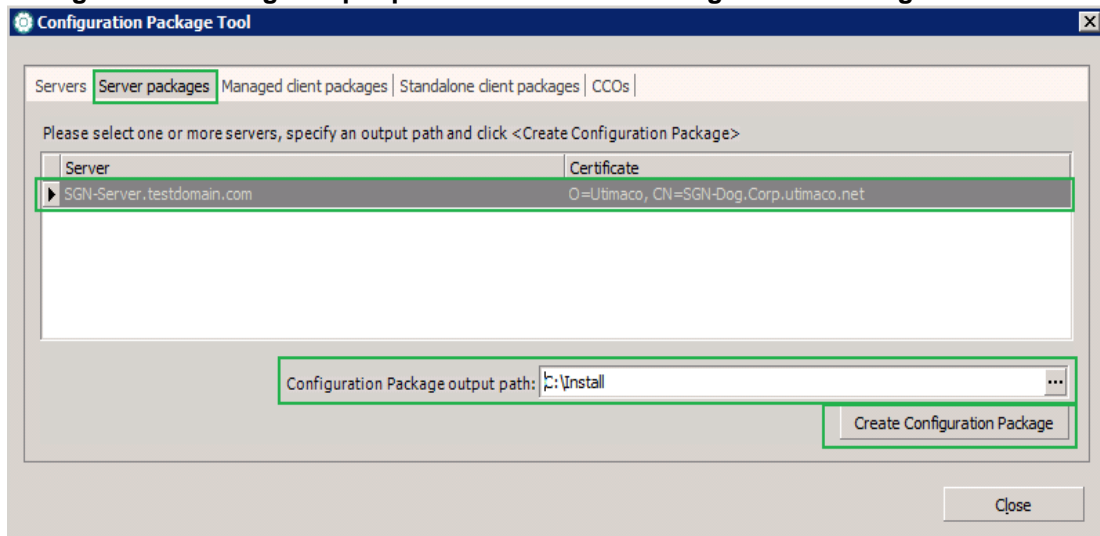
As soon as the certificate is imported the FQDN Name of the SafeGuard Enterprise Server is displayed in the server name field.



- A new entry appears on the **Register Server** tab.



- Switch to the **Server packages** tab. Select the server entry from the list. Define the **Configuration Package output path**. Click **Create Configuration Package**.



The output name of the file will be *[Server FQDN Name.msi]*.

- Copy the newly created server configuration package to the IIS machine that runs the SafeGuard Enterprise Server.

4.3 Installing the SafeGuard Enterprise Server configuration package

- Switch to the machine that runs the SafeGuard Enterprise Server.
- Copy the server configuration package to the server.
- Run the MSI package by double-clicking it.
- Accept all defaults in the installation wizard.
- The package does not need a reboot but restarting the IIS afterwards is recommended.

The installation of the SafeGuard Enterprise Server is now completed. The next step is to verify that everything is working as expected.

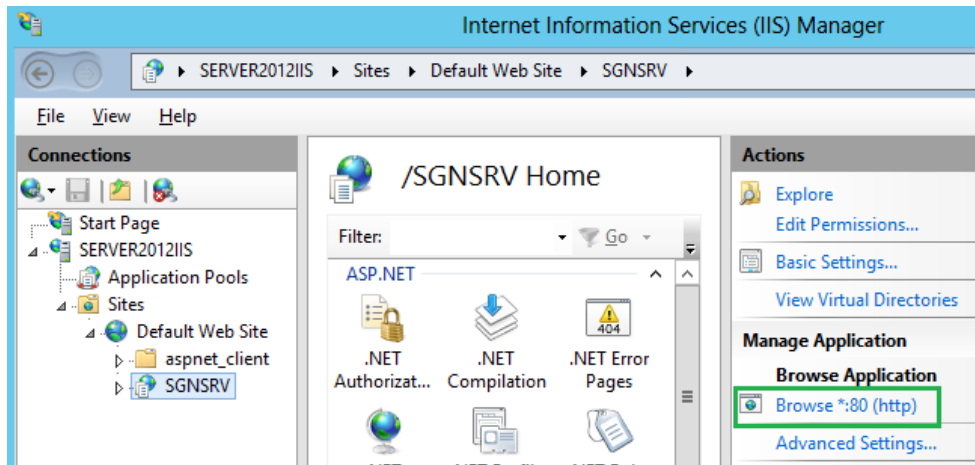
4.4 Running the invoke test

SafeGuard Enterprise offers a possibility to check if the SafeGuard Enterprise Server is correctly configured and working.

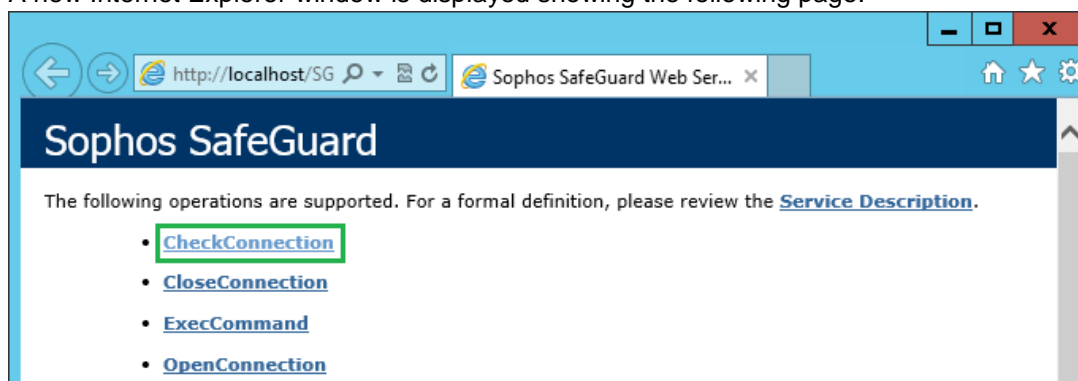
Note: Whenever changing something in the back-end such as logon data to the SQL server we recommend running an invoke test to double-check that the communication between the SafeGuard Enterprise server and the database is still working. The same applies to any changes to the **IUSR** under Windows.

The invoke test is part of the SafeGuard Enterprise web page SGNSRV. To run the test follow these steps:

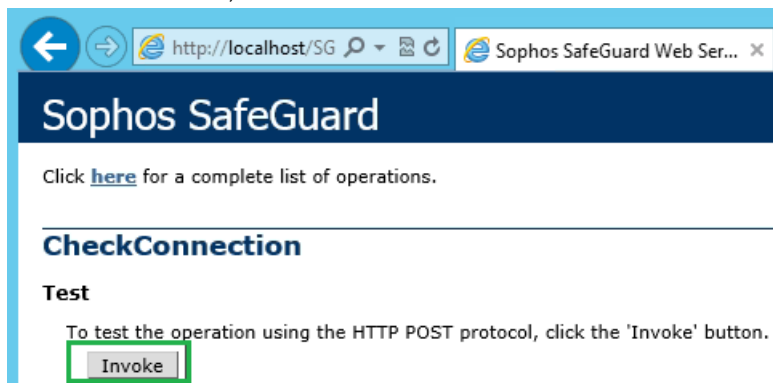
1. Open the **Internet Information Services Manager** (*run > inetmgr.exe*) and browse to the **SGNSRV** web page. In the right hand pane click on **Browse *:80 (http)** in the **Manage Application** section.



