

SOPHOS

SafeGuard® Enterprise 5.50 Web Helpdesk

Document date: April 2010



Content

- 1 SafeGuard Enterprise web-based Challenge/Response 2
- 2 Installation 4
- 3 Authentication..... 9
- 4 Recovery types 11
- 5 Recovery for SafeGuard Enterprise Clients 13
- 6 Recovery using Virtual Clients..... 20
- 7 Recovery for SafeGuard Standalone Clients..... 25
- 8 Technical support..... 29
- 9 Copyright 30

1 SafeGuard Enterprise web-based Challenge/Response

To smoothen the workflow in an enterprise environment and to reduce help desk cost, SafeGuard Enterprise provides a web-based recovery solution. Web Helpdesk offers help to SafeGuard Enterprise users failing to log on to their computers or failing to access encrypted data by providing a user-friendly Challenge/Response mechanism.

1.1 Benefits of Challenge/Response

The challenge/response mechanism is a secure and efficient emergency system to fall back on.

- No confidential data is exchanged in unencrypted form throughout the entire process.
- There is no point in third parties eavesdropping on this procedure because the data spied out cannot be used at any later point in time or on any other devices.
- The user computer to be accessed does not need an online network connection. The Response Code Wizard for the helpdesk also runs on a standalone PC without the need for a complex infrastructure.
- The user can start working again quickly. No encrypted data is lost only because the password has been forgotten.

1.2 Challenge/Response Workflow

During the Challenge/Response procedure a challenge code (an ASCII character string) is generated on the user computer and the user provides this code to a help desk officer. Based on the challenge code the help desk officer then generates a response code which authorizes the user to perform a specific action on the computer.

1.3 Typical emergency situations for requiring helpdesk assistance

- A user has forgotten the password for logging on and the computer has been locked.
- A user has forgotten or lost the token/smartcard.
- The Power-on Authentication local cache is partly damaged.
- A user is not available at the moment due to illness or vacation but the data on the computer must be accessible to a colleague.
- A user wants to access a volume encrypted with a key that is not available on the computer.

SafeGuard Enterprise Web Helpdesk offers different recovery workflows for these typical emergency scenarios enabling the users to access their computers again.

1.4 Scope of Web Helpdesk

Web Helpdesk provides the SafeGuard Enterprise Challenge/Response mechanism through a web based interface. Access control for this web application can be regulated through SSL and gives the helpdesk ways of delegating tasks flexibly within the enterprise. This is achieved without the need to give helpdesk employees access to confidential configuration settings or to the SafeGuard Enterprise central management.

Web Helpdesk is available over the Internet/Intranet without having any SafeGuard Enterprise software installed on the user's computer. The websites need to be separately hosted on an Internet Information Services (IIS) based SafeGuard Enterprise Server.

Web Helpdesk can be run in addition to the SafeGuard Management Center.

Note: We recommend to only make Web Helpdesk available within the Intranet of your enterprise. For security reasons Web Helpdesk should not be put on the Internet.

1.4.1 Web Helpdesk provides recovery for:

- SafeGuard Enterprise Clients
- Virtual Clients
- SafeGuard Standalone Clients

In case of a SafeGuard Enterprise Client, the program dynamically determines if a native Enterprise volume-based encrypted Client or BitLocker encrypted Enterprise Client is in use and adjusts the recovery workflow accordingly.

2 Installation

Web Helpdesk must be installed on an IIS based web server equipped with SafeGuard Enterprise Server. During the Web Helpdesk installation it is checked, whether SafeGuard Enterprise Server is already available on the server and if it is not available, it is automatically installed in a separate Application Pool called “SGNWHD-Pool“. After Web Helpdesk installation you need to configure the web server.

On the Web Helpdesk officer’s computer only a browser needs to be installed.

2.1 Requirements

2.1.1 Server Requirements

Detailed system requirements for the server are described in the Release Notes.

- You need to have Windows administration rights.
- Microsoft Internet Information Services (IIS) must have been installed.
- .NET Framework 3.0 Service Pack 1 with ASP.NET 2.0 must be installed.

2.1.2 Client Requirements

A browser must be installed on the Web Helpdesk officer’s computer. Web Helpdesk supports the following browsers:

- Microsoft Internet Explorer 7.0
- Mozilla Firefox 2 and Firefox 3

Note: We recommend to only make Web Helpdesk available within the Intranet of your enterprise. For security reasons Web Helpdesk should not be put on the Internet.

2.2 Installing Web Helpdesk

You can find the required installation package SGNWebHelpDesk.msi on the product CD.

1. Start SGNWebHelpDesk.msi from the product CD.
2. Click **Next** in the Welcome window.
3. Accept the license agreement.
4. Select an installation path.
5. Confirm the successful installation.

The Web Helpdesk setup checks if SafeGuard Enterprise Server is already available on the IIS web server. If it is not available, SafeGuard Enterprise Server is automatically installed on the IIS web server. Web Helpdesk is then installed on the IIS web server in a separate Application Pool called “SGNWHHD-Pool”.

2.2.1 Configuring the web server with SSL

To enhance security, the IIS web server should be configured in the following way:

1. Deploy Web Helpdesk to the Intranet only.

Make sure to put Web Helpdesk on the Intranet of your enterprise only. For security reasons Web Helpdesk should not be put on the Internet.

2. Establish an SSL connection.

You can limit the availability of Web Helpdesk to defined users using the standard IIS configuration shipped with IIS. Make sure to have SSL Security Certificate installed on the IIS server. Then the whole communication of Web Helpdesk will be carried out via SSL.

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

- a) Certificate Authority must be installed for issuing certificates used by SSL encryption.
- b) A certificate must be issued and the IIS server configured to use SSL and point to the certificate.
- c) The server name specified when configuring the SafeGuard Enterprise Server must be the same as the one specified in the SSL certificate. Otherwise client and server cannot communicate. For each SafeGuard Enterprise Server a separate certificate is needed.

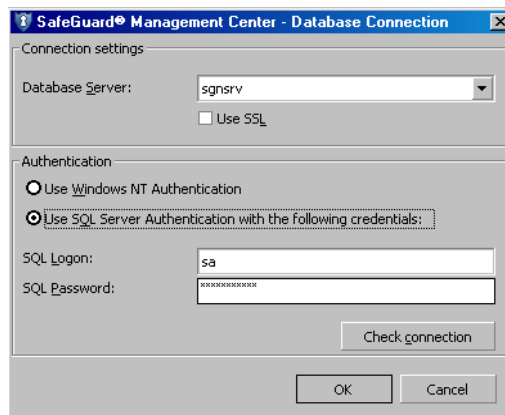
For further information on SSL setup refer to the following links or contact our technical support:

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

2.2.2 Configuring and registering SafeGuard Enterprise Server

If SafeGuard Enterprise Server has not already been installed and registered prior to the Web Helpdesk installation, you need to register the SafeGuard Enterprise Server in the SafeGuard Management Center after Web Helpdesk installation has completed.

