SOPHOS

Security made simple.

SafeGuard Enterprise

Web Helpdesk

Product version: 7

Document date: December 2014

Contents

1 SafeGuard web-based Challenge/Response

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

Additionally, the SafeGuard Configuration Protection policy can be suspended.

Benefits of Challenge/Response

The challenge/response mechanism is a secure and efficient emergency system.

- 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 cannot be used at a later stage or on any other devices.
- The endpoint that is 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 just because the password has been forgotten.

Challenge/Response workflow

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

Typical emergency situations requiring helpdesk assistance

- A user has forgotten the password for logging on and the endpoint has been locked.
- A user has forgotten or lost their 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 endpoint must be accessible to a colleague.
- A user wants to access a volume encrypted with a key that is not available on that endpoint.

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

2 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 helpdesk endpoint. 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 that you only make Web Helpdesk available on the intranet of your enterprise. For security reasons Web Helpdesk should not be put on the internet.

Web Helpdesk provides recovery for:

- SafeGuard encrypted endpoints (managed SafeGuard Enterprise clients)
- Virtual Clients
- SafeGuard encrypted endpoints (unmanaged SafeGuard Standalone clients)

3 Installation

Web Helpdesk must be installed on an IIS based web server equipped with SafeGuard Enterprise Server. If SafeGuard Enterprise Server is not available, the user is prompted to install it. 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.

3.1 Requirements

Server Requirements

Detailed system requirements for the server are described in the release notes.

- Make sure that you have Windows administration rights.
- Microsoft Internet Information Services (IIS) must be installed.
- .NET Framework 4 with ASP.NET 4 must be installed.
- For Windows Server 2012: The ASP.NET role must be installed (Server Roles > Web Server (IIS) > Web Server > Application Development > ASP.NET 4.5).

Note: For Windows Server 2012 the following applies: ASP.Net applications come pre-wired with a handlers section in the web.config. Within feature delegation in IIS this is set to read only. In the IIS Manager, check under the server name > feature delegation. If the handler mappings are set to read only and your site web.configs have a handlers section, change the value to read/write.

Endpoint Requirements

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

- Microsoft Internet Explorer 7 and above
- Mozilla Firefox 2 and above

3.2 Install Web Helpdesk

You can find the required installation package SGNWebHelpDesk.msi in your product delivery.

1. Double-click SGNWebHelpDesk.msi. A wizard guides you through installation. Accept the default values wherever possible. Select a **Complete** installation if prompted.
2. When installation is complete, you may be prompted to restart. Click **Yes** or **Finish**.

The Web Helpdesk setup checks if SafeGuard Enterprise Server is already available on the IIS web server. If it is not available, you are prompted to install it.

3.2.1 Configure the web server with SSL

To enhance security, configure the IIS web server as follows:

1. Deploy Web Helpdesk to the intranet only.

   Make sure that you put Web Helpdesk on the intranet of your enterprise only. For security reasons, do not put Web Helpdesk 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 that you have SSL Security Certificate installed on the IIS server. Then all communications with Web Helpdesk will be carried out using SSL.

   The following general tasks must be carried out to set 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.

   d) The worker processes for the application pool **`SGNWHD-Pool`** must not be increased to more than 1 (default). Otherwise authorization to Web Helpdesk will fail.

For further information, contact our technical support or see:

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

3.2.2 Register and configure SafeGuard Enterprise Server

If SafeGuard Enterprise Server has not already been installed and registered before installing Web Helpdesk, you need to register the SafeGuard Enterprise Server in the SafeGuard Management Center.

1. Start the SafeGuard Management Center.
2. On the **Tools** menu, click **Configuration Package Tool**.
3. Select **Servers** tab and then click **Add...**.

4. In **Server Registration** click **[...]** to select the server's machine certificate. This is generated when the SafeGuard Enterprise Server is installed. By default it is located in the **`MachCert`** directory of the SafeGuard Enterprise Server installation directory (file name**`<Computername>.cer)`**. If the SafeGuard Enterprise Server is installed on a different computer from the SafeGuard Management Center, this **`.cer`** file must be accessible by a network permission or its copy must be made available.

