SafeGuard Device
Encryption
Recovery options

Document date: December 2014
This document applies to the following Sophos products:

<table>
<thead>
<tr>
<th>Product</th>
<th>Version(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SafeGuard Enterprise / SafeGuard Easy</td>
<td>5.6x, 6.x, 7.x</td>
</tr>
</tbody>
</table>
Introduction

This document will guide you through the required steps in order to solve common issues that might arise on a client or the backend and require recovery.

When to use this document?

The most challenging part is to determine the correct situation and the version in use. Based on these information it is then possible to take appropriate recovery steps.

However, should you encounter an error on the back-end such as a failing import of the Active Directory, a concrete error message or if you encounter problems on a client such as policies aren’t applied or that a user cannot be registered this document is inappropriate. In this case please consider the public knowledge database on www.sophos.com for further information.

Also for any recovery option for OPAL drives do not use the described steps in this document but contact local support instead.

This document targets recovery scenarios for SafeGuard Enterprise and SafeGuard Easy 5.x and later on none OPAP drives. Most recovery scenarios should also apply to Sophos Disk Encryption (SDE). Should you encounter any problems with earlier version of SafeGuard Easy (4.x) do not use this document but search the knowledge base for further information!

In order to provide the appropriate recovery steps the document is using scenarios.

How to use this document?

This document was designed to cover the most common recovery scenarios that might come up either on the client or on the back end side. The document is written from a second person perspective describing given scenarios. By comparing the scenarios with the current situation it will be possible to determine the next steps.

The document contains internal cross links. This means that the navigation from scenario to scenario is done by following the links in each chapter and not by reading from top to bottom. All links are blue and underlined (just as this example text).

As soon as you have found the appropriate section which fits most to your scenario please click on the link at the end of the decision and follow the steps in the next scenario/chapter afterwards.

The document starts with Determine the Environment/Product in use

What can you expect from the document?

This document was designed to provide solution steps for common issues in given scenarios. This document does not cover scenarios that are not mentioned explicitly in here.

Since this document cannot cover all possible scenarios please be aware that this document might not bring up a solution but requires opening a new support ticket.
Determine the Environment/Product in use

Select the appropriate next steps by comparing the scenarios given below with the current situation and follow the links for further information.

**Managed Environment (SafeGuard Enterprise managed)**

Client

Password Lost

*Password Recovery in SafeGuard Enterprise 5.6x and later*

Disk inaccessible

*Recovering Data by slaving Hard Drives*
*Accessing Data by assigning Keys temporarily*

Backend (Management Center, Web Server (IIS), SQL database)
*SafeGuard Enterprise Backend Recovery in 5.6x and later*

**Unmanaged Environment (SafeGuard Easy 5.x, SafeGuard Disk Encryption 5.x, SafeGuard Enterprise unmanaged)**

Client

Disk inaccessible

*Recovering inaccessible Disks of unmanaged Clients as of version 5.6x*

Back end (Policy Editor, SQL database)

*Policy Editor Recovery as of 5.6x*

**Definition unmanaged**

In an unmanaged environment there is no communication between the client and the back end.

**Exclusion**

For any recovery option for OPAL drives do not use the described steps in this document but contact local support instead.
Password Recovery in SafeGuard Enterprise 5.6x and later

SafeGuard Enterprise Version 5.5x offers the ability to use either Challenge/Response or Local Self Help to recover a machine in case of forgotten passwords or a locked POA.

Which type of Challenge/Response is required can be determined by using the flow chart on the next page.

Detailed information:

Creating a Challenge/Response code for a Managed

Detailed information: Local Self Help in SGN 5.6x and later

By following the flow chart it will be possible to determine the required steps to recovery a machine if the user has forgotten the password and recovery steps have already been carried out or not.

Best practice

In order to avoid problems with lost passwords and passwords getting out of band do not reset password centrally in the Active Directory. Instead we recommend using the SafeGuard Enterprise Challenge/Response feature which will enable a user to define a new password without resetting it centrally in the Active Directory before.

If the password has already been reset centrally it might be required to delete the user certificate from the Management Center and re-initialize the User Machine Assignment for that user.

Details can be found in the flow chart mentioned.
SafeGuard Device Encryption

Start User calls Helpline

Identify the user. Provide user that the call is the password calls to tel.
SOS needs access to SafeNC.
In some cases the SD needs to issue the certificate within the NC to continue on further steps.
This function is used for user/patlent authentication only and the option "Show user password" might impact on company security policy.
Always use this function from the beginning and fill in the "user name" field (left side). Focus start from anywhere else within the flowchart. Use the Recovery options from SafeNC instead of reissuing the password within After Directions if the user has forgotten his password, if possible.

Get User ID
Get Machine ID
Check local or NC

Start Challenge Response process and enter challenge code then press next.

What are the actions of this machine?

Is the user assigned to this machine?

Is the user connected to the network?

Login the user by using the Challenge/Response process. Select action about Windows client guided connection?

What is the user’s window setup?

Start Challenge Response process and enter challenge code then press next.

In the option "Show user password" in the Challenge/Response process of network?

Login the user by using the Challenge/Response process. Select action about Windows client guided connection?

The AD password was read.
The PPA and AD password cannot be a set of same data. Then machine is user.

Login the user by using the Challenge/Response process. Select action about Windows client guided connection?

Is the machine connected to the network?