1. Start the Management Center and select **Tools > Configuration Package Tool** from the menu bar.
2. Select **Register Server** and click **Add**.
3. Select the server's machine certificate. This is generated when the SafeGuard Enterprise Server is installed. By default it is located in the MachCert directory of the SafeGuard Enterprise Server installation directory. Its file name is <Computername>.cer. If the SafeGuard Enterprise Server is installed on a different PC than the SafeGuard Management, this .cer file must be accessible in the form of a copy or a network permission.
4. The server and its properties are displayed in the **Register Server** tab.
5. Activate **Scripting allowed** to make use of the Scripting API.
6. Click **Database Connections** and then [...] to configure the connection to the database.



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

Use **SQL Authentication** for computers that are not part of a domain, otherwise use Windows NT authentication, this however requires additional configuration. If you use **SQL authentication**, we strongly recommend to secure the connection to the database with SSL to encrypt the transport of the SQL credentials.

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

You can change the properties and settings for any registered server and its database connection at any point in time. Simply ensure to create a new server package afterwards and distribute it to the respective server. After the updated server package is installed on the server, the new database connection can be used.

7. Switch to the **Create Server Package** tab.
8. Select the required server.
9. Specify the output path.
10. Click **Create Server MSI**. An .msi file named <Server>.msi is created under the output path.
11. Run this new .msi configuration file on the SafeGuard Enterprise Server.

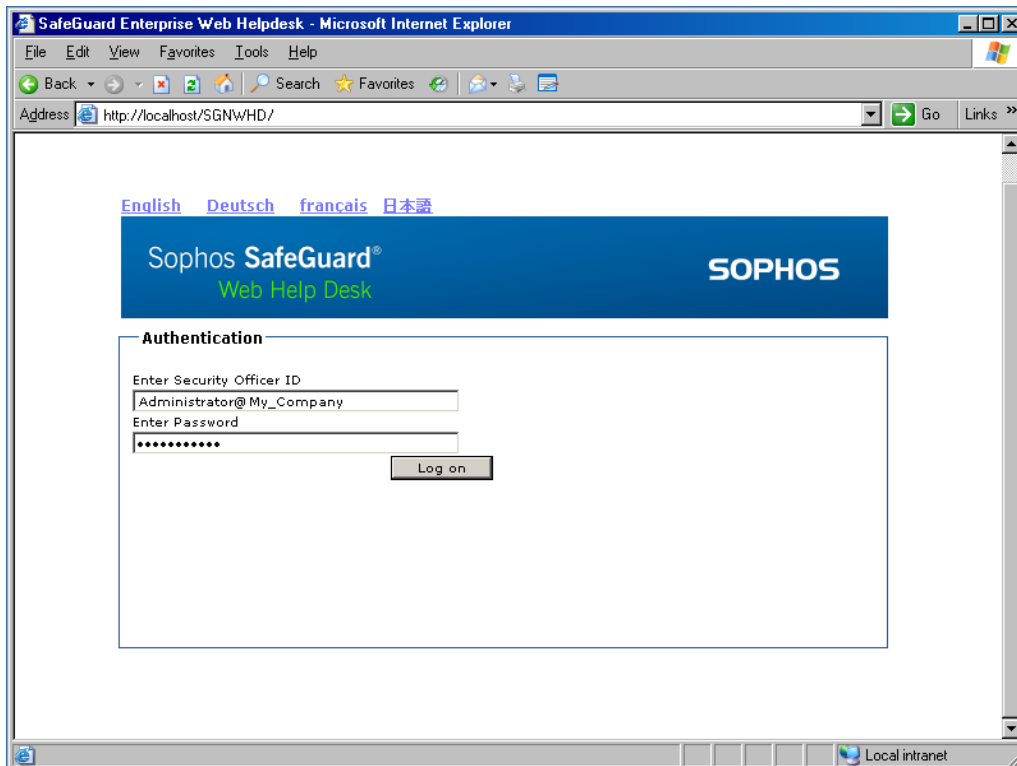
The computer is registered as SafeGuard Enterprise Server.

2.3 Updating Web Helpdesk

When updating Web Helpdesk to the latest version, it is recommended to uninstall Web Helpdesk and to install the latest version of Web Helpdesk afresh. The server configuration package needs only to be created afresh, if any server settings need to be updated.

2.4 Language support

Web Helpdesk supports several languages. You can dynamically change the language of the application in the Web Helpdesk Logon screen. Click the desired language and the application will be displayed in the requested language immediately.



3 Authentication

Security officers need to authenticate at Web Helpdesk and against the SafeGuard Enterprise Server in order to be able to use the web-based recovery wizard. Security officers log on to Web Helpdesk with their security officer ID and their password which are equivalent to their Windows credentials.

Only users who have been promoted to security officer in the SafeGuard Management beforehand are able to access Web Helpdesk.

3.1 Preparations in the SafeGuard Management Center

For access to be granted to Web Helpdesk the following prerequisites need to be fulfilled and the following preparations need to be taken in the SafeGuard Management Center. For detailed information see the SafeGuard Enterprise Administrator's Manual.

1. Web Helpdesk users must have been imported from an Active Directory into the SafeGuard Enterprise database.
2. User certificates must have been assigned to these users or imported for them and the certificates (.p12 file) must be available in the database.
3. Future Web Helpdesk users must then be promoted to security officers.

The promoted security officers can then log on to Web Helpdesk with their defined security officer ID, which is a combination of their Windows user name and the name of the domain assigned to them. The password required is the Windows password protecting their certificates.

4. Security officers need to have the role Helpdesk Officer assigned to them in order to be able to authenticate at Web Helpdesk.