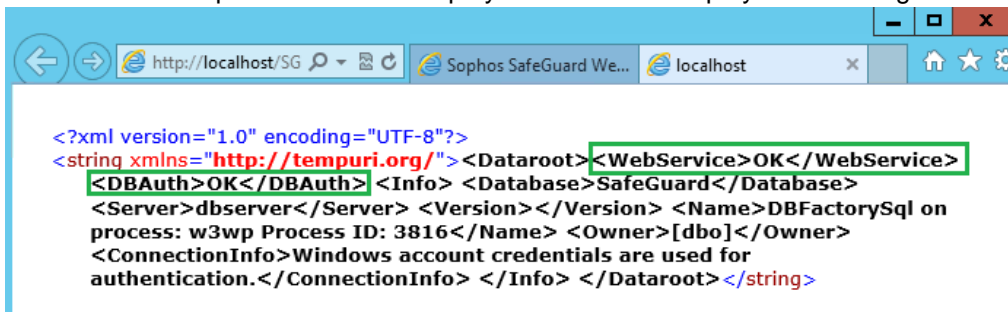
A new Internet Explorer window is displayed showing the following page:



2. Click **Check Connection**.
3. In the next window, click **Invoke**.



A new Internet Explorer window is displayed and should display the following result:



5. Configuring the SGNSRV web page to use SSL transport encryption

The data transfer between SafeGuard clients and the SafeGuard Server can be encrypted using either the Sophos encryption or SSL. Sophos recommends using SSL (default as of SGN 6.10) as it has huge performance benefits (especially in environments with more than 100 clients).

Please Note: If you want to manage OSX Clients, SSL transport encryption is a requirement.

■ Using SSL

The following steps describe how to implement SSL to secure the communication between the SafeGuard Client and the SafeGuard Server.

The main advantage of using SSL is the performance win compared to the integrated encryption. Using SSL is approximately 40% faster and can furthermore parallelize connections to multiple threads and CPU's.

Setting up SSL encryption to secure the communication requires a valid certificate. The following certificate types can be used in order to secure the communication:

1. A self- signed certificate
2. Certificate issued by a PKI having a private or a public root certificate

This document describes the installation procedure using a self-signed certificate.

Important note: In case only a certificate created by a public PKI and no PKI infrastructure is available it is not possible to use this certificate to secure the communication with SSL.

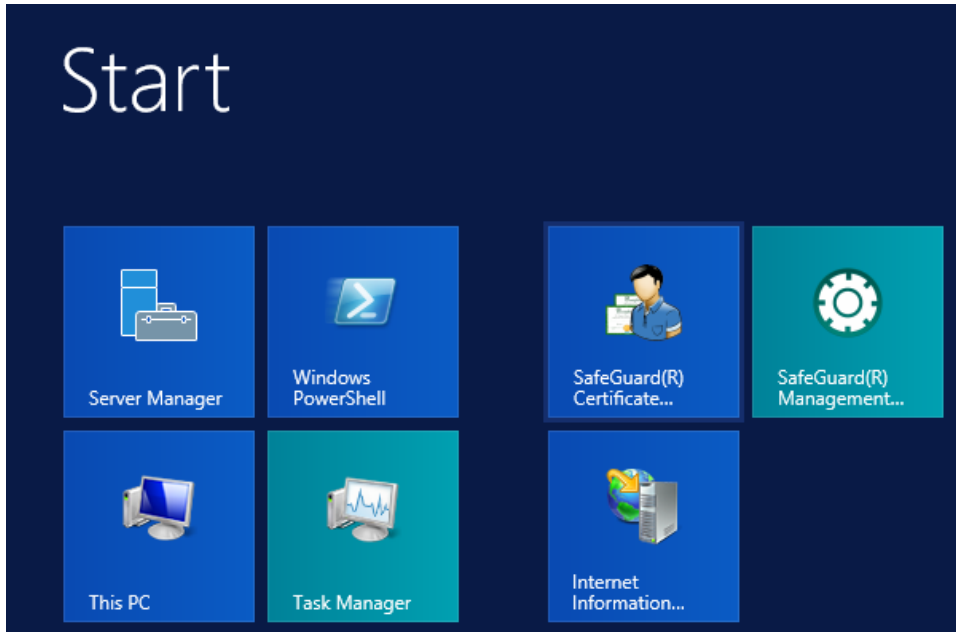
5.1 Quick installation reference

1. Create a new self-signed certificate.
2. Configure the SGNSRV web page to accept a certificate.
3. Deploy the certificate.

5.2 Creating a self-signed certificate

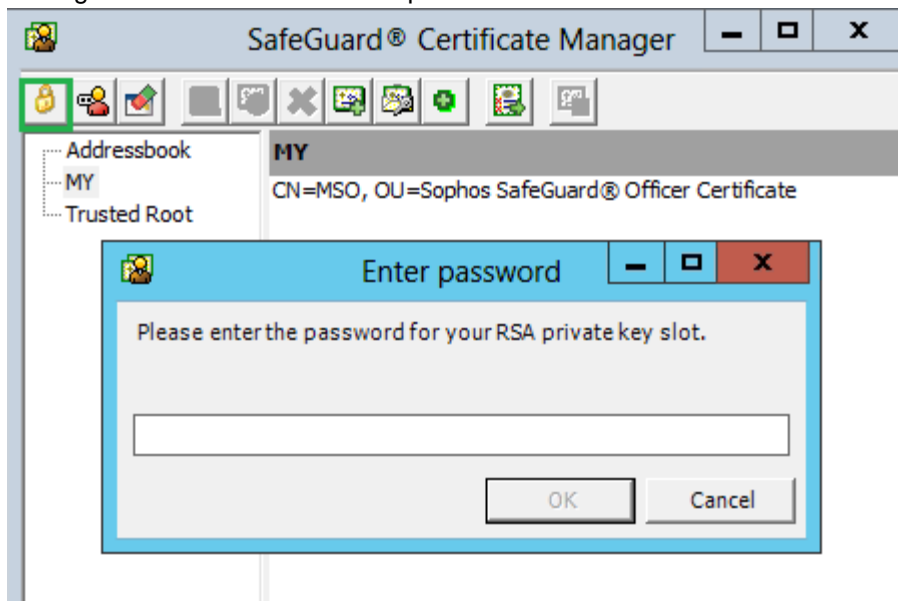
To create a self- signed certificate using SafeGuard Enterprise please follow these steps:

1. Open the SafeGuard Certificate Manager (which is installed on the same machine as the SafeGuard Management Center) **Start > SafeGuard Certificate Manager**.