Does the user have Windows client guided connection on this machine?

Inform the user that they only can use their own machines as corporate security policy.
Inform the user that he will need a Challenge/Response again at the local authentication as well as the network.
Inform the user that he cannot log in to SafeNC until the machine is connected to the network again.

User will be logged into Windows automatically.

End
Creating a Challenge/Response code for a Managed Client

This part will describe how to create a C/R code step by step. These steps will describe the complete C/R procedure on the Client as well as on the Management Center chronologically.

On the Client – Step 1
1. Enter the logon user name at POA level
2. Call your Helpdesk
3. Press the Challenge Button
   
   ![Challenge Button Image]

4. Tell the helpdesk operator the user name, the domain, the machine name and the challenge code as it is displayed

   ![Challenge Code Image]

On the Management Center
1. Open the Management Center
2. Open Tools → Recovery
3. The “Recovery Wizard” window will come up

![Recovery Wizard window](image1)

4. Go to the field “Online Client” chose Domain and Computer. After that click on next

![Recovery Wizard window](image2)
5. Now choose the User. After that click on Next

6. Enter the challenge code according to the information as it is presented by the user.

7. After that the action drop down list will become active. The field will offer to **Boot the Machine with or without user logon**. In case you pick the alternative with user logon the option “Show user password” will also become active and can be checked. The usage of this special function will be displayed later on in the chapter 3.1 “Recovering passwords in SafeGuard Enterprise”. 
8. The response code will now be displayed. Pass the information to the client requesting the C/R code.

**On the Client – Step 2**

1. After presenting the challenge code please wait for the confirmation from the helpdesk operator that the presented code is valid. After that click on next.

2. A new window will come up. Enter the response code as it passes by the helpdesk operator. After that click on OK and the system will boot and perform the requested action.
Local Self Help in SGN 5.6x and later

Beginning with version 5.50 SafeGuard Enterprise offers client based log on recovery via Local Self Help (LSH).

By using Local Self Help the user is able to recover a machine without contacting the local help desk by answering a set of questions at POA level. However, in order to use Local Self Help several conditions must be met:

Local Self Help must be activated via policy and the policy must be assigned to the client
Before using Local Self Help the user needs to answer the pre-defined questions
Local Self Help can only be used to recover forgotten passwords. Should the machine be locked due to a local cache corruption it is required to perform a normal Challenge/Response using the Management Center or Web Help Desk (which is an additional component that needs to be installed separately)
Local Self Help cannot be used in combination with all log on methods. Ensure that the correct method is in use corresponding to the version in use else Local Self Help will not be available as a recovery option at POA level

<table>
<thead>
<tr>
<th>Method</th>
<th>Recovery Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>UID / Password</td>
<td>LSH available</td>
</tr>
<tr>
<td>Crypto Token or Token only</td>
<td>No LSH</td>
</tr>
<tr>
<td>Token or UID / Password</td>
<td>LSH available</td>
</tr>
<tr>
<td>Fingerprint or UID / Password</td>
<td>LSH available</td>
</tr>
<tr>
<td>Fingerprint only</td>
<td>No LSH</td>
</tr>
</tbody>
</table>
Configuring Local Self Help

In order to use Local Self Help perform these configuration steps:

Open the Management Center and create a new policy allowing Local Self Help. Local Self Help is disabled by default.

Open the Management Center > Switch to the Policy Tab > Select Policy Items > Create a new Policy of type General Settings Policy > Local Self Help in the right hand pane > Enable Local Self Help > Set to Yes

Assign the policy to the user and synchronize the client with the server

As soon as the policy has reached the client Local Self Help can now be activated

Right click on the SafeGuard Enterprise tray icon > Local Self Help
A dialog comes up asking the user to authenticate. Log on using the (domain) password of the user. After that, answer the number of questions defined by the Administrator.

**Note**
Minimum number of available questions/answers and Number of questions presented in POA can be configured as of version 5.60 in the Management Center. In earlier versions these numbers were set to 10/5.

Open the Management Center > Switch to the Policies tab > in the left hand pane select Local Self Help questions > it is now possible to define these values on the right side.

As soon as all questions are answered Local Self Help can now be used

**Using Local Self Help**
Local Self Help recovery is done like this

1. Start the client machine
2. At POA level enter the user name
3. Click on Recovery

If Local Self Help and Challenge/Response are available for logon recovery, a dialog with both recovery methods for selection is displayed. Click **Local Self Help**.

Answer the pre-defined number of questions

At the end the password of the user will be displayed as soon as all questions have been answered correctly.
Recovering inaccessible Disks in SafeGuard Enterprise

Under special circumstances it might be possible that Microsoft Windows will not boot up any more. The reason for this can be an incompatibility with software on the machine, for example, or worst case a virus. In such a situation the authentication to the POA in general is possible.

Another scenario might be that a colleague is not available, but the data on his machine needs to be accessed nevertheless.

In such situations the data on the drive can be accessed anyhow! SafeGuard Enterprise offers different ways of accessing and recovering data depending on the situation:

- Recovering Data by slaving Hard Drives
- Accessing Data by assigning Keys temporarily
- Recovering data using an external boot medium
- Recovering a Client with broken MBR
  - Retrieving data using Virtual Client
Recovering Data by slaving Hard Drives

Due to the fact that SafeGuard Enterprise has a flexible key management it is possible to assign the key that was used to encrypt the drive to a different user and attach the hard drive with an external USB connector to a machine that should have access to the data e.g. the Administrator PC.