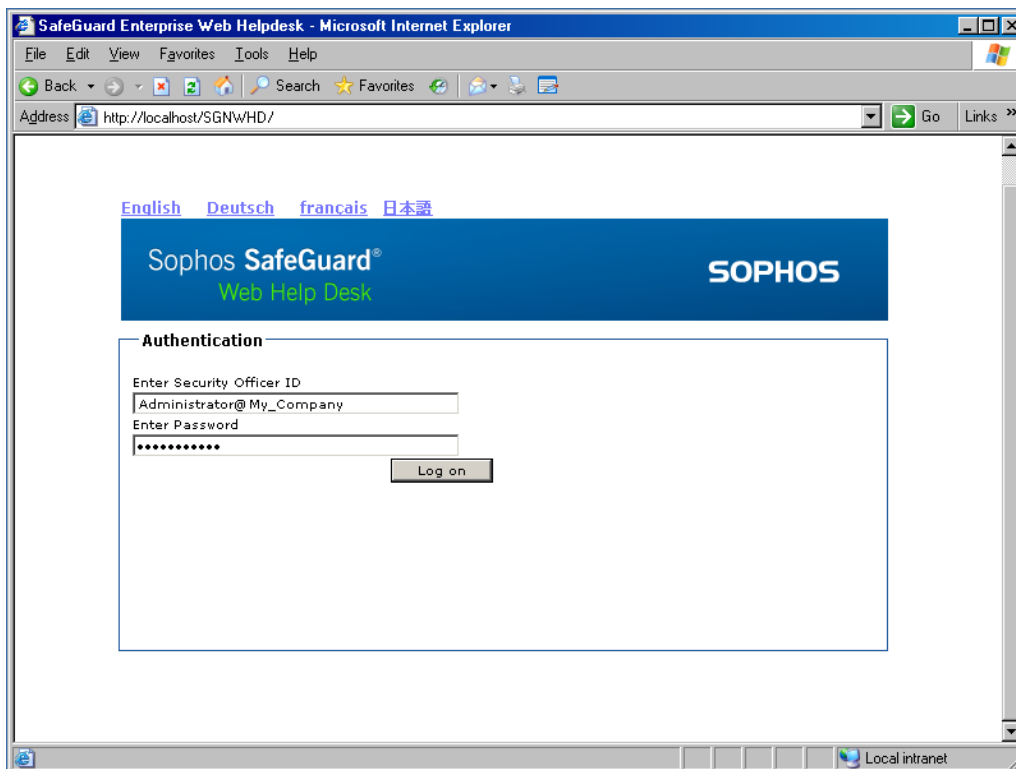
The prerequisites for a successful authentication at Web Helpdesk are fulfilled.

Note: As Web Helpdesk security officers need to authenticate against the SafeGuard Enterprise Server, authentication via token is not supported in Web Helpdesk.

3.2 Logging on to Web Helpdesk

Do the following:

1. Start your browser.
2. Call the application in your browser by entering the URL: `https://<Host-ID oder IP-Adresse>/SGNWHD`



3. In the welcome screen, enter your security officer ID exactly as defined in the SafeGuard Management Center, in the following way: `<user name>@<DOMAIN>` for example `WHDOFFICER@MYDOMAIN`.

Please note that the entry is case-sensitive, so make sure that the user name is spelled correctly. A list of user names will not be provided in order to hide the information from unauthorized users.

4. Enter your password. The required password is your Windows password.
5. Click **Log on**.

The Web Helpdesk recovery wizard is started.

4 Recovery types

The following Recovery types are provided:

■ SafeGuard Enterprise Clients

User computers that are centrally managed by the SafeGuard Management Center. They are listed in the Users & Computers area in the SafeGuard Management Center.

■ Virtual Clients

Easy recovery for encrypted volumes can even be achieved in cases where Challenge/Response would usually not be supported, for example when the POA is corrupted.

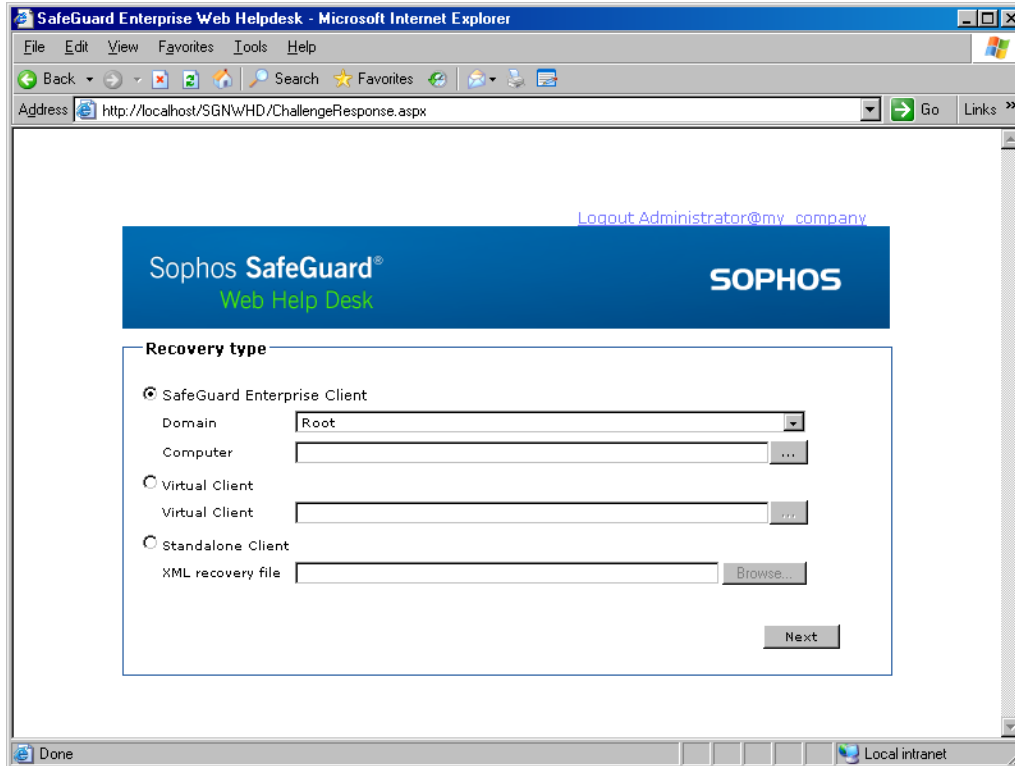
To enable a Challenge/Response procedure in this situation, specific files called Virtual Clients can be created and distributed to the user prior to the Challenge/Response session. Challenge/Response can then be initiated on the user computer with the help of these Virtual Clients via the key recovery tool RecoveryKeys.exe from the product CD. The user then only needs to inform the helpdesk officer of the required keys and enter the response code in order to regain access to the encrypted volumes.