   Do not select the MSO certificate.

   The FQDN, for example **`server.mycompany.com`** and certificate information, is displayed.

   If you use SSL as transport encryption between endpoint and the SafeGuard Enterprise Server, the server name specified here must be identical to the one specified in the SSL certificate. Otherwise, they cannot communicate.

5. Click **OK**.

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

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

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

7. Click **OK** to confirm the success message.
8. In the **Servers** tab, click **Close**.

SafeGuard Enterprise Server is registered and configured. Next, install the server configuration package (MSI) on the computer running the SafeGuard Enterprise Server. You can change the server configuration in the **Servers** tab any time.

Note: If you want to install a new server configuration package (MSI) on the SafeGuard Enterprise Server, make sure that you uninstall the outdated server configuration package before installing a new one.

3.3 Update Web Helpdesk

When updating Web Helpdesk to the latest version, we recommend that you uninstall Web Helpdesk and then install the latest version of Web Helpdesk. You only need to create a new server configuration package if any server settings have been updated.

3.4 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 is displayed in the requested language immediately.

4 Allow Web Helpdesk logon for users without SafeGuard Enterprise client installed

It is possible to use Web Helpdesk without having a SafeGuard Enterprise client installed.

Access rights can be managed by adding or removing Windows users or groups.

Note:

This feature makes use of Windows Authentication. If Windows Authentication is enabled, traditional login via a promoted Active Directory user is no longer possible.

4.1 Prerequisites for logon without SafeGuard Enterprise client

The following prerequisites must be met:

1. A Windows user group must be set up and configured containing users who are allowed to access Web Helpdesk (see *SafeGuard Enterprise Administrator help* for more information).
2. Windows Authentication at the Web Helpdesk must be enabled (**Tools - Configuration Package Tool - "Servers" tab - Win. Auth. WHD**, see *SafeGuard Enterprise Installation guide* for more information).

4.2 Enable Windows Authentication for SafeGuard Web Helpdesk application

1. Open the Internet Information Services (IIS) Manager window.
2. Under **Sites** > **Default Web Site**, select the user node, for example SGNWHD.
3. Select **Authentication**.
4. Select the entry name **Windows Authentication** in the list of authentications.
5. Click **Enable** on the **Actions** bar on the right-hand side.
6. Then, select **.NET Authorization rules** to add three .NET authorization rules.

   Note: In Windows 2008 Server, there is no icon in the IIS for **.Net Authorization Rules**. There is an **Authorization Rules** link. To be able to edit those rules, the **URL Authorization** role should be installed by using **IIS** > **Security** > **URL Authorization**.

7. On the **Actions** bar, click **Add Deny Rule...**.
8. A dialog is opened. Deny access by activating **All anonymous users**. Confirm with **OK**.
9. Go back to the **Actions** bar and click **Add Allow Rule...**.

10. A dialog is opened. Activate **Specified roles or user groups** and enter your user group name including domain name into the field (for example <Domain Name>\WHD Users) to allow user group access for your specific user group.
11. Confirm with **OK**.
12. Go back to the **Actions** bar and click **Add Deny Rule...**.
13. A dialog is opened. Activate **All users** to deny access for all users. Confirm with **OK**.
14. Make sure the order of the entries is as follows:
    - Deny - Anonymous Users - Local
    - Allow - <Domain name\Group name> - Local
    - Deny - All Users - Local
    - Allow - All Users - Inherited

In order to test the functionality, log on as described in Logon with Windows Authentication enabled (page 9). The Welcome screen should appear.

If you need to disable Windows Authentication to allow traditional login via a promoted Active Directory user, remove the rule **Deny - All anonymous users**.