2. **Enter the password for the certificate store.**

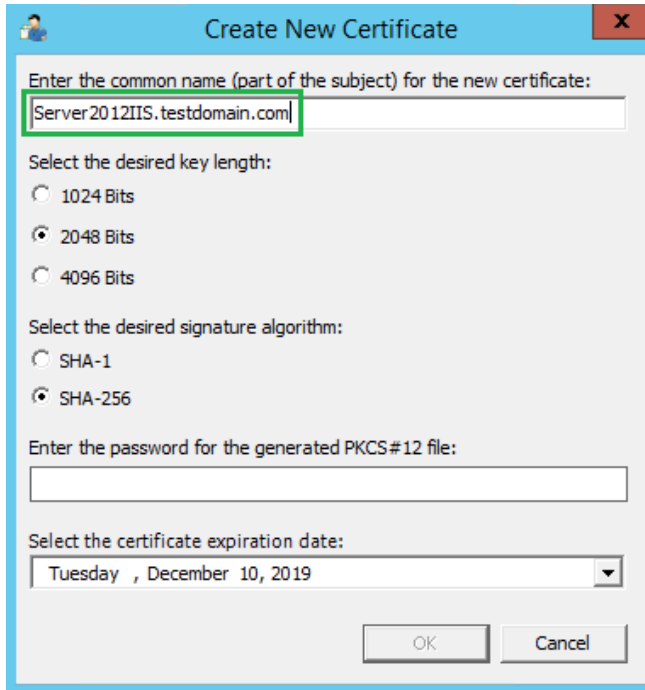
To authenticate use the same password that is used to log on to the SafeGuard Management Center: in this example it would be 123456.



3. Create a new certificate. The name of the certificate must be the FQDN name of the IIS Server.

In this case the certificate's name would be "Server2012IIS.testdomain.com" as the name of the machine is "Server2012IIS" and the name of the domain is "testdomain.com".

The key length of the certificate remains on the default value. The password can be set just as desired.



4. After pressing **OK** save the cert and the .p12 file to a destination that can be reached from the machine which hosts the IIS.

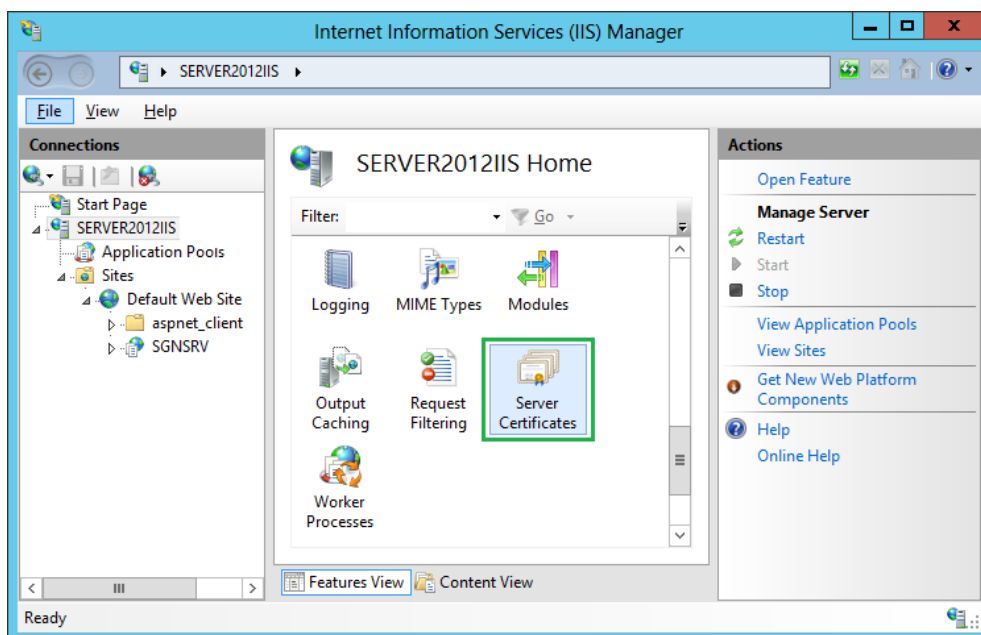
Note:

If you're using a PKI please create a certificate for the machine that is running the SafeGuard Enterprise Server. The certificate's name must be identical to the identity that is shown in the Internet Information Service (IIS) Manager top node. Besides this the certificate must be issued to the machine using the FQDN name of this machine.

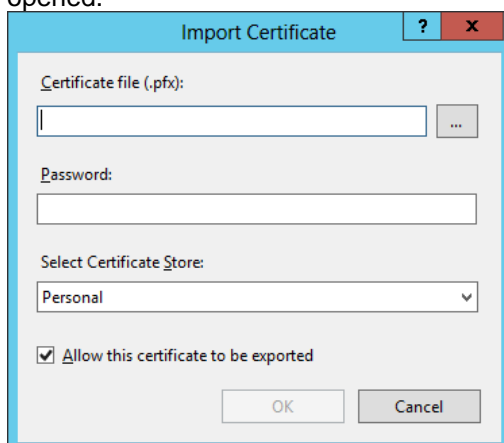
5.3 Configuring the SGNSRV web page to accept certificates

As soon as a valid certificate in order to use SSL is available, it is possible to configure the SGNSRV web page to accept a certificate secured connection. To do so, follow these steps:

1. Open the Internet Information Services (IIS) Manager.
2. Click on the server name.
3. From the center menu, double-click the "Server Certificates" button in the "IIS" section center pane.



4. From the **Actions** menu (on the right), select **Import**. The **Import Certificate** wizard is opened.

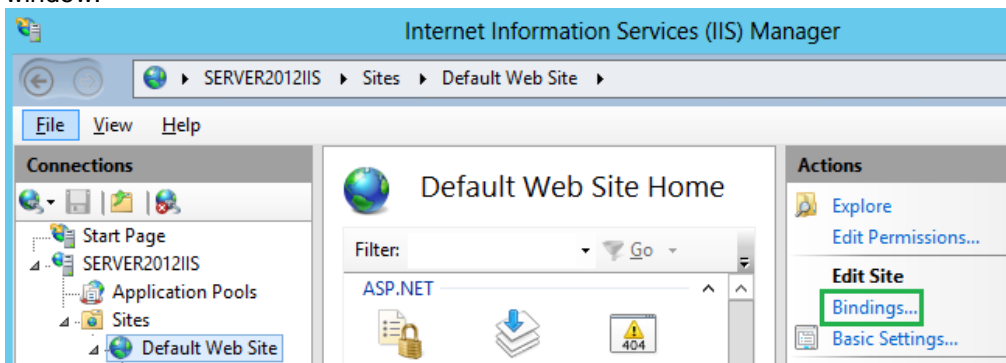


5. In the open dialog change the file extension to *.* and browse to the location where the .p12 and the .cer file are stored. Select the p12 file that was created before. In case that file extensions are disabled please select the file with the description *Personal information Exchange*

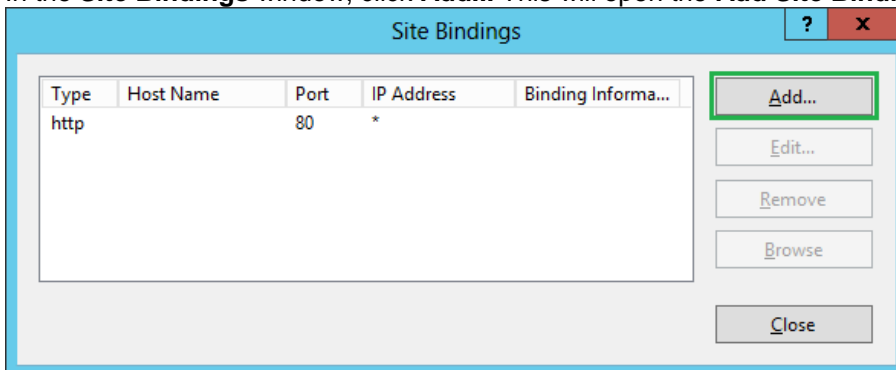
- Once the certificate has been installed successfully on the server, you will need to assign that certificate to the appropriate website using IIS.