■ Sophos SafeGuard Standalone Clients

User computers that are locally managed. They never have any connection to the SafeGuard Enterprise Server. For each SafeGuard Standalone Client a recovery file (.xml file) is generated during configuration. It contains the defined machine key which is encrypted with the company certificate. If this recovery key file is available, e.g. on a memory stick or via a shared network path so that the help desk officer can access it, Challenge/Response for a SafeGuard Standalone Client is supported.

4.1 Selecting the recovery type

After successfully having logged on to Web Helpdesk, you can select which type of recovery is requested.



5 Recovery for SafeGuard Enterprise Clients

SafeGuard Enterprise offers recovery for Enterprise Clients registered in the database in various disaster scenarios, such as password recovery or accessing data by booting from external media.

Challenge/Response is supported for both SafeGuard Enterprise native clients or BitLocker encrypted clients. During Challenge/Response it is dynamically determined which type of Enterprise Client is in use and the recovery workflow is adjusted accordingly.

5.1 Recovery actions for SafeGuard Enterprise Clients

The recovery workflow depends on which type of Enterprise Client recovery is requested for.

Note: For BitLocker encrypted computers the only recovery action is to recover the key used to encrypt a specific volume. No password recovery is provided.

5.1.1 Recovering the password at POA level

One of the most common scenarios is that users have forgotten their password. By default SafeGuard Enterprise is installed with an activated Power-on Authentication (POA). The POA password for accessing the computer is the same as the Windows password.

If the user has forgotten the password at POA level, the helpdesk officer can generate a response for **Booting SGN client with user logon**, but without displaying the user password. However, in this case, after entering the response code the computer will boot into the operating system, so the user has to change the password at Windows level, subject to the condition that the domain is accessible. The user can then log on to Windows as well as to the Power-on Authentication with the new password.

Best practice for recovering the password at POA level

Note: Note: We recommend to primarily use the following methods when the user has forgotten their password to avoid that the password has to be centrally reset:

Use Local Self Help. With recovery via Local Self Help the user can have the current password displayed and may continue using this password without having to reset it and without any help desk assistance. For further information see the Administrator help.

When using Challenge/Response: We recommend avoiding centrally resetting the password in the Active Directory prior to the Challenge/Response procedure. Avoiding this will ensure that the password remains synchronized between Windows and SafeGuard Enterprise. Ensure that the Windows help desk is educated accordingly.

As a SafeGuard Enterprise help desk officer, generate a response for **Booting SGN client with user logon** with option **Display user password**. This is advantageous as the password then does not have to be reset in the Active Directory. The user may continue working with the old password and change it locally afterwards, if desired.

5.1.2 Displaying the user password

SafeGuard Enterprise offers users to have their password displayed during Challenge/Response. This is advantageous as the password then does not have to be reset in the Active Directory. The option is only available if **Booting SGN client with user logon** is requested.

5.1.3 Accessing data by booting from external media

Challenge/Response can also be used to allow a computer to be booted from external media such as WinPE. To do so, the user has to select **Continue Booting from: Floppy Disk/External Medium** in the POA logon dialog and initiate the Challenge. When receiving the response the user can enter the credentials in the POA as usual and continue booting from external medium.

The following requirements must be fulfilled to access an encrypted volume:

- The device to be used must contain the SafeGuard Enterprise filter driver. See the knowledge database on how to obtain such a driver CD:
<http://www.sophos.com/support/knowledgebase/article/108805.html>.
- The user must boot from external medium and must have the right to do so. This right can be granted to them by defining a policy in the SafeGuard Management Center and assigning it to the client (policy **Authentication > Access: User may only boot from hard disk** must be set to **No**). By default the right to boot from external media is not assigned.
- The user computer must generally support booting from different media other than a fixed hard drive.
- Only volumes encrypted with the defined machine key can be accessed. This key encryption type can be defined in a device encryption policy in the Management Center and assigned to the client.

Note: Please note that using external media such as a WinPE to access an encrypted drive will only partly allow access to the volume.

5.1.4 Restoring the SafeGuard Enterprise policy cache

This procedure is necessary, if the SafeGuard policy cache is damaged. In this case the user will automatically be prompted to initiate a Challenge/Response procedure when logging on to the Power-on Authentication.

5.2 Creating a Response for SafeGuard Enterprise Clients

To generate a response during Challenge/Response for a SafeGuard Enterprise Client, the name of the respective user computer and the domain are required.

Note: This name must always be the distinguished name of the computer.

1. In the **Recovery type** window select **SafeGuard Enterprise Client**.
2. Select the required domain from the list.
3. Enter the required computer name. There are several possibilities to do so:
 - Select a name by clicking [...] and then **Search** in the pop-up window. A list of computers is displayed. Select the required computer and click **OK**. The computer name is then displayed in the **Recovery type** window below **Domain**.
 - Enter the short name of the computer. When clicking **Next**, the database is searched for this name and if found, the distinguished computer name is displayed.
 - Enter the computer name directly in distinguished name format, for example:
CN=Desktop1,OU=Development,OU=Headquarter,DC=Utimaco,DC=edu
4. Click **Next**.

The program then dynamically determines if a native SafeGuard Enterprise computer or BitLocker encrypted computer is in use and adjusts the recovery workflow accordingly. In case of a native SafeGuard Enterprise computer the next step requires the selection of the user information. In case of a BitLocker encrypted computer the next step requires the selection of the volume to be decrypted.

5.2.1 Creating a Response for native SafeGuard Enterprise Clients

In case of a native SafeGuard Enterprise Client the database is checked for the respective computer. Then the corresponding user name and domain need to be selected for recovery of a SafeGuard Enterprise Client.

1. In **Domain** select the required domain of the user. In case of a local user select **Local user on <computer name>**.
2. Enter the required user name. There are several possibilities to do so:
 - Select the user name by clicking [...] and then **Search** in the pop-up window. A list of user names is displayed. Select the required name and click **OK**.
 - Enter the name of the user directly. Make sure the name is spelled correctly.