Slaving a drive that is encrypted is done like this:

- Take the drive that should be accessed out of the machine affected and plug it into an USB hard drive converter.
- Attach the USB converter to a machine that has SafeGuard Enterprise installed.
- Under “My Computer” the drive will be displayed with a red key icon which indicates that the drive is encrypted but the key is not available.
- In order to check which key was used right click on the drive and select Properties. Open the Encryption tab. Within this tab the Unique Key ID will be displayed.

- Should the key not be displayed perform these additional steps else proceed with the next section:
  1. Browse to Tools folder in the installation source of SafeGuard Enterprise
  2. Copy the complete folder KeyRecovery and Restore to the local machine that should gain access to the drive
  3. Open the folder and start RecoverKeys.exe
  4. All connected drives will show up. The key ID of the attached drive is displayed and can now be searched in the Management Center
- Open the SafeGuard Management Center and switch to the user that should gain access to the files requested. This user can be understood as guest user.

- Switch the focus to the middle window by simply clicking into it. The key symbol (marked as 1 in the picture) will change from "grayed out" to "available".

Click on the binocular symbol (marked as 2 in the picture). A new search window will appear. Switch to Key-ID in the Find field and search for a key with its Unique ID as shown above.

**Note**
Recovery Options

It is not necessary to type the whole ID. Since all the ID’s are unique it should be sufficient to search for the first five characters. The search result will show the key name and not only the Key-ID. So in case the search result does not present a unique key it is possible to use more characters for the search in order to find only the key that is searched.

- By double clicking on the key name it will now be assigned to the user and show up in the key tab.

Please note: Every other key can be assigned by "dragging and dropping" the key from the right pane window named "Available keys" to the key section of the user. The boot key of a SafeGuard Enterprise protected machine will not be displayed in this list even if searching for it.

- Logon to Windows with the user to whom the key was assigned. It might require an additional reboot until access to the drive is possible.

- Attach the USB connector to the machine. The drive will be recognized as an external media. Access is now available just as to a normal hard drive.

:Back:
Accessing Data by assigning Keys temporarily

SafeGuard Enterprise uses a flexible way to manage encryption keys. Every user has his personal key ring which can be enlarged on demand with keys of other groups or users if requested. This procedure allows a user to access files that are encrypted with a personal or group key of a colleague who is not available due to illness or vacation. In order to access these files please perform these steps:

The user that should access the data must gain physical access to the machine storing the data
Start the machine > At POA level do not enter a user name > request a Challenge/Response. This will automatically create a response code to boot the SGN Client without user logon

Further Details about C/R:
Creating a Challenge/Response code for a Managed

In case the data is stored on the %SYSTEMDRIVE% no further actions are required. The machine will automatically load the boot key which will automatically enable access to all files stored on this partition.

Should the data still be inaccessible please either assign the key for the file or for the drive to the user to access the data.

To check the key to be used for encryption for a file based encrypted file take these steps:
Right click on the file that should be accessed
Select File encryption > Encryption Status

The key presented in the next dialog is the one that needs to be assigned to the user. The detailed process of assigning a key to a user is described in a different section. Please ignore the part about slaving the disk and only use the key assigning section described here

Recovering Data by slaving Hard Drives
Recovering a Client with broken MBR (Master Boot Record)

The SafeGuard Enterprise boot process

SafeGuard Enterprise encrypts files and drives transparently. Boot drives can also be encrypted. This means that decryption functionalities such as code, encryption algorithms and encryption key must be available very early in the boot phase. Therefore, encrypted information cannot be accessed if the crucial SafeGuard Enterprise modules are unavailable or do not work.

SafeGuard Enterprise's Power-on Authentication is loaded from the MBR on a computer's hard disk. When the installation is done, SafeGuard Enterprise saves a copy of the original - as it was before the SafeGuard Enterprise installation - in its kernel and modifies the MBR loader from LBA 0. In its LBA 0, the modified MBR contains the address of the first sector of the SafeGuard Enterprise kernel and its total size.

1.1.1 Recovering/Restoring MBR

Problems with the MBR can be resolved using the SafeGuard Enterprise recovery tool “BE_RESTORE.exe”. This tool is a Win32 application and must run under Windows - not under DOS.

A faulty MBR loader will mean an unbootable system and can have effects like shown in the following pictures:

The MBR can be restored in two ways using the pre available WinPE CD with integrated SafeGuard Enterprise drivers.

Restoring MBR with an existing MBR
Restoring MBR with an existing MBR Backup

Recovering the MBR of a machine using an existing backup is done in two steps.

First export the MBR backup on a USB sticks and then restore the backup using the available WinPE CD.

Exporting the MBR Backup

Every SafeGuard Enterprise client saves its own computer's SafeGuard Enterprise MBR (LBA 0 of the boot hard disk after being modified by SafeGuard Enterprise) in the SafeGuard Enterprise database.

To export the MBR backup from the SafeGuard Enterprise Management Center:

Start the Management Center > Users & Computers > select the specific computer (i.e. “SGNCLIENT”) > right-click > Properties
Switch to the Machine Settings tab > Backup > MBR (Master Boot Record) > Export

This produces a 512 byte file with the file extension .BKN, which contains the MBR. Copy this file onto a USB stick.