From the **Connections** pane on the left-hand side in the main Internet Information Services (IIS) Manager window, select the name of the server on which the certificate was installed.

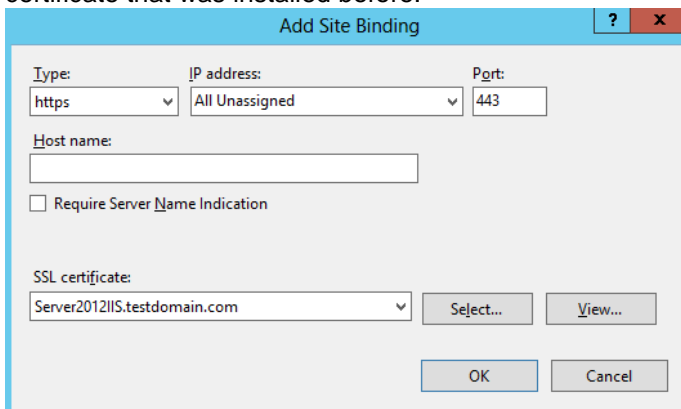
- Under **Sites**, select the site to be secured with SSL.
- From the **Actions** menu (on the right), select **Bindings**. This will open the **Site Bindings** window.



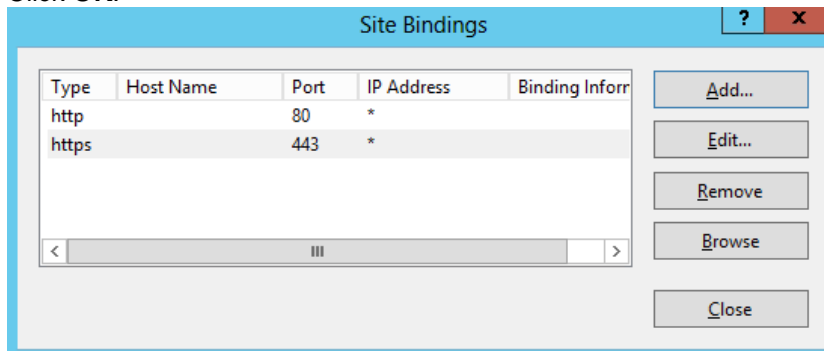
- In the **Site Bindings** window, click **Add...** This will open the **Add Site Binding** window.



- Under **Type** choose **https**. The IP address should be **All Unassigned**, and the **Port** over which traffic will be secured by SSL is **443**. The **SSL certificate** field should specify the certificate that was installed before.



11. Click **OK**.



The certificate is now installed and the website configured to accept secure connections. **Please Note:** Traffic via port 443 needs to be allowed in the firewall configuration of your network.

5.4 Deploying the certificate to the clients

To complete the SSL configuration, you need to deploy the certificate to the SafeGuard Enterprise Clients as well

There are multiple ways of assigning a certificate to a client. One way of doing the assignment, is using a Microsoft Group Policy. This is the way that will be described here. In case a different way of distribution should be used, please ensure that the certificate is stored in the Computer Certificate Store.

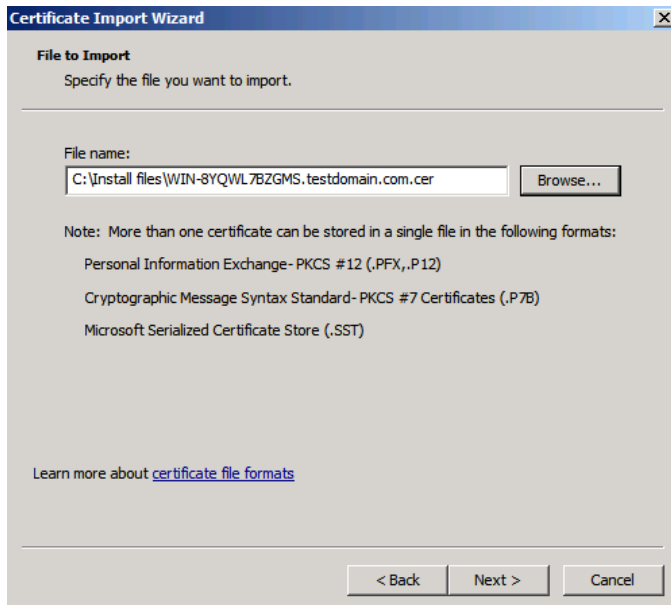
To assign the certificate to the client using the Active Directory group policy mechanism perform the following steps.

Note: Ensure that the policy with the certificate deployment reaches all machines that should be installed with SafeGuard Enterprise especially if these objects are not centrally stored in one single OU.

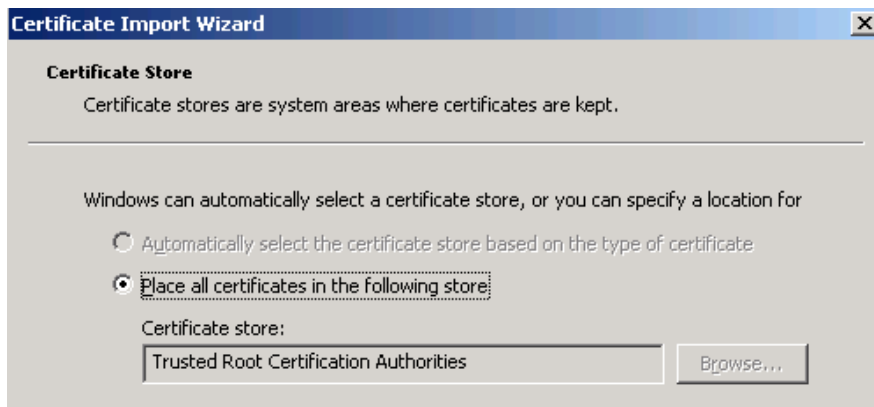
The detailed steps are:

1. Open the Group Policy Management console (*Gpeditmc.msc*).
2. Create a new group policy object.
3. Open the new GPO and browse to **Computer Configuration > Windows settings > Security. Settings > Public Key Policies > Trusted Root Certification Authorities**.
4. Right-click in the right-hand pane window and click **Import**.