SafeGuard Enterprise Web Helpdesk - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites Go Links >>

Address http://localhost/SGNWHDD/ChallengeResponse.aspx

Logout Administrator@my_company

Sophos SafeGuard® Web Help Desk SOPHOS

User

Domain DC=My_Company,DC=edu

User CN=Administrator,CN=Users,DC=My_Company,DC=edu

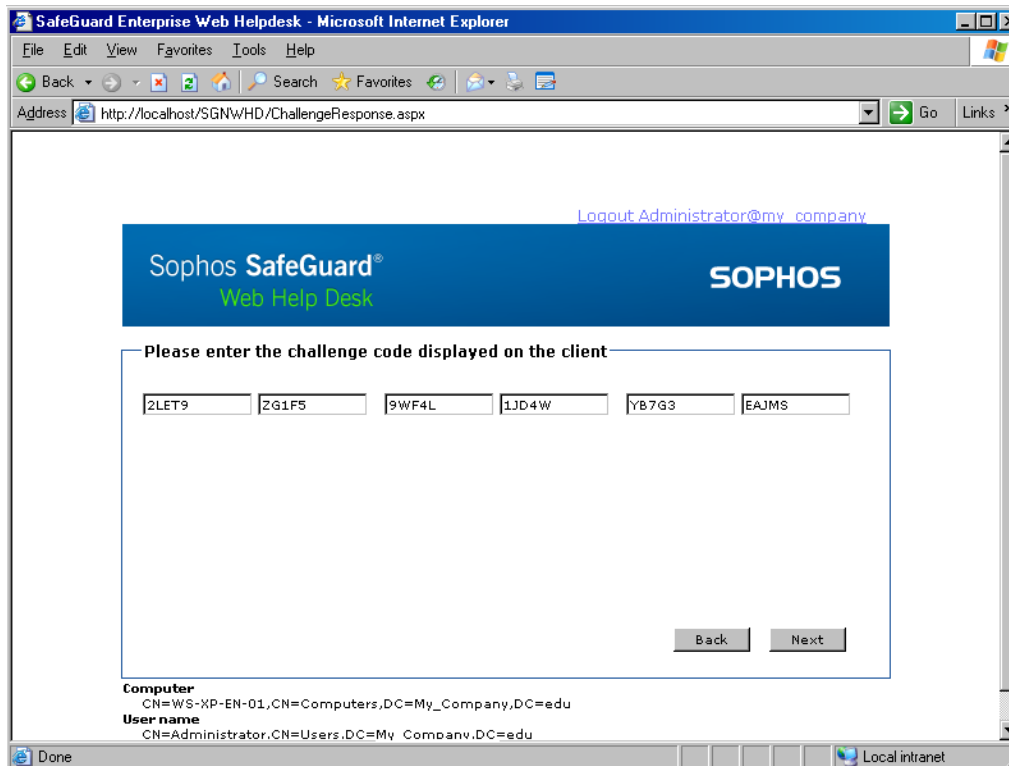
Back Next

Computer

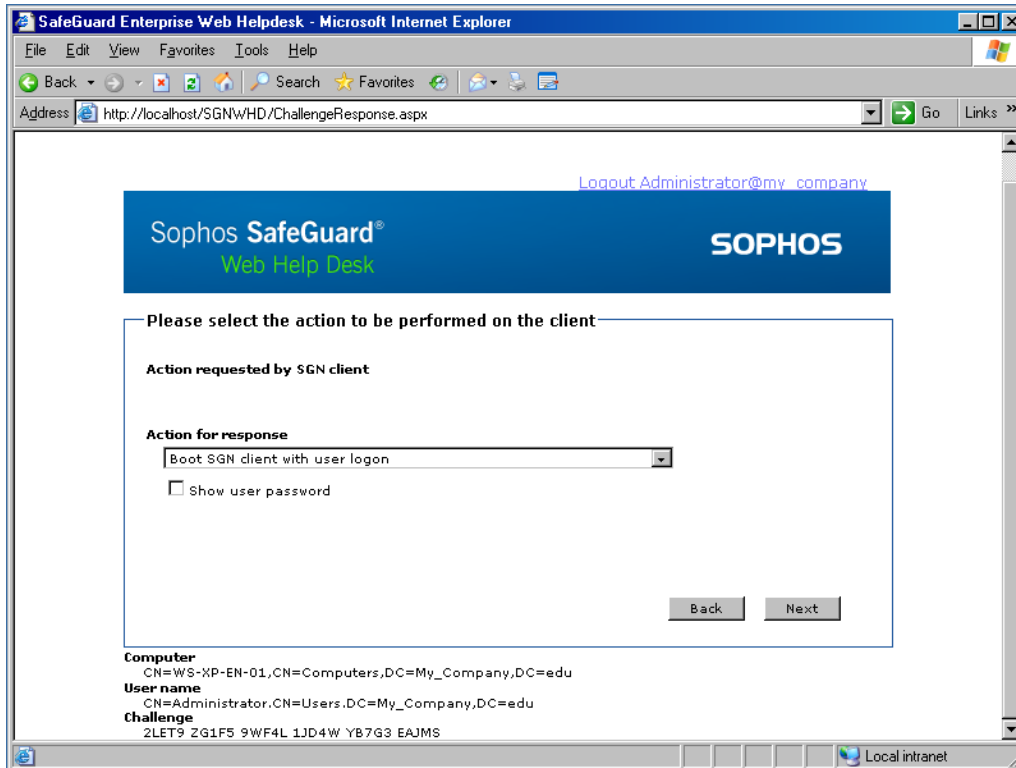
CN=WS-XP-EN-01,CN=Computers,DC=My_Company,DC=edu

Done Local intranet

3. Click **Next**. A window is displayed where you can enter the challenge code.
4. Enter the challenge code the user has passed on to you and click **Next**. The challenge code is verified. If the code has been entered incorrectly, Invalid is displayed below the block containing the error.