Restoring the MBR using WinPE

In order to restore the MBR it is required to boot the system using the correct WinPE CD with the correct driver version of SafeGuard Enterprise.

Downloadable ISO images for all versions can be found in KBA 108805 on www.sophos.com

As soon as the image is available burn the ISO file to a CD.

Next put the Windows PE Boot CD into the PC, attach the USB stick with the SGN files to machine and switch the computer ON. Boot from the CD before the POA.

As soon as the CD is loaded select Be_restore in AC43 file browser. Now select the option to repair the MBR and load the bkn file from the USB stick.

As soon as the process is completed restart the machine and check if booting is possible now.
Repairing the MBR without Backup

Even when there is no MBR backup file available locally, BE_Restore.exe can repair a damaged MBR loader. The BE_Restore.exe repair option locates the SafeGuard Enterprise kernel on the hard disk, uses its address, and re-creates the MBR loader.

This is highly advantageous, especially as there is no need for a computer specific MBR backup file locally. However, this will take longer because BE_Restore.exe has to carry out a time consuming search for the SafeGuard Enterprise kernel on the hard disk.

To use the repair function in Be_Restore just do the same steps as described under Restoring MBR with an existing MBR beginning at Restoring the MBR using WinPE.

This time select “Repair MBR” instead of “Restore MBR”.

Be_Restore will then search the SGN kernel on the hard disk.

If more than one kernel is found when using the BE_Restore.exe repair option MBR with the most recent time stamp is restored.
Retrieving data using Virtual Client

SafeGuard products offer the possibility to recover data in case a machine is unbootable. This means that the POA doesn’t start any more or access to the system is not possible for some reason.

In such a case it is possible to recover data using an external boot media such as a WinPE CD. Since the drive is encrypted it is required to use a WinPE CD with the correct driver version of SafeGuard Enterprise.

In order to complete the next sections please create a WinPE CD based on the SafeGuard product version in use.

Downloadable ISO images for all versions can be found in [KBA 108805](http://www.sophos.com) on www.sophos.com

The following chapter will describe how to gain access to an encrypted drive (In this case the D:\ drive) using the WinPE CD. This process can be applied to any other internal drive as well.

### 1.1.2 Booting the System using the WinPE CD

Make sure that the boot sequence in the BIOS-settings allows booting from a CD. After that put the CD into the optical drive of the computer and start the machine.

The bootable WinPE CD will load without any user interaction and an integrated file manager comes up once the load is completed.

At a glance, you can see the mounted volumes and CD/DVD drives. In this example when selecting the encrypted Volume D: no files and folders are displayed.
Creating the Virtual Client

The next step is to create a virtual client file that can be used to generate a Challenge/Response which is required to load the key into the PE environment.

To create a virtual client start:

Either via the SafeGuard Management Center > Switch to the Keys and Certificates section > Press the Add Virtual Client button on the right hand side and define a name.

Or via the SafeGuard Policy Editor > select the Virtual Client tab > Press the Add Virtual Client button on the right hand side and define a name.

In this example the name of the Virtual Client is VC1.

Next step is to export the “Virtual Client” VC1. Just press the Export Virtual Client button on the right hand side.
The destination for the exported recoverytoken.tok file should be a removable media - a USB stick is recommended - because the virtual client file has to be transferred to the broken computer.
Importing the Virtual Client into the KeyRecovery.exe Wizard

In the virtual environment ensure that the USB-Drive with the recoverytoken.tok file stored on it has been mounted correctly during startup.

In this example the USB stick was mounted to the drive F: (Utimaco)

Browse to the Removable Media and select the recoverytoken.tok file. Next step is to copy this file to the SGN-Tools folder on the WinPE which shows up as volume X:\ (Boot).

Using the implemented file manager, there are several ways to copy the recoverytoken.tok file from the USB-Stick to the drive X: into the folder X:\Tools\SGN-Tools, where the RecoverKeys.exe is located.

You can copy the file recoverytoken.tok e.g. by

- drag and drop (see the picture above)
- copy and paste
- using the menu option "Edit - Copy to Folder".
Once the file is copied open the **KeyRecovery Tool** with a single click on the KeyRecovery symbol. You can find this at the bottom of the File Manager in the section *“Quick Launch”*. The KeyRecovery tool starts and displays the Key ID of each encrypted Drive. This Key ID will be demanded later. Therefore, write down the first five characters of the ID.

Select *Import By C/R* > This will generate a challenge code.
Creating the Response Code

The next step is to generate the appropriate response code for the challenge just created.

To create the response code start the SafeGuard Enterprise Management Center > Tools > Recovery

Define the recovery type as “Virtual Client”
In the next dialog press “Find Now” and select the appropriate virtual client (VC1 in this example).

After that proceed by clicking “Next”.

Recovery type

Please select recovery type

- **Online Client**
  - Computer information
    - Domain:
    - Computer:
    - Distinguished name:

- **Virtual Client**
  - Virtual Client: VC1

- **Offline Client**
  - BAK file:
Click “Next” to start the search for the Key ID.

The next steps depend on the fact whether a managed or an unmanaged client should be recovered:

**Managed**

**Unmanaged**
Managed

Next step is to either enter the key name or the key ID since the key name is unknown a key ID will be used. Enter the search field as shown below.