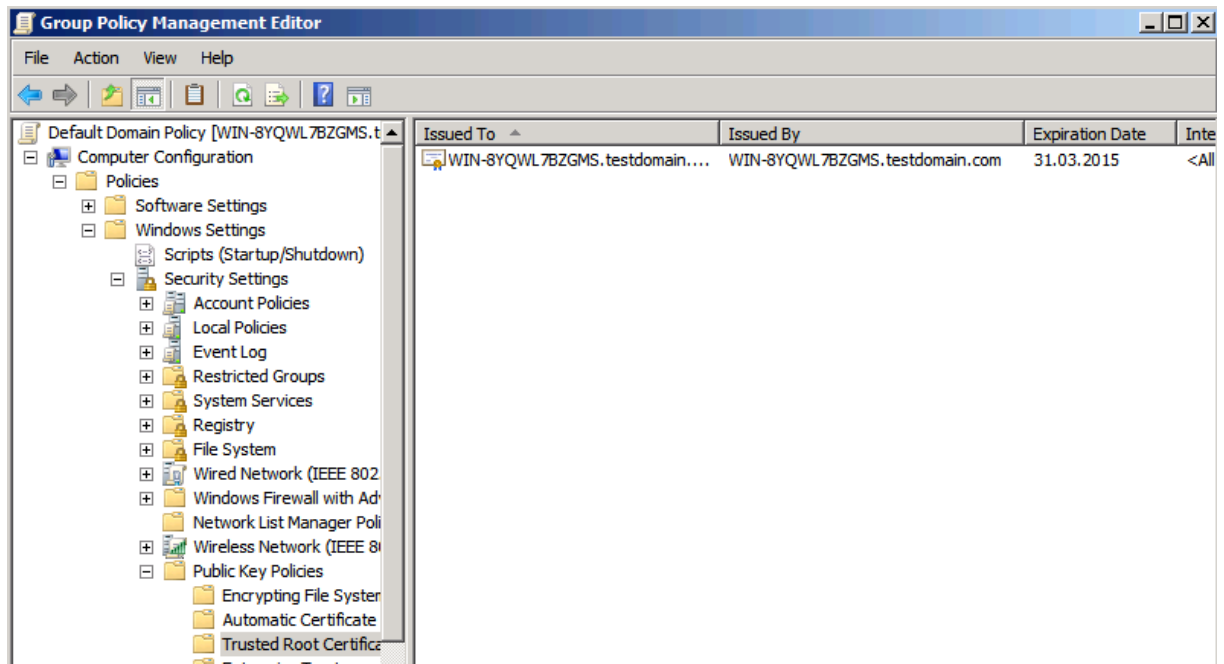
5. Browse to the .cer file which was created to secure the communication and select it.



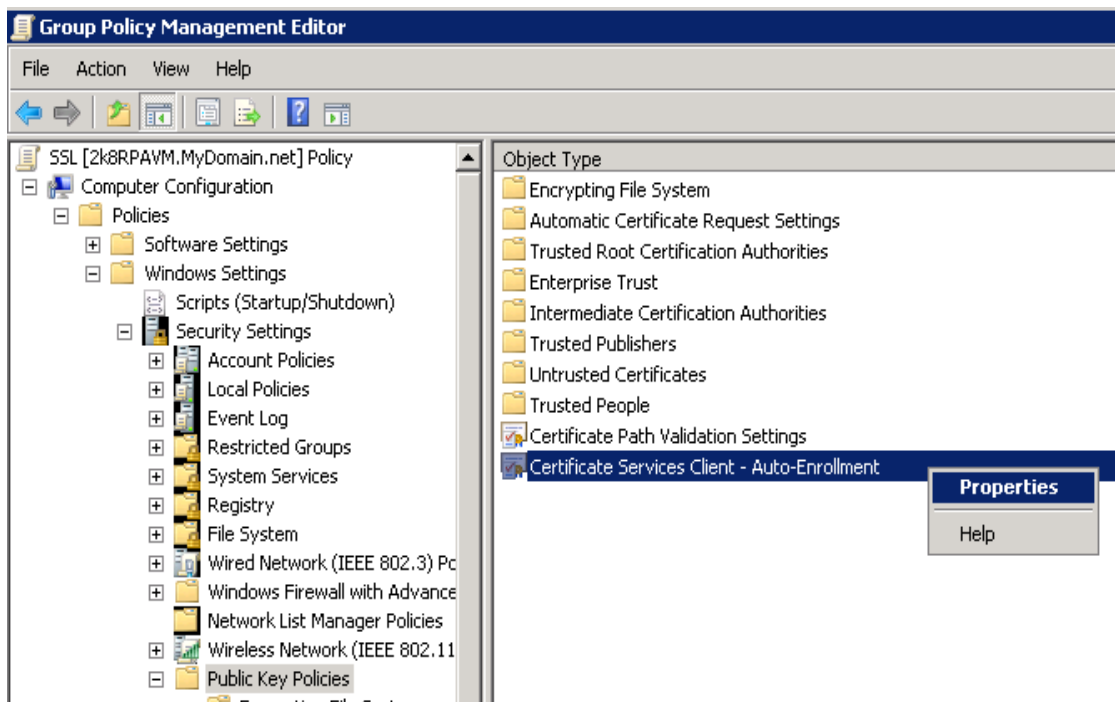
6. By default the certificate will be located in the correct Certificate store on the client.



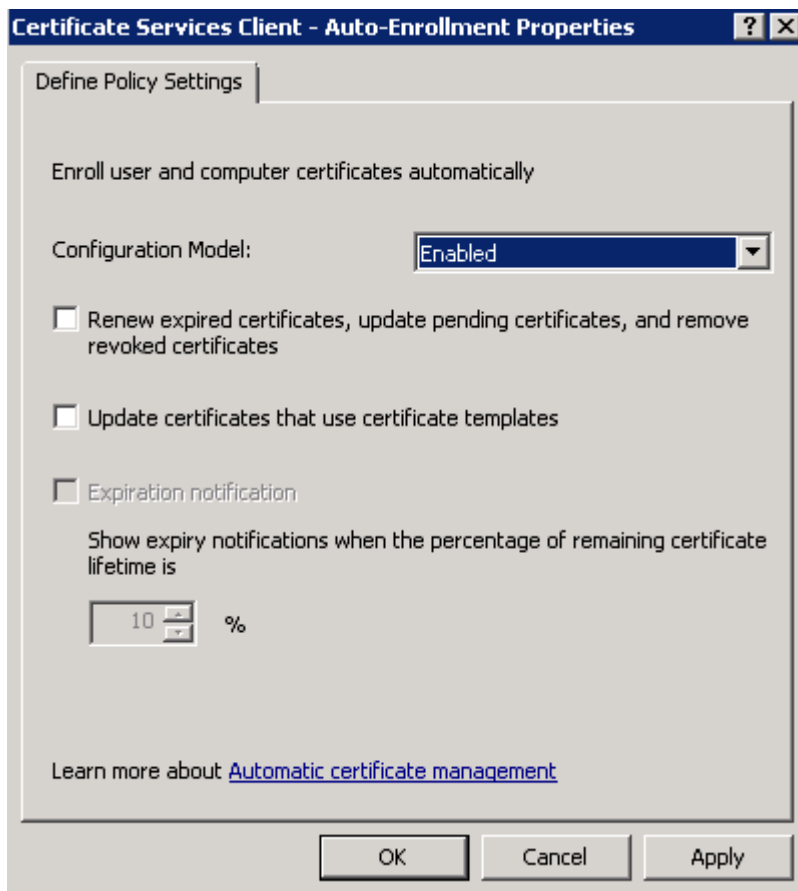
7. Having completed this successfully the GPO will look like this:



8. Browse back to the **Public Key Policies** node. Right-click on **Certificate Services Client - Auto-Enrollment** in the right-hand pane and select **Properties**.



9. Activate the automatic enrollment of certificates. This will ensure that every client receives the required policy.



10. Apply the changes and close the snap-in.

The configuration of the SafeGuard Enterprise back-end is now completed!