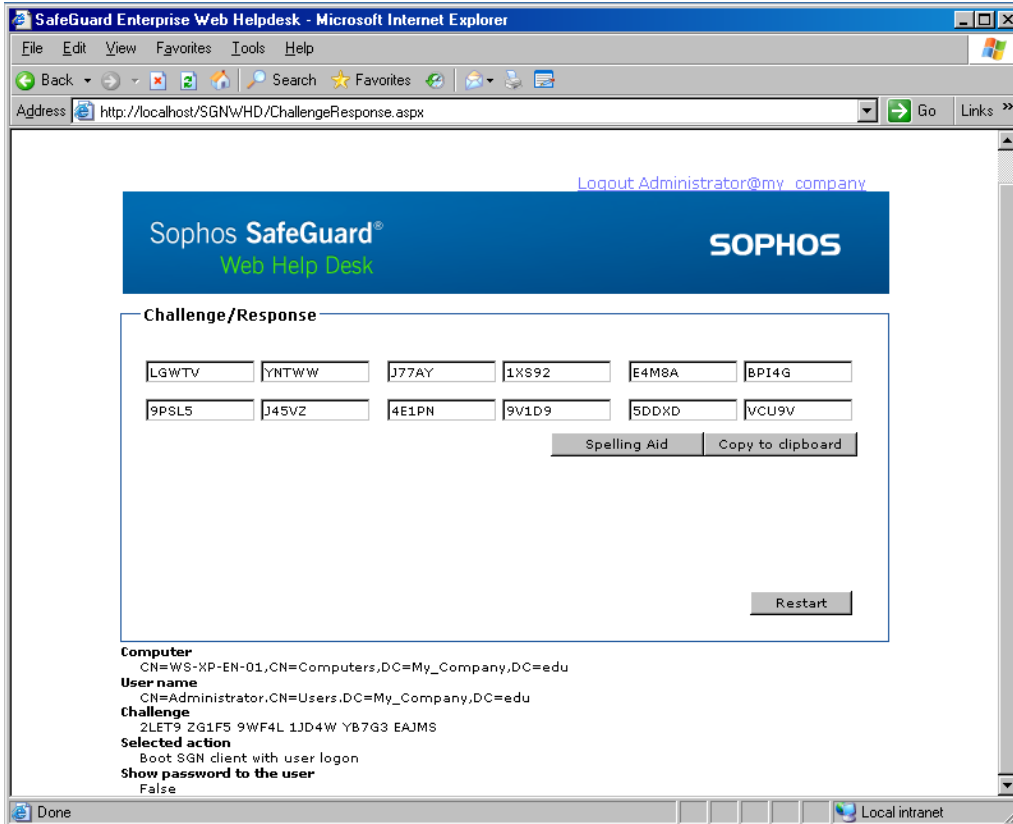


5. If the challenge code has been entered correctly, the recovery action requested by the SafeGuard Enterprise Client as well as the possible recovery actions on the client are displayed. The possible actions for response depend on the actions requested on the client side when calling the challenge. For example, if **Crypto token requested** is required on the client side, the available actions for response are **Boot SGN client with user logon** and **Boot SGN client without user logon**.



6. Select the action the user needs to perform.
7. If **Booting SGN client with user logon** has been selected as response action, you may additionally select **Show user password** to have the password displayed on the target computer.
8. Click **Next**. A response code is generated.

9. Read the response code to the user. A spelling aid is provided. You can also copy the response code to the clipboard.



The user can then enter the response code on the user computer and perform the authorized action.

5.2.2 Creating a Response for BitLocker protected SafeGuard Enterprise Clients

For BitLocker protected SafeGuard Enterprise Clients a volume that cannot be accessed any more may be recovered. The database is checked for the respective computer. Then the required volume needs to be selected for recovery of a BitLocker encrypted computer.

1. Select the volume to be accessed from the list and click **Next**. Web Helpdesk then displays the corresponding 48-digit recovery key.
2. Read this key to the user.

The user can then enter the key to recover access to the BitLocker encrypted volume on their computer.

6 Recovery using Virtual Clients

With Virtual Client recovery SafeGuard Enterprise offers recovery of encrypted volumes even in complex disaster situations.

Recovery using Virtual Clients may be applied in the following typical situations:

- The Power-on Authentication is corrupted.
- A volume is not encrypted with the computer's defined machine key but with a different key. The necessary key is not available in the user's environment. It must therefore be identified in the database and transferred to the computer in a secure way.

Note: Virtual Client recovery should only be used to resolve complex disaster situations: If both of the above mentioned issues apply, a Virtual Client recovery is appropriate. If, however only a key is missing to recover a volume, the best way to recover the volume would simply be to assign the missing key to the respective user's key ring.

In these situations SafeGuard Enterprise offers the following solution:

To enable a Challenge/Response procedure in this situation, specific files called Virtual Clients can be created in the SafeGuard Management Center and distributed to the user prior to the Challenge/Response session. Challenge/Response can then be initiated on the user computer with the help of the Virtual Client files via the key recovery tool RecoverKeys.exe from the product CD and a SafeGuard Enterprise modified WinPE CD. The helpdesk officer then selects the required keys and generates a response code. Access to the encrypted volumes is enabled when the user enters the response code, as the required keys are being transferred within the response.

6.1 Recovery using Virtual Clients: Workflow

Note: For a detailed description of the workflow see the SafeGuard Enterprise Administrator's manual.

Do the following:

1. The helpdesk officer needs to create the Virtual Client in the **Keys & Certificates** area of the SafeGuard Management Center and export them to a file. This file, called recoverytoken.tok must be distributed to the users and must be available to them prior to the Challenge/Response session.
2. The user can then start a SafeGuard Enterprise recovery CD or any other CD with a SafeGuard Enterprise modified WinPE on their computer from BIOS without any POA logon and initiate a Challenge/Response session with a key recovery tool.

As reference in the SafeGuard Enterprise database the Virtual Client file is used and stated in the challenge instead of the user/computer name which is not available in this case.

3. The user's key recovery tool then tells the user which volumes are encrypted and which keys are used for each of these volumes. The user will present this information to the helpdesk officer.
4. The helpdesk officer will identify the Virtual Client in the database and select the required key for accessing the encrypted volumes: either a single key or several keys exported to a key file. The help desk officer will then generate the response code.
5. The user enters the response code. Within the response code the required keys are transported. By entering the response code and restarting the computer the user can then reaccess the encrypted volumes again.

6.2 Recovery actions using Virtual Clients

In order to access the volumes encrypted with keys that are not available to the user, the correct encryption key/keys must be transferred from the database to the user's environment.

Challenge/Response therefore covers two actions using virtual clients:

- transferring a single key
- transferring several keys in an encrypted key file

6.2.1 Transferring a single key

Challenge can be initiated to recover a single key for accessing an encrypted volume. The helpdesk officer must select the necessary key in the database and generate a response code. The key is encrypted and transferred to the user computer by entering the response code. If the response code was correct, the transferred key will be imported to the local key store. After that, all volumes that are encrypted using this key can be accessed.

6.2.2 Transferring several keys in an encrypted key file

Challenge can be initiated to recover multiple keys for accessing encrypted volumes. The keys are stored in one file which is password encrypted. A prerequisite for this is that the helpdesk officer exports one or more required keys to be stored in a file. This file is encrypted with a random password, which is stored in the database. The password is unique for each created key file.

The encrypted key file needs to be transferred to the user environment and must be available to the user. In order to decrypt this key file the user will then have to initiate Challenge/Response via the key recovery tool RecoverKeys.exe during which the password is transferred to the target computer. The helpdesk officer will generate a response and select the respective password to decrypt the key file. The password is passed on to the target computer within the response code. The key file can then be decrypted with the password.