Note: You can also enable Windows Authentication by modifying the web.config file. For example:

```
<configuration>
  <system.web>
    <authentication mode="Windows" />
    <authorization>
      <allow roles="HelpDesk" />
      <deny users="*" />
    </authorization>
  </system.web>
</configuration>
```

4.3 Logon with Windows Authentication enabled

Proceed as follows:

1. Open the browser and enter the URL.
2. To call the application in your browser, enter the URL: **`https://<Host ID or IP address>/SGNWHD`**
3. Select the required option **Recovery** or **Approve Suspension** and proceed as described in About recovery types (page 13) and the following sections.

5 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 user name and their password which are equivalent to their Windows credentials.

For users, two authentication scenarios are possible:

- Users who have been promoted to security officers in the SafeGuard Management Center will log on as described in Log on to Web Helpdesk without Windows Authentication enabled (page 10).
- Users who have been assigned to a specific Web Helpdesk user group with "Windows Authentication enabled" will log on as described in Logon with Windows Authentication enabled (page 9).

5.1 Preparations in the SafeGuard Management Center

To be able to authenticate at Web Helpdesk without Windows Authentication enabled the following prerequisites must be met and the following preparations need to be taken in the SafeGuard Management Center. For further information, see the *SafeGuard Enterprise Administrator help*.

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 be promoted to security officers.

   The promoted security officers can then log on to Web Helpdesk with their defined security officer name, which is a combination of their Windows user name and the name of the domain assigned to them. The required password is the Windows password protecting their certificates.
4. Security officers need to have the role Helpdesk Officer assigned to them to be able to authenticate at Web Helpdesk.
5. They also need to have access rights for the objects they need to work with, for example domains or organizational units. For further information see the *SafeGuard Enterprise Administrator help*, chapter *Assigning directory objects to a security officer*.

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

5.2 Log on to Web Helpdesk without Windows Authentication enabled

1. Start your browser.

2. To call the application in your browser, enter the URL: **`https://<Host ID or IP address>/SGNWHD`**
3. On the **Welcome** page, enter your security officer name as defined in SafeGuard Management Center, in the following way: **`<user name>@<DOMAIN>`** for example **`WHDOfficer@MYDOMAIN`**.

   The entry is case-sensitive. Make sure that the user name is spelled correctly.

4. Enter your Windows password.
5. Click **Log on**.

You are logged on to Web Helpdesk.

Note: If the certificate is created when users are promoted, they have to use the certificate password to log on to the SafeGuard Management Center. They have to enter the certificate password although they are prompted for the Windows password.

6 Select the Web Helpdesk Wizard

1. On the **Home** page, do one of the following:
   - To authorize recovery actions on endpoints, select **Recovery**, see About recovery types (page 13).
   - To authorize suspension of the SafeGuard Configuration Protection policy on endpoints, select **Approve Suspension**, see SafeGuard Configuration Protection (page 24).

7 About recovery types

Select which type of recovery is required. The following recovery types are provided:

- **SafeGuard Enterprise clients (managed)**

  Logon recovery for endpoints that are centrally managed by the SafeGuard Management Center. Managed endpoints are listed in the **Users and Computers** area in the SafeGuard Management Center.

- **Virtual Clients**

  Easy recovery for encrypted volumes can be achieved even when Challenge/Response is not usually 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 before the Challenge/Response session. Challenge/Response can then be initiated on the endpoint with the help of these Virtual Clients and the key recovery tool **`RecoveryKeys.exe`** that is available in the product delivery. 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 clients (standalone)**

  Logon recovery for endpoints that are locally managed. They never have any connection to the SafeGuard Enterprise Server. For each unmanaged Sophos SafeGuard endpoint 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, for example on a USB memory stick or on a shared network path so that the helpdesk officer can access it, Challenge/Response for an unmanaged Sophos SafeGuard protected computer is supported.

8 Recovery for managed endpoints (managed SafeGuard Enterprise clients)

SafeGuard Enterprise offers recovery for managed SafeGuard Enterprise protected endpoints in various disaster recovery scenarios, such as password recovery or accessing data by starting from external media.

The program dynamically determines if SafeGuard Enterprise full disk encryption or BitLocker Drive Encryption is in use and adjusts the recovery workflow accordingly.