The next step is to proceed with the installation of the client.

6. Installing the SafeGuard Enterprise Client on Windows

As soon as the back-end is running the deployment and installation of the SafeGuard Enterprise Clients can begin.

There are some things that should be considered such as preparation tasks prior to the installation. Although these steps are only optional we recommend following these steps to ensure a smooth implementation.

The SafeGuard Enterprise Client can be installed on different kinds of hardware and on different operating systems. A list of all supported operating systems and the minimum system requirements can be found in the *Release Notes* which are available for each SafeGuard Enterprise version in the Sophos Knowledge Database.

Besides this there is a list of hardware which has been tested successfully or which is already known to need a POA hot key to function properly. Further details about SafeGuard Enterprise POA hot keys can be found in the Sophos knowledge base under <http://www.sophos.com/support/> please use *SGN POA hot key* or *SGN hardware* as search expression. Reading these articles is recommended before starting the installation of the SafeGuard client.

This example uses a Windows 8 (64 bit) machine to demonstrate the installation.

6.1 Quick installation reference

1. Check that the certificate has reached the client.
2. Prepare the operating system using *chkdsk /f /v /x* and *defrag*.
3. Install the SafeGuard Client package including the latest hardware compatibility file (POACFG).
4. Create a new client configuration package.
5. Install the client configuration package.
6. First reboot and user initialization.

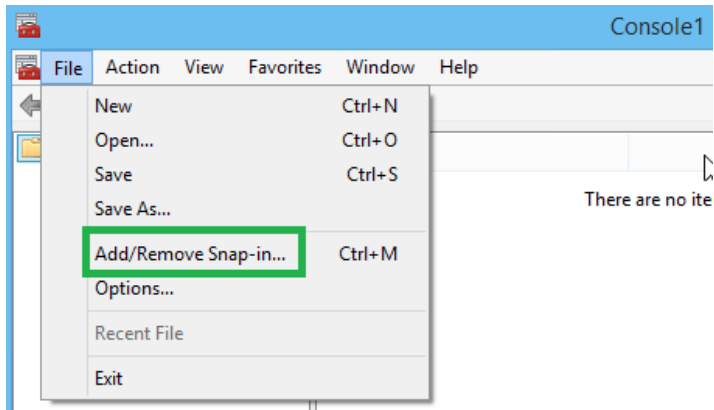
6.2 Checking the availability of the SSL certificate on the client

To check if the certificate was distributed correctly please take these actions.

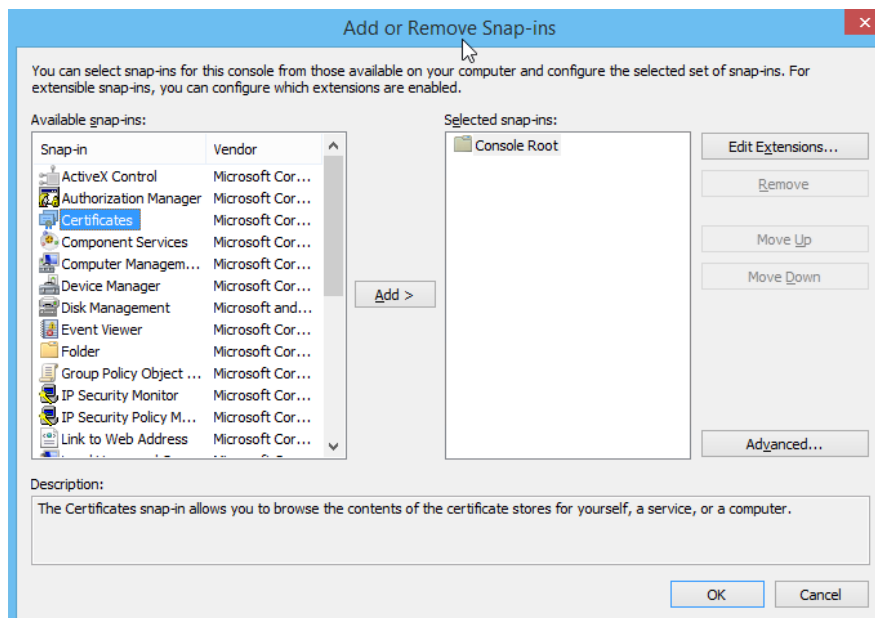
The certificate must be assigned to the computer and not to the user. The **certificate file** must be available in the Certificate Store of Microsoft under **Trusted Root Certification Authorities** (if a PKI is running this is not required).

To do so follow these steps on the client:

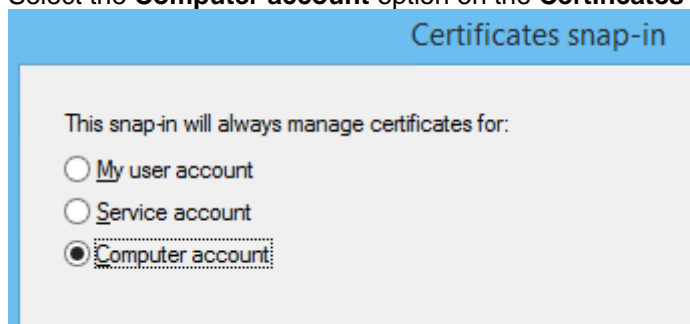
1. Log on to the machine using an administrative account.
2. Click **Run > mmc**.
3. In the **Console1** window, click the **File** menu and then click the **Add/Remove Snap-in** command.



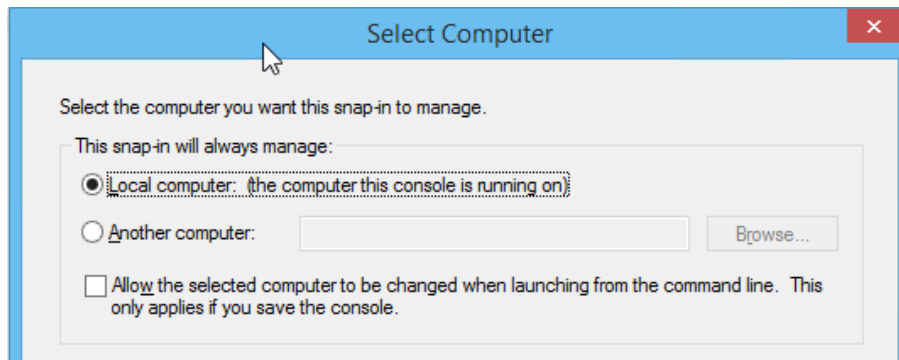
4. In the **Add/Remove Snap-in** dialog box select **Certificates** in the left hand pane and click the *Add* button in the center afterwards.