Change the Find Section to *Key IDs* and enter the first five characters of the key ID into the *Search Name field*. Press “Find now” to get a list of available keys.
The Key ID is the one shown when starting RecoverKeys.exe

Select the proper Key ID and click “OK”.

Note
Using a dedicated Key ID will reduce the search result to a minimum – the section above displays all available keys.
Click the “Next” button to confirm the appropriate key.

The next step will be Providing the Challenge Code
Unmanaged

Next step is to select the key file from the client machine in order to load the machine key.

Select the key backup xml belonging to the machine. Identification will be possible via the machine name marked red in this example.

The next step will be **Providing the Challenge Code**

**Providing the Challenge Code**

Type in the challenge code that has been created on the client side.
SafeGuard Device Encryption

If the challenge code matches, a Response Code will be generated.

On the client side, enter the response code in the KeyRecovery Tool to get access to the encrypted drive.
Once the process has been completed successfully select the read enabled volume (in this case D:\) in the file manager window.

Once the C/R is done all files and folders of drive D:\ are visible in the file manager. Drive D: is read enabled now and access to the data stored on this partition is reconstituted.
SafeGuard Enterprise Backend Recovery in 5.6x and later

The SafeGuard Enterprise backend contains three modules:
- The Management Center
- The Server (IIS)
- The database

Compared to earlier versions of SafeGuard Enterprise, new recovery options have been integrated into the product as of version 5.6x. These will provide more fault tolerance and flexibility when recovering data. Some of the options in this section are not available in earlier versions!

Although each module has its own installation, the recovery has to cover all parts of the back end since there is permanent communication between all modules.

However, please select the appropriate module to start the recovery steps.

**Recovering the SafeGuard Enterprise Management Center**

**Error! Reference source not found.**

**Recovering the SafeGuard Enterprise**
Recovering the SafeGuard Enterprise Management Center

The SafeGuard Management Center is used to manage all imported Active Directory objects as well as groups, users and policies. It performs the challenge response procedure. Furthermore, the SafeGuard Enterprise Management Center is used to manage all SafeGuard Security Officers, active and retired keys as well as certificates. It also creates the client or server configuration packages and displays internal reports.

Actually, there are a couple of things that must be available if the Management Center needs to be recovered:

- The p12 file of a Security Officer. These files should be saved to an external device anyhow.
- The SafeGuard Enterprise database must be up and running. The database stores all necessary information so that SGN can run properly. If it is not available the SG MC cannot logon to the database and display anything.

Should one of these files or conditions not be available a recovery will not be possible!

In case the Management Center gets corrupted and needs to be installed simply remove the program via “Add or Remove Programs” out of Windows and install it again. Upon the next reboot the SafeGuard Management Configuration Wizard will come up again in order to set up the database connection and to define the SafeGuard Security Officer that should be used for the authentication to the Management Center.

When going through the Wizard please make sure that you pick the already existing and running database. Do not create a new one.

The whole procedure of initializing a SafeGuard Management Center looks like this:

1. Uninstall the SafeGuard Management Center that is not working from the affected machine.
2. After that reboot the machine
3. Install the Management Center again.
4. A message will come up. Please accept it. Otherwise the process will terminate immediately.

5. After that the SafeGuard Management Center Configuration Wizard will come up just as if the Management Center was installed the first time.
6. First select the SQL server that stores the database and the authentication method.

7. In the next step it is necessary to pick the existing database and not to create a new one. (The existing one should be pre-selected)

8. After that there will be no dialog to create a new MSO but to choose an already existing SO. This can either be the one that was used before or a different one that should be used now to authenticate to the Management Center.
9. The next time the Management Center is started the normal Management Center logon dialog will be displayed.

10. The certificate of the SO is not available and the personal key store has not yet been initialized on this machine. For that reason a message box will come up in order to import this information.

11. Within the next dialog the certificate of the SO must be browsed (1). Then the password for the MSO key file as well as the password for the certificate store must be entered (2) in order to authenticate to the certificate. This will ensure that no one can access the system by only importing a valid SGN certificate.
12. After completing step 10 the personal certificate store must be created for the Windows user. This will automatically be done in the next step. Please note: Here you have to enter the initial password that was just entered before.

13. After that the logon window to the Management Center will come up again and an authentication is possible now.
Recovering the SafeGuard Enterprise Database

SafeGuard Enterprise uses a single database in the background to save all necessary data that is needed to run the complete SafeGuard Enterprise environment. In this database, all key and certificate information, assigned users, Active Directory objects, assigned policies and the company certificate information is stored. This database is normally created during the installation process. In case this database gets corrupted without having a backup available the potential risk of losing data increases dramatically.

For that reason it is recommended to backup this database regularly to ensure that data can be recovered as up to date as possible in a worst case scenario. You as a customer can decide which backup strategy should be used/to use for the database.

However, the database recovery in SafeGuard Enterprise has been improved beginning with version 5.4x. There are two options to recover the SafeGuard Enterprise database:

Recreating the SafeGuard Enterprise Database by restoring a valid backup
Creating a new database and importing an existing company certificate

The main difference between these two options is that all server created keys (OU keys, group keys, domain keys) will be lost when creating a new database running the old company certificate. As a result it will not be possible to recover data that has been encrypted with these keys.

However, for the SafeGuard Enterprise clients it will still be possible to send the computer keys back to the server. This will ensure that Challenge/Response can still be done and clients don’t need to be reinstalled. This means that using a new database in combination with an old company certificate can be seen as an emergency solution – restoring a proper database backup is the preferred recovery option.