8.1 Recovery actions for managed endpoints

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

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

8.1.1 Recover 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 endpoint 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 **Boot SGN client with user logon**, but without displaying the user password. However, in this case, after entering the response code the endpoint will start the operating system, so the user has to change the password at Windows level, subject to the conditions set on the domain. 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

We recommend that you use the following methods when the user has forgotten their password to avoid resetting the password centrally:

- **Use Local Self Help.** Local Self Help allows the user to have their current password displayed and to continue using it. This avoids the need to reset the password or to involve the helpdesk. For further information, see the *SafeGuard Enterprise administrator help*.

- **When using Challenge/Response on SafeGuard Enterprise clients (managed):** We recommend that you avoid resetting the password centrally in the Active Directory before the Challenge/Response procedure. Avoiding this will ensure that the password remains synchronized between Windows and SafeGuard Enterprise. Make sure that the Windows helpdesk is informed of this fact.

As a SafeGuard Enterprise helpdesk officer, generate a response to **Boot SGN Client with user logon** with the option **Show user password**. This avoids resetting the password in Active Directory

for the user. The user may continue working with the existing password and change it locally afterwards, if desired.

8.1.2 Display the user password

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

8.1.3 Access data by starting the endpoint from external media

Challenge/Response can also be used to allow to start an endpoint 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 the external media device.

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

- The device to be used must contain the SafeGuard Enterprise filter driver. For further information on how to obtain such a driver CD, see: http://www.sophos.com/en-us/support/knowledgebase/108805.aspx
- The user must start the endpoint from an external media device. The right to do so can be granted to them by defining a policy in the SafeGuard Management Center and then assigning it to the endpoint (policy **Authentication > Access: User may only boot from internal hard disk** must be set to **No**).
- The endpoint must allow starting from external media.
- 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 SafeGuard Management Center and assigned to the endpoint.

Note: When you use external media such as WinPE to access an encrypted drive, this only gives partial access to the volume.

8.1.4 Restore the SafeGuard Enterprise policy cache

If the SafeGuard Enterprise policy cache is damaged, the user will automatically be prompted to initiate a Challenge/Response procedure when logging on at the Power-on Authentication.

8.2 Create a response for managed computers

To create a response for managed computers (SafeGuard Enterprise clients), the computer name and the domain name are required.

1. On the **Recovery type** page, select **SafeGuard Enterprise Client**.
2. Select the relevant domain from the list.

3. Enter the required computer name. There are several ways to do this:
   - 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 under **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 the distinguished name format, for example:

     `CN=Desktop1,OU=Development,OU=Headquarter,DC=Utimaco,DC=com`

4. Click **Next**.

The program then dynamically determines if SafeGuard Enterprise full disk encryption or BitLocker Drive Encryption is used on the computer and adjusts the recovery workflow accordingly.

- In the case of a SafeGuard Enterprise protected computer the next step requires the selection of the user information.
- In the case of a BitLocker encrypted computer a volume that cannot be accessed any more may be recovered. The next step requires the selection of the volume that is to be decrypted.

8.2.1 Create a response for computers protected by SafeGuard Enterprise full disk encryption

1. In **Domain** select the required domain of the user. In the case of a local user select **Local user on <computer name>**.
2. Search for the required user name. Do one of the following:
   - Click **Search by Display Name**. Select the required name from the list and click **OK**.
   - Click **Search by Logon Name**. Select the required name from the list and click **OK**.
   - Enter the name of the user directly. Make sure that the name is spelt correctly.
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 available recovery actions on the endpoint are displayed. Available actions for response depend on the actions requested on the endpoint when calling the challenge. For example, if **Crypto token requested** is required, 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 **Boot SGN client with user logon** as mentioned above has been selected as the response action, you can additionally select **Show user password** to have the password displayed on the target endpoint.
8. Click **Next**. A response code is generated.
9. Read or send 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 endpoint and perform the authorized action.