The keys in the key file will be imported into the key storage on the user computer and all volumes encrypted with the available keys can be accessed again.

Note: With Web Helpdesk, a key file and the corresponding password are deleted in the database after having once been successfully used in a Challenge/Response session. In this case you therefore have to create a new key file and password after every successful Challenge/Response session.

6.3 Response using Virtual Clients

To create a response using Virtual Clients the following prerequisites must be met.

6.3.1 Prerequisites

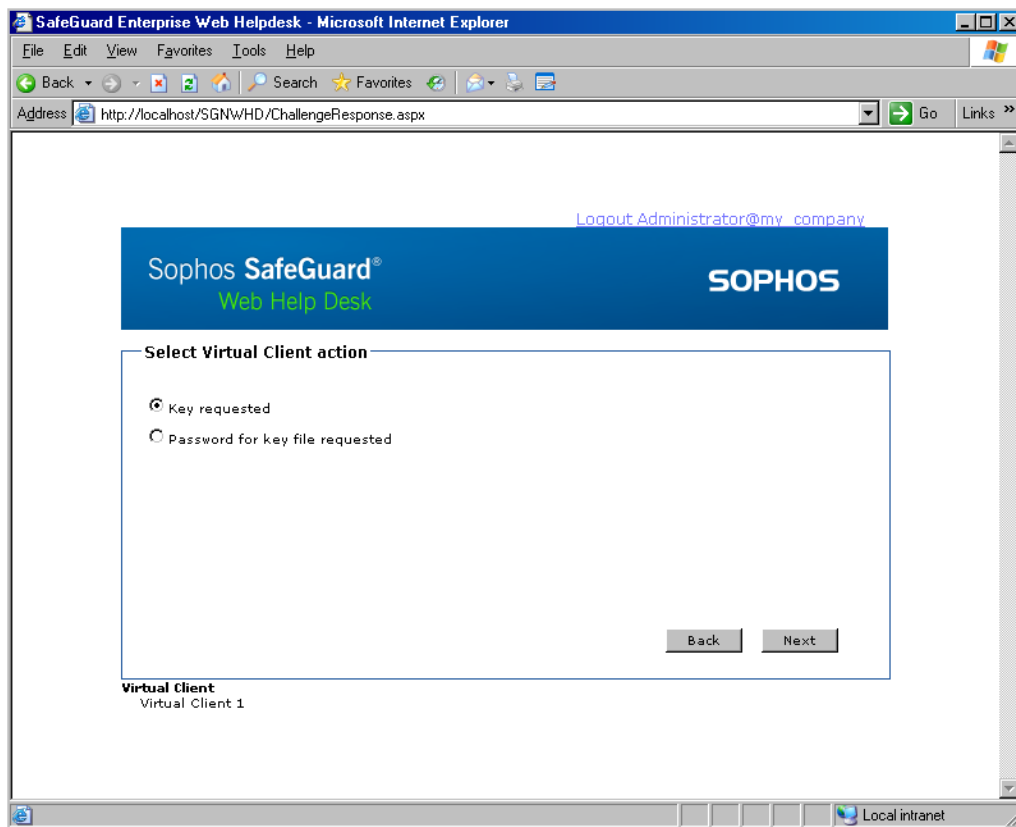
The following prerequisites must be met:

- The Virtual Client must have been created in the SafeGuard Management Center in **Keys & Certificates**. See the Administrator's manual for further information.
- The helpdesk officer must be able to locate the Virtual Client in the database. Virtual Clients are identified uniquely by their names.
- The Virtual Client file **recoverytoken.tok** must be available to the user. This file must be stored in the same folder as the key recovery tool. We recommend storing this file on a memory stick.
- When recovery for several keys is requested, the helpdesk officer must have created a key file containing the necessary recovery keys in the SafeGuard Management Center in **Keys & Certificates** beforehand. The key file must be available to the user before a recovery to take effect. The password encrypting this key file must be available in the database. See the SafeGuard Enterprise Administrator's manual for further information.
- The user must have started the key recovery tool and must have initiated the Challenge/Response session.
- A response can only be initiated for assigned keys. If a key is inactive, i.e. the key is not assigned to at least one user, a Virtual Client Response is not possible. In such a case the inactive key can be reassigned to any other user and a response for this key can be generated again.

6.3.2 Creating a Response using Virtual Clients

Do the following:

1. As a Helpdesk Officer select **Virtual Client** in the **Recovery type** window.
2. Enter the name of the Virtual Client the user has given to you. There are different ways to do so:
 - Enter the unique name directly.
 - Select a name by clicking [...] and then **Search** in the pop-up window. A list of virtual clients is displayed. Select the required one and click **OK**. The name of the Virtual Client is then displayed in the **Recovery type** window in **Virtual Client**.
3. Click **Next**. The window where you can select the recovery action will be displayed.



4. Select the recovery action to be taken by the user and then click **Next**.
 - If you need to transfer a single recovery key only, select **Key requested**. select the respective key from the list. Click [...]. You can either display the keys by key ID or by symbolic name. Click **Search**, select the key and click **OK**.
 - If the user needs a key file containing several keys for recovery, select **Password for key file requested** to transfer the password for the encrypted key file to the user. Select the required key file. Click [...] and then **Search**. Select the key file and click **OK**.

Password for key file selected can only be selected when a key file has previously been created in the SafeGuard Management Center in **Keys & Certificates** and the password encrypting the key file has been stored in the database. With Web Helpdesk, key files and the corresponding passwords are deleted in the database after having once been successfully used in a Challenge/Response session. In this case you therefore have to create a new key file and password after every successful Challenge/Response session

5. Click **Next**. The window to enter the challenge code is displayed.
6. Enter the challenge code the user has passed on to you and click **Next**. The challenge code is verified. If the code has been entered incorrectly, Invalid is displayed below the block containing the error.
7. If the challenge code has been entered correctly, the response code is generated. Read the response code to the user. A spelling aid is provided. You can also copy the response code to the clipboard.
 - If a single key is requested the generated key is transferred within the response code.
 - If a password for the encrypted key file is requested it is transferred within the response code. The key file then is deleted.
8. The user must enter the response code on the user computer.
9. The user needs to restart the computer and log on again to access the respective volumes.

The volumes can be accessed again.

7 Recovery for SafeGuard Standalone Clients

SafeGuard Enterprise also provides Challenge/Response for SafeGuard Standalone Clients. SafeGuard Standalone Clients never have any connection to the SafeGuard Enterprise Server. They operate in standalone mode and are locally managed. As they are not registered in the SafeGuard Enterprise database no information on their identification needed for a Challenge/Response is available.