It is possible to decide between two recovery methods:

- **Recreating the SafeGuard Enterprise Database by restoring a valid**
- **Creating a new Database and importing an existing Company Certificate**
Recreating the SafeGuard Enterprise Database by restoring a valid Backup

In case the SafeGuard database gets corrupted, perform the following steps:

1. Stop the IIS server in order to prevent write access to the database. In case the SafeGuard Enterprise Server is not accessible the clients will simply hold all information locally until they can reach the SafeGuard Enterprise Server again.

2. Stop the SQL services and cut all open connections to the SafeGuard Enterprise database. This will ensure that no changes can be made to the database from any SafeGuard Enterprise Management Center in the network.

3. Restore the latest backup of the database.

4. Restart all SQL services and the IIS Server.

5. Check the result of the invoke test. If the test passes the result will look like below.

We recommend checking the latest actions that were performed in the SafeGuard Enterprise Management Center before an issue occurred in order to make sure that no key data is lost. If an encryption key of a machine is not available please uninstall SafeGuard Enterprise from this machine (will include a decryption) and reinstall. This will ensure that all necessary key data is available if such a machine must be restored.
Creating a new Database and importing an existing Company Certificate

In order to create a new database with an existing company certificate the certificate needs to be exported before any issue arises.

It is not possible to export the company certificate once an issue has happened!

A backup of the company certificate is done like this:

Start the SafeGuard Enterprise Management Center

Go to Tools > Options > Switch to the Certificates tab > Select Export in the Company Certificate section

Enter a password to secure the exported file and store it in a safe location, for example, on an external media.

Once the file has been saved a recovery will be possible. Should an issue come up perform these steps to start with a new database running the old company certificate:

1. Uninstall the SafeGuard Management Center that is not working from the affected machine.
2. After that reboot the machine.
3. Install the Management Center again.
4. A message will come up. Please accept, otherwise the process will terminate immediately.
5. After that the SafeGuard Management Center Configuration Wizard will come up just as if the Management Center was installed the first time.
6. First select the SQL server that stores the database and the authentication method

![Database Server Connection]

7. In the next step create a new database

![Database Settings]

Create a new Master Security Officer just as running the installation for the first time.
Detailed information about the process of creating a Master Security Officer and running the Management Center for the first time can be found in [KBA 110259](https://www.sophos.com) on [www.sophos.com](http://www.sophos.com)

The next step is to specify that an existing company certificate should be used instead creating a new one. Import the file that was previously exported from the old installation. Confirm the dialog that comes up with Yes else the Import... button will remain grayed out.
After that the database will be created just as usual.

Next step is to restore the server as described here Error! Reference source not found.
Create a new client configuration package in case the SafeGuard Enterprise server name was changed else the clients will automatically start communicating back to the database sending their keys and re-registering in the SafeGuard Enterprise Management Center.

**Note**

When using this type of recovery clients will fall back to autologon mode and the UMA will be lost on all machines and needs to be reinitialized; however, all machines will remain encrypted.

Additionally Challenge / Response will not be possible until the client has reported back to the server.
Unmanaged installations of SafeGuard Enterprise 5.4x and SafeGuard Easy 5.x do not offer the wide range of possible recovery scenarios available in a managed environment.

Unmanaged installations only offer the ability to use Challenge/Response. Then they remove the User Machine Assignment or Local Self Help to recover a machine in case of forgotten passwords. This option will only be possible if a second user is available to log on to the machine.

In case no further users are available on a machine it is only possible to retrieve data by using the WinPE CD with a subsequent reinstallation of the operating system.

If POA is locked Challenge/Response is the only option to unlock such a machine again.

The available recovery options are:

- **Creating a Challenge/Response for an unmanaged Client**
- **Resetting the UMA**
- **Local Self Help in SGE 5.x and SafeGuard Enterprise 5.6x and later**

If the POA is locked only the first option can be used.

In case of a forgotten password either resetting the UMA or Local Self Help can be used. Local Self Help will only be available if it was configured before the issue came up.
Resetting the UMA (User Machine Assignment)

In opposite to password recovery in a managed environment a central password reset is needed in order to recover a machine.

The detailed steps are like this:

Create a Challenge/Response to boot the machine to Gina or Credential Provider level

**Detailed information:** Creating a Challenge/Response for an unmanaged Client

Either change the password of the user centrally or log on to the machine with a second local user and change the password of the affected user.

After that log on to the operating system using a user account (either local or domain depending on the setup – it is possible to use a local user on a domain machine as well) that is allowed to run scripts!

Once logged on download a ZIP file with two **VBS scripts** from KBA 108795 on www.sophos.com. This is needed to recover the machine

Save the file to an appropriate location on the affected machine and unzip it. It contains the two scripts CreateUMAOff.vbs and ImportUMAOff.vbs

Run the CreateUMAOff.vbs script on the client

The script creates an XML file which has to be signed in the Management Center or Policy Editor. The file is created in the same folder where the VBS script was started from.

Copy the file to the machine running the Policy Editor or send it to the help desk officer via email

1. The help desk officer must start the Policy Editor or Management Center now
2. Go to **Tools > Options > select the Company Certificate tab > click the button Sign File for Policy Cache**
Browse to the file that was created and click "OK". A new file with the filename filename_signed.xml is created at the same location as the original file.