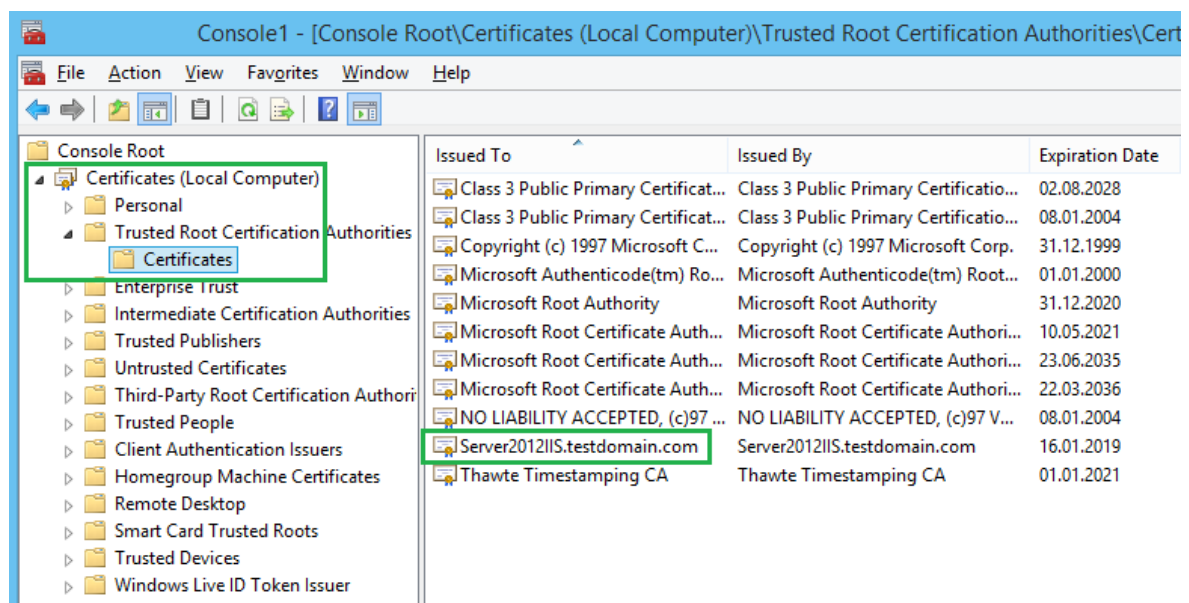
5. Select the **Computer account** option on the **Certificates snap-in** page.



6. Select **Local computer: (the computer this console is running on)** on the **Select Computer** page. Click **Finish**.



7. Click **OK** in the **Add Standalone Snap-in** dialog box.
8. In the left pane click **Console Root > Certificates (Local Computer) > Trusted Root Certification Authorities > Certificates**.
9. Check in the right hand pane if the certificate which was created before is available in the store.



If the certificate appears this step is completed.

Note: If the certificate does not appear take these steps:

- a. `run > gpupdate /force >` a Windows command box is displayed.
- b. Wait until the box has closed and perform the above steps again starting at 1.

6.3 Preparing the client for installation

Even if it is possible to start the client installation without checking the system in any way it is highly recommended to perform these steps prior to the installation.

The main preparation points are:

- Before installing SafeGuard Enterprise, always back up your data completely.
- Use CHKDSK to check the hard disks for errors (further information can be found in the Knowledge Base searching for 107799). It is not recommended to install SafeGuard Enterprise on a faulty HDD.

Note: When running `chkdsk /f /v /x` on your system a reboot will be required. Do not start the SafeGuard Enterprise installation without completing this reboot!

- If you are using a 3rd-party boot manager, consider re-installing the system without the boot manager.
- If an imaging tool was used to install the operating system, it is recommended to "re-write" the master boot record (MBR).
- 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. If the system was not changed this step can be skipped.
- Defragment the harddrive – further information regarding this can be found in <http://www.sophos.com/support/knowledgebase/article/109226.html> - How and why to use "defrag" within Windows (not applicable on SSD drives)

6.4 Installing the SGNClient_x64.msi and the SGxClientPreinstall.msi

The client installation is divided into five steps:

1. Pre-installation steps in chapter 6.2.
2. Installing the SGxClientPreinstall.msi.
3. Installing the SGNClient_x64.msi.
4. Installing the SafeGuard Enterprise client configuration package
5. Reboot

As an alternative to the SGxClientPreinstall.msi it is possible to install the Microsoft vcredist_x86.exe package that is also available in the Product delivery.

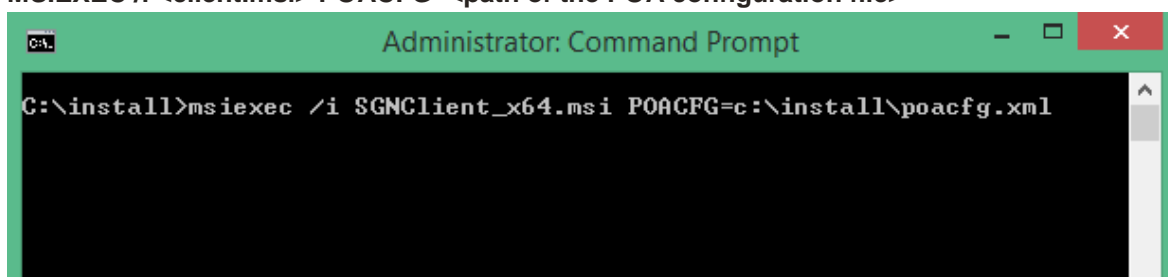
To install the SafeGuard Enterprise Client follow these steps:

1. Copy the SGNClient_x64.msi package and the SGxClientPreinstall.msi package to the client.
2. Install the SGxClientPreinstall.msi package – the installation is done by double-clicking the MSI package. The installer does not require any configuration
3. Download the current POACFG file as described in the knowledgebase:
<http://www.sophos.com/support/knowledgebase/article/65700.html>.

Note: The POACFG file is constantly updated. Before starting any client installation please check if a new revision of the POACFG file is available. We recommend using the latest file for new installations.

4. Download the latest version of the file and save it centrally so that it can be reached from every client.
5. Open a new administrative command line box on the client.
6. Change to the folder containing the SafeGuard installation files (C:\install in this example).
7. Start the installation using this command:

MSIEXEC /i <client.msi> POACFG=<path of the POA configuration file>



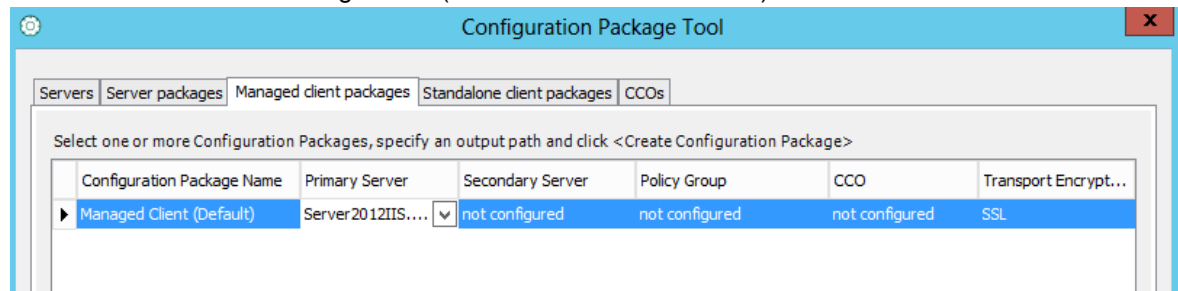
```
Administrator: Command Prompt
C:\install>msiexec /i SGNClient_x64.msi POACFG=c:\install\poacfg.xml
```

8. The SafeGuard Enterprise Client installation wizard starts.
9. Go through the installation wizard:
 - a. Accept the legal disclaimer.
 - b. Select the installation path. We recommend not changing the suggested path.
 - c. Select the required modules which should be installed.
 - d. Finish the installation

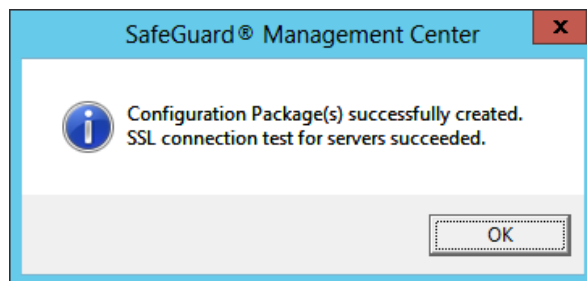
6.5 Creating the SafeGuard Enterprise Client configuration package

The installation of the SafeGuard Client is completed by installing a configuration package. This package is created in the SafeGuard Management Center.