8.2.2 Create a response for computers protected by BitLocker Drive Encryption

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

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

9 Recovery using Virtual Clients

Using Virtual Clients for recovery in SafeGuard Enterprise, access to encrypted volumes can be recovered even in complex recovery situations.

This recovery type can 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 endpoint in a secure way.

Note: Virtual Client recovery should only be used to resolve complex recovery situations: If both of the above mentioned issues apply, a Virtual Client recovery is appropriate. If however only the key needed is missing, 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 before the Challenge/Response session is started. Challenge/Response can then be initiated on the endpoint with the help of the Virtual Client files and the key recovery tool **`RecoverKeys.exe`** 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 transferred within the response.

Note: In Web Helpdesk, Recovery using Virtual Clients is not supported for unmanaged endpoints (Sophos SafeGuard Clients standalone). Use the SafeGuard Management Center instead.

9.1 Recovery workflow using Virtual Clients

For further information, see the *SafeGuard Enterprise Administrator help*.

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

   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 key recovery tool then tells the user which volumes are encrypted and which keys are used for each of these volumes. The user presents this information to the helpdesk officer.
4. The helpdesk officer identifies the Virtual Client in the database and selects the required key for accessing the encrypted volumes: either a single key or several keys exported to a key file. The helpdesk officer then generates 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 access the encrypted volumes again.

9.2 Recovery actions using Virtual Clients

To access volumes that are encrypted with keys which are not available to the user, the correct encryption key(s) 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

9.2.1 Transfer a single key

Challenge/Response 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 endpoint by entering the response code. If the response code is correct, the transferred key will be imported to the local key store. After that, all volumes that are encrypted with this key can be accessed.

9.2.2 Transfer several keys in an encrypted key file

Challenge/Response 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 key file created.

The encrypted key file needs to be transferred to the user environment and must be available to the user. To decrypt this key file the user then has to initiate a Challenge/Response session with the key recovery tool **`RecoverKeys.exe`**. During this session the password is transferred to the target endpoint. The helpdesk officer generates a response and selects the respective password to decrypt the key file. The password is transferred to the target endpoint within the response code. The key file can then be decrypted with the password.

The keys in the key file are imported into the key storage on the endpoint 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. Therefore you must create a new key file and a password after each successful Challenge/Response session.

9.3 Response using Virtual Clients

9.3.1 Prerequisites

- The Virtual Client must have been created in the SafeGuard Management Center in **Keys and Certificates**. For further information, see the *SafeGuard Enterprise Administrator help*.
- The helpdesk officer must be able to locate the Virtual Client in the database. Virtual Clients are identified uniquely by their name.
- 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 that you store this file on a memory stick.
- When recovery for several keys is requested, the helpdesk officer must previously have created a key file containing the necessary recovery keys in the SafeGuard Management Center in **Keys and Certificates**. 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. For further information, see the *SafeGuard Enterprise administrator help*.
- 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, this means that if 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.

9.3.2 Create a response using Virtual Clients

1. As a helpdesk officer, select **Virtual Client** on the **Recovery type** page.
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 page where you can select the recovery action is 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 required 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 requested can only be selected when a key file has previously been created in the SafeGuard Management Center in **Keys and 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. Therefore you have to create a new key file and password after every successful Challenge/Response session.

5. Click **Next**. The page 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 endpoint.
9. The user needs to restart the computer and log on again to access the respective volumes.

The volumes can be accessed again.

10 Recovery for unmanaged endpoints (Sophos SafeGuard clients standalone)

SafeGuard Enterprise also provides Challenge/Response for unmanaged endpoints (Sophos SafeGuard clients standalone). They 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, their identification needed for a Challenge/Response is not available.

Therefore Challenge/Response for unmanaged endpoints is based on the recovery key file created during endpoint configuration. The recovery file (.xml file) is generated for each unmanaged endpoint 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 on a memory stick or a shared network path, a response can be generated.