Copy the signed file into the Import folder of the client.

Windows XP
C:\Documents and Settings\All Users\Application Data\Utimaco\SafeGuard Enterprise\import

Windows VISTA / 7
C:\ProgramData\Utimaco\SafeGuard Enterprise\Import

Run the "ImportUMAOff.vbs" script on the client to import the signed file. The XML-file should disappear from the import folder once the script is completed.

Reboot the machine.

The POA will now run in autologon mode and the user who authenticates at GINA/Credential Provider level after the next reboot activates the POA again.
Creating a Challenge/Response for an unmanaged Client

On the Client – Step 1

1. Boot the machine to POA level
2. Call your helpdesk
3. Press the Recovery button

Tell the helpdesk the key recovery file for this machine

Press Next > the challenge code will be displayed
On the Policy Editor

1. Open the Policy Editor
2. Open Tools → Recovery

3. The “Recovery Wizard” window will come up. Select **Standalone Client** and browse to the XML file of the machine that should be recovered

4. Enter the challenge code provided by the end user.

5. After that the action drop down list will become active showing all available actions. Select the appropriate actions and press Next
The response code will now be displayed. Pass the information to the client requesting the Challenge/Response code.

On the Client – Step 2

1. After presenting the challenge code please wait for the confirmation of the helpdesk operator that the presented code is valid. After that click on next

2. A new window will come up. Enter the response code as it passes by the helpdesk operator. After that click on OK and the system will boot and perform the requested action.
Local Self Help in SGE 5.x and SafeGuard Enterprise

5.6x and later

By using Local Self Help the user is able to recover a machine without contacting the local help desk by answering a set of questions at POA level. However, in order to use Local Self Help several conditions must be met:

Local Self Help must be activated via policy and the policy must be assigned to the client.

Before Local Self Help can be used, the user needs to answer the pre-defined questions.

Local Self Help can only be used to recover forgotten passwords. Should the machine be locked due to a local cache corruption it is required to perform a normal Challenge/Response using the Management Center or Web Help Desk (which is an additional component that needs to be installed separately).

Local Self Help cannot be used in combination with all log on methods. Ensure that the correct method is in use corresponding to the version in use. If not the Local Self Help will not be available as a recovery option at POA level.

<table>
<thead>
<tr>
<th>Log on Mode</th>
<th>SGN/SGE 5.6x and later (unmanaged)</th>
</tr>
</thead>
<tbody>
<tr>
<td>UID/Password</td>
<td>LSH available</td>
</tr>
<tr>
<td>Crypto Token or Token only</td>
<td>No LSH available</td>
</tr>
<tr>
<td>Token or UID/Password</td>
<td>LSH available</td>
</tr>
<tr>
<td>Fingerprint or UID/Password</td>
<td>LSH available</td>
</tr>
<tr>
<td>Fingerprint only</td>
<td>No LSH available</td>
</tr>
</tbody>
</table>

1 The log on mode is not available in this version.
Configuring Local Self Help

In order to use Local Self Help it is required to activate the feature per policy. As of version 5.5x Local Self Help is enabled in the default policy.

Should the default policy not be used to install the client perform these configuration steps to activate Local Self Help:

Open the Policy Editor and create a new policy allowing Local Self Help. Local Self Help is disabled by default.

Open the Management Center > Switch to the Policy Tab > Select Policy Items > Create a new Policy of type General Settings Policy > Local Self Help in the right hand pane > Enable Local Self Help > Set to Yes

Assign the policy to a policy group and deploy the policy to the client using the client configuration package

As soon as the policy has reached the client Local Self Help can now be activated. Right click on the SafeGuard Enterprise tray icon > Local Self Help
A dialog comes up asking the user to authenticate. Log on using the (domain) password of the user. After that, answer the number of questions defined by the administrator.

**Note**
Minimum Number of available questions / answers and Number of questions presented in POA can be configured as of version 5.6x in the Policy Editor. In earlier versions these numbers were set to 10/5.

Open the Policy Editor > In the left hand pane select Local Self Help questions > it is now possible to define these values on the right side.

As soon as all questions are answered Local Self Help can be used now.

**Using Local Self Help**
Local Self Help recovery is done like this

1. Start the client machine
2. At POA level enter the user name
3. Click on Recovery

If Local Self Help and Challenge/Response are available for logon recovery, a dialog with both recovery methods for selection is displayed. Click **Local Self Help**.

Answer the pre-defined number of questions

At the end the password of the user will be displayed as soon as all questions have been answered correctly.
Recovering inaccessible Disks of unmanaged Clients as of version 5.6x

Unmanaged installations of SafeGuard Enterprise 5.5x and its subsequent versions as well as SafeGuard Easy 5.x installations offer a wider range of disk recovery options compared to earlier versions.

The available recovery options are Challenge/Response and booting via WinPE before the POA.

Last but not least, it is still possible to boot from external media after the POA although this is something hardware dependent whereas booting before POA will always work.

Limitations

Challenge/Response can only be used to unlock a machine in case of a locked POA.

Detailed Information: Retrieving data using Virtual Client

Detailed information: Creating a Challenge/Response for an unmanaged Client

Detailed information: Booting from external Media after the POA
Booting from external Media after the POA

SafeGuard products offer the ability to continue booting after POA either to the internal hard drive or to an external media such as a WinPE CD.