Challenge/Response for SafeGuard Standalone Clients is therefore based on the recovery key file created during the configuration of the Standalone Client. The recovery file (.xml file) is generated for each Standalone Client and contains the defined machine key which is encrypted with the company certificate. This file needs to be stored in a location a helpdesk officer is able to access during Challenge/Response. When the helpdesk officer is able to access the respective recovery file, for example via a memory stick or a shared network path, a response can be generated.

7.1 Recovery actions for SafeGuard Standalone Clients

Challenge/Response for a SafeGuard Standalone Client must be initiated in the following situations:

- The user has entered the password incorrectly too often.
- The user has forgotten the password.
- A corrupted cache needs to be repaired.

For a SafeGuard Standalone Client no user key is available in the database. Therefore, the only recovery action possible in a Challenge/Response session is **Booting SGN client without user logon**.

The Challenge/Response procedure will enable the user to log on at the Power-on Authentication. The user will also be enabled to log on to Windows, even if the Windows password needs to be reset.

7.1.1 The user has entered the password incorrectly too often

As in this case resetting the password is not needed, Challenge/Response procedure will enable the user log on to the Power-on Authentication. The user can then enter the correct password at Windows level and use the computer again.

7.1.2 The user has forgotten the password

Note: We recommend to primarily use Local Self Help to recover a forgotten password. With recovery via Local Self Help the user can have the current password displayed in a confidential way in the Power-on Authentication and may continue using this password. This will avoid that the password has to be reset at all and will also avoid help desk assistance. For further information, see the Administrator help.

When recovering a forgotten password via Challenge/Response a password reset is required.

1. The Challenge/Response procedure will enable the computer to boot through Power-on Authentication.
2. In the Windows logon dialog, the user does not know the correct password either and therefore needs to change it at Windows level. This requires further recovery actions outside the scope of SafeGuard Enterprise, via standard Windows means. We recommend using the following methods to reset the password at Windows level.
 - Via a service or administrator account available on the computer with the required Windows rights.
 - Via a Windows password reset disk.

As a help desk officer you may inform the user which procedure should be used and either provide the additional Windows credentials or the required disk.

3. The user enters the new password at Windows level that the help desk has provided. The user then changes this password immediately to a value only known to the user.
4. SafeGuard Enterprise detects that the newly chosen password does not match the current SafeGuard Enterprise password used in the POA. The user is therefore prompted to enter the old SafeGuard Enterprise password and, since the user has forgotten this password, needs to click **Cancel**.
5. In SafeGuard Enterprise, the definition of a new password without providing the old one requires a new certificate. The user has to confirm this procedure.
6. A new user certificate will be created based on the newly chosen Windows password. This enables the user to log on to the computer again and to log on at the Power-on Authentication with the new password.

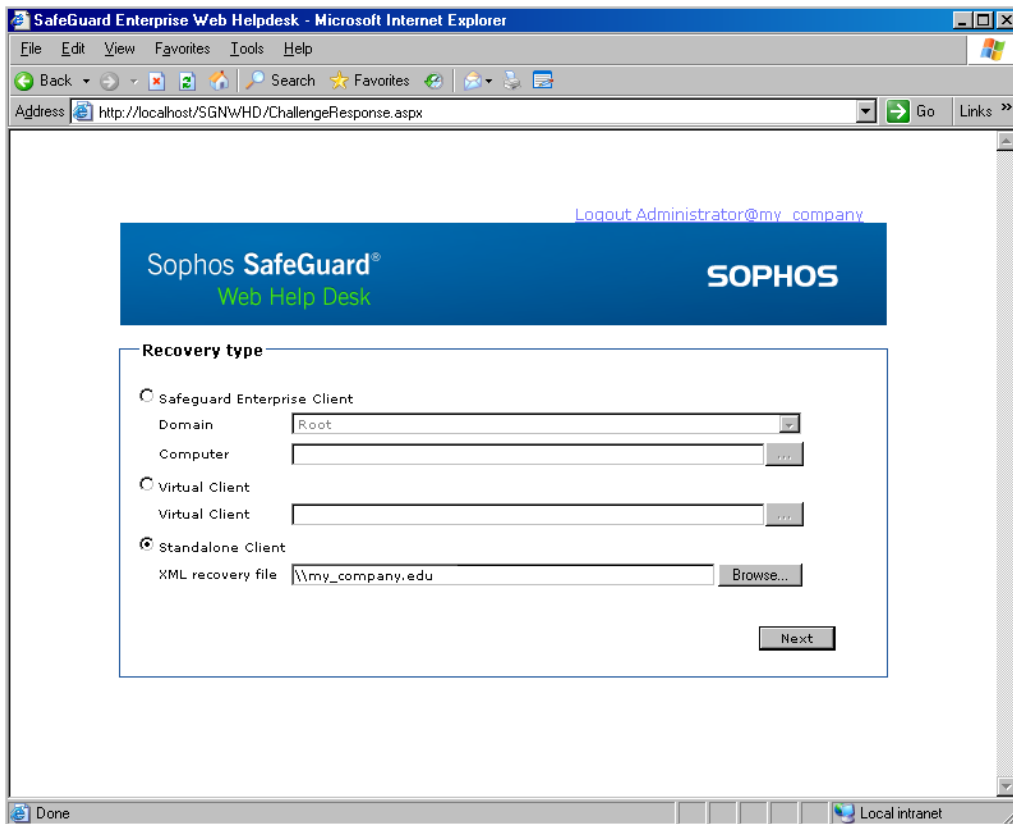
Keys for SafeGuard Data Exchange

When the user has forgotten the Windows password and it has been reset, the user will not be able to use the keys already created for SafeGuard Data Exchange without the corresponding passphrase. To be able to continue using the already generated user keys for SafeGuard Data Exchanges the user has to remember the SafeGuard Data Exchange passphrases to reactivate these keys.

7.2 Creating a Response for SafeGuard Standalone Clients

To generate a response during a Challenge/Response session for a Standalone Client, the name of the recovery file (.xml file) is required.

1. As a Helpdesk Officer select **Standalone Client** in the **Recovery type** window.
2. Select the required recovery file (.xml file) by clicking **Browse**.



3. You are asked to enter the challenge code the user has passed on to you.
4. Select the required action to be taken by the user and then click **Next**.
5. A response code is generated. Read the response code to the user. A spelling aid is provided.
You can also copy the response code to the clipboard.

The user can enter the response code and is able to reaccess the computer.

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 Copyright

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

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

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

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

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