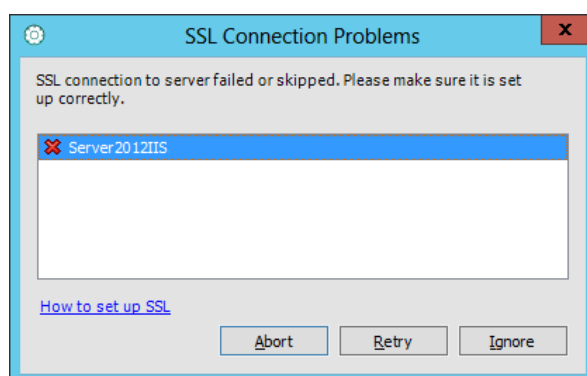
1. Switch to the machine that hosts the SafeGuard Management Center.
2. Open the SafeGuard Management Center.
3. **Select Tools > Configuration Package Tool > Managed client packages.**
4. In the dropdown box "Primary Server" of the "*Managed Client (default)*" package, switch to the server which was registered (Server2012IIS in this case).



5. Save the client configuration package via **Configuration Package output path** (lower right corner) and **Create Configuration Package** at a place where it can be reached by every client. The Management Center will perform a check that verifies that the configured server can be reached using an SSL encrypted connection. When the certificate was properly deployed and the server can be reached the package is created and a success message is displayed.



Please Note: If the SSL connection check fails, you can create the client configuration package anyway by clicking "Ignore". You have to ensure though, that the communication between the SafeGuard Client and the SafeGuard Server is possible using SSL.



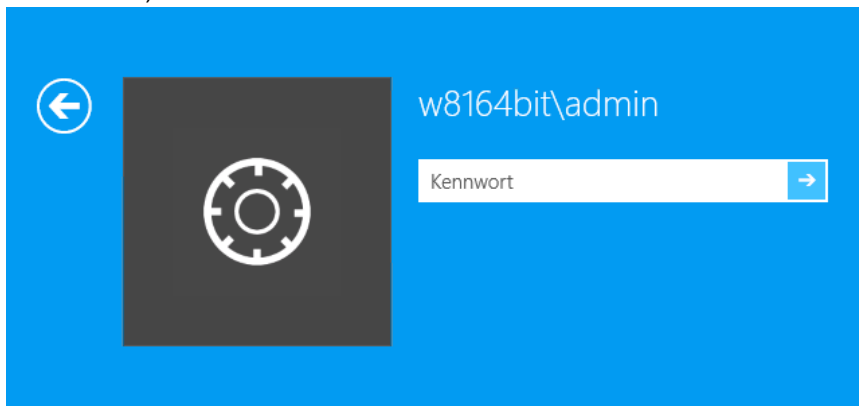
6.6 Installing the client configuration package

1. Copy the client configuration package to the machine on which the SafeGuard Client has already been installed.
2. Double-click the configuration package (MSI file). This will start the installation. The package does not require any configuration.
3. As soon as the installation is done, you are prompted to reboot the computer. **Reboot the machine at this point.**

6.7 Rebooting the machine after installation and initializing the user

At the end of the configuration package installation the machine forces a reboot. The machine reboots.

1. At the Windows logon dialog you'll notice that the credential provider icon has changed. Logon to the OS using the SafeGuard Enterprise credential provider (as shown in the screenshot).



2. When you switch to the desktop, a new tray icon appears in the taskbar which can be used to check the status of the client, trigger a synchronization with the server, etc.
3. As soon as the client can contact the SafeGuard Enterprise server the user initialization will be done automatically.
4. On success a popup message confirms that *Initial User synchronization completed.*

The installation of the SafeGuard Enterprise Client is now complete!

7. Installing the SafeGuard Enterprise Clients on Mac OS X

As soon as the back-end is running, the deployment and installation of the SafeGuard Enterprise Clients can begin.

There are some things that should be considered such as preparation tasks prior to the installation. Although these steps are only optional we recommend following these steps to ensure a smooth implementation.

The SafeGuard Enterprise Client can be installed on different kinds of hardware and on different operating systems. A list of all supported operating systems and the minimum system requirements can be found in the *Release Notes* which are available for each SafeGuard Enterprise version in the Sophos Knowledge Database.

Reading these articles is recommended before starting the installation of the SafeGuard client.

This example applies to a Mac OS X 10.8.x, Mac OS X 10.9.x or Mac OS X 10.10 computer. We install both available Mac OSX clients of SafeGuard Enterprise, File Encryption for Mac and SafeGuard Disk Encryption for Mac.

7.1 Quick installation reference

1. Install Fuse version 2.6.x if you want to use SafeGuard Enterprise File Encryption for Mac (proceed with step 7.3 if only Disk Encryption for Mac should be used).
2. Install SafeGuard Enterprise File Encryption for Mac
3. Install SafeGuard Disk Encryption for Mac
4. Import the SSL certificate to the system keychain
5. Import the SafeGuard Enterprise configuration zip file

7.2 Install Fuse (only required for File Encryption)

1. Downloaded the Fuse here: <http://osxfuse.github.io/>
2. Install the fuse *.dmg file

7.3 Install SafeGuard Enterprise File Encryption for Mac

1. Install the “Sophos SafeGuard FE.dmg” file by double clicking it

7.4 Install SafeGuard Enterprise Disk Encryption for Mac

1. Install the “Sophos SafeGuard DE.dmg” file by double clicking it

7.5 Import the SSL certificate to the system keychain

1. Open the Mac OS X keychain tool and select the System tab at the left side
2. Unlock the System keychain by using an Mac Admin user account
3. Import the same certificate (*.cer) as you have used before to implement the SSL function for the used IIS (described at cap. 6.2.9.)
4. Trust this IIS server certificate for using SSL for the System.

7.6 Import the SafeGuard Enterprise configuration zip file

1. After following chapter 6.5 of this guide, you get a valid client configuration Windows installer file (*.msi) and in addition to that a *.zip file with the same name.
2. Open the Mac OS X "System Preferences" and choose "Sophos Encryption", Select the "Server" tab and Drag and drop the configuration zip file into the corresponding field.
3. After a few seconds you should see the "last server contact" information.

8. Technical support

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

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

9. Legal notices

Copyright © 1996 - 2014 Sophos Group. All rights reserved. SafeGuard is a registered trademark of Sophos Group.

Sophos is a registered trademark of Sophos Limited, Sophos Group and Utimaco Safeware AG, as applicable. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

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