Prerequisites

- The BIOS of the computer must be set to the correct boot order, e.g. CD-ROM (first boot device), Hard Drive (second boot device) etc. On some machines it is necessary to define it the other way round.
- A policy that allows "booting to external device" ("booting to hard disk only" set to NO) must have already been applied.

Hint: In order to restore the MBR it is required to boot the system using the correct WinPE CD with the correct driver version of SafeGuard products. Downloadable ISO images for all versions can be found in KBA 108805 on www.sophos.com. As soon as the image is available burn the ISO file to a CD.

Boot Procedure

1. Insert CD in the CD-ROM drive
2. Boot from the hard disk so that the POA will come up
3. Type in the username and the password
4. Under Options choose Continue Booting from: external Media
5. SafeGuard will load. As soon as you see ‘Boot from CD-ROM, press any key’ message, press any key.

Once the WinPE is loaded it is possible to access all machine key encrypted data via the integrated file browser A43 that will start automatically or to restore the MBR of the machine using BE_restore. Access to data encrypted with a different key will not be possible.

Detailed information: Repairing the MBR without

Although, it will not be possible to restore an existing MRB backup (this option is only available in managed environments), it is possible to use BE_restore to repair the MBR automatically.

Additional information

If booting from external media (e.g. CD) after POA does not work, the main reason is essentially an issue associated to the BIOS versions on the machines. The BIOS incompatibility occurs because of the way external media is addressed at boot time. Some BIOS functions are only available at the point when the BIOS requires them. The reason for this is a lack of available memory in the BIOS Flash, some parts of the code are stored in a compressed form and are only ever extracted if needed.

As soon as the function is called by SafeGuard the required code is not loaded and boot will fail.
Policy Editor Recovery as of 5.6x

Beginning with SafeGuard 5.4x new and better recovery options were implemented into the Policy Editor enabling easier recovery in case of a problem. However, the main conditions remain unchanged.

The SafeGuard Policy Editor is installed on single machine. In case of an issue the whole installation has to be recovered and not only parts of it as in a managed environment.

To recover a Policy Editor installation a good backup of the SafeGuard database along with the Certificate (.cer) and Private Key (.p12) of the security officer is required. Should one of these things not be available recovery will not be possible.

A database backup can either be created manually using a case sensitive OSQL command or via the Policy Editor as of version 5.6x

The OSQL command is:

```
osql -S [Machine Name]\SQLEXPRESS -E -Q "backup database Safeguard_[Domain Name]_[Machine Name] TO DISK = '[Destination]'"
```

For example, on a workgroup machine called “Client” the call could be like this:

```
osql -S client\SQLEXPRESS -E -Q "backup database safeguard_client_client TO DISK = 'C:\DBBACKUP\DBBACKUP'"
```

Beginning with version 5.6x it will be possible to create a DB backup in the Policy Editor. Open the Policy Editor > Tools > Database backup/restore > Backup database.

As of version 5.5x there are two ways of restoring the Policy Editor:

- **Restore using a Database (DB)**: Backup
- **Restore using available Cert and p12**
**Restore using a Database (DB) Backup**

The detailed steps to recover a Policy Editor by restoring a DB backup are:

1. **(Re)Install the Policy Editor**
2. Once the installation is completed, the initial wizard will start > Close the Wizard
3. Restore the DB backup of the existing installation using OSQL. The DB name can be chosen freely.

    **Detailed steps:**
    - Open a new CMD promptly (Start > Run… > CMD)
4. Type the following **case sensitive** command. Below example stores the DB backup file DBBACKUP which is kept under C:\DBBACKUP

    ```cmd
    osql -S [Machine Name]\SQLSERVER -E -Q "RESTORE DATABASE [DB Name] FROM DISK = '[Path to backup file]' with replace"
    ```

    ```cmd
    C:\>osql -S client\SQLSERVER -E -Q "RESTORE DATABASE RESTORED_Safeguard FROM DISK = 'C:\DBBACKUP\SCNDBBACKUP.bak' with replace"
    Processed 344 pages for database 'RESTORED_Safeguard', file 'SafeGuard_CLIENT_CLIENT_Data' on file 1.
    Processed 7 pages for database 'RESTORED_Safeguard', file 'SafeGuard_CLIENT_CLIENT_Log' on file 1.
    RESTORE DATABASE successfully processed 351 pages in 0.654 seconds (4.392 MB/sec).
    C:\>
    ```
5. Start the Policy Editor
6. The initial wizard will come up again
7. Select the restored database

[![SafeGuard® Policy Editor Configuration](image)](image)

8. Select the saved p12 of the security officer and proceed with next at the end.
9. The Policy Editor starts. Policies and settings will be available at the status as the backup was done.
The detailed steps to recover the system by importing existing p12 files are like this:

1. (Re)Install the Policy Editor
2. Once the installation is done the initial wizard will start
3. Create a new database > Next
4. The security officer dialog comes up

Uncheck Automatically create Certificate and > Press the Import button > Select the saved p12 of the Security Officer and proceed with next at the end.

5. The company certificate dialog comes up

Again uncheck Automatically create Certificate and > Press the Import button > Select the saved p12 of the company certificate and proceed with next at the end.

6. Complete the wizard just as normal

7. The policy editor starts. Customized policies and settings must be recreated now. Challenge and response for existing clients will be possible though.
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.
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.