10.1 Recovery actions for unmanaged endpoints

Challenge/Response for unmanaged endpoints (Sophos SafeGuard client standalone) must be initiated in the following situations:

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

For unmanaged endpoints no user key is available in the database. Therefore, the only recovery action possible in a Challenge/Response session is **Boot Sophos SafeGuard client without user logon**.

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

10.1.1 The user has entered the password incorrectly too many times

As in this case resetting the password is unnecessary, the Challenge/Response procedure enables the user to log on at the Power-on Authentication. The user can then enter the correct password at Windows level and use the endpoint again.

10.1.2 The user has forgotten the password

Note: We recommend that you usually use Local Self Help to recover a forgotten password. Local Self Help allows you to have the current password displayed and to continue using it. This avoids the need to reset the password or to involve the helpdesk. For further information, see the *SafeGuard Enterprise Administrator help*.

When you recover a forgotten password using Challenge/Response a password reset is required.

1. The Challenge/Response procedure enables the computer to start through Power-on Authentication.
2. At the Windows logon prompt, the user does not know the correct password and needs to change password at Windows level. This requires further recovery actions outside the scope of SafeGuard Enterprise, by standard Windows means. We recommend that you use the following methods to reset the password at Windows level.
   - Using a service or administrator account available on the computer with the required Windows rights.
   - Using a Windows password reset disk.

   As a helpdesk 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 the Windows logon prompt that the helpdesk 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 prompted to enter the old SafeGuard Enterprise password and, since the user has forgotten this password, needs to click **Cancel**.
5. In SafeGuard Enterprise, a new certificate is needed in order to set a new password without providing the old one.
6. A new user certificate is 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 existing user keys for SafeGuard Data Exchange the user has to remember the SafeGuard Data Exchange passphrases to reactivate these keys.

10.2 Create a response for unmanaged computers

To generate a response for an unmanaged computer, the name of the recovery file (.xml file) is required.

1. In Web Helpdesk, on the **Tools** menu, click **Recovery**.
2. In **Recovery type**, select **Standalone Client**.
3. Locate the required key recovery file (.xml) by clicking **Browse**.
4. Enter the challenge code the user has passed on to you.
5. Select the action to be taken by the user and click **Next**.
6. 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, perform the requested action and resume working.

11 SafeGuard Configuration Protection

The module SafeGuard Configuration Protection is no longer available as of SafeGuard Enterprise 6.1. The corresponding policy is still available in the SafeGuard Management Center 6.1 to support SafeGuard Enterprise 6.x clients with Configuration Protection installed and managed with a 6.1 Management Center.

For further information on SafeGuard Configuration Protection, refer to the *SafeGuard Enterprise 6 Web Helpdesk* manual: http://www.sophos.com/en-us/medialibrary/PDFs/documentation/sgn_60_m_eng_web_helpdesk.pdf.

12 Logging Web Helpdesk events

Events for Web Helpdesk can be logged in the Windows Event Viewer or in the SafeGuard Enterprise Database. Events of all helpdesk activities can be logged, for example who logged on to Web Helpdesk, which user requested a challenge or which recovery actions have been requested.

Event logging for Web Helpdesk is activated in the SafeGuard Management Center by a policy that needs to be published into a configuration package and deployed on the Web Helpdesk service.

Events that are logged in the central SafeGuard Enterprise Database can be viewed in the SafeGuard Management Center Event Viewer.

12.1 Enable logging for Web Helpdesk events

Logging for Web Helpdesk is configured in the SafeGuard Management Center.

You need to have the required rights to create policies and view events.

1. In the SafeGuard Management Center, in the **Policies** navigation area, create a policy of the type **Logging**. Select the events to be logged. Save your changes.
2. Create a new **Policy Group**. Add the policy of the type **Logging** to this group. Save your changes.
3. On the **Tools** menu, click **Configuration Package Tool**. Select **Managed client packages** and click **Add Configuration Package**. Select the previously created policy group to be included in the configuration package. Select a storage location and click **Create Configuration Package**.
4. In the SafeGuard Management Center, assign the policy group to the domain that contains the Web Helpdesk server. Then activate it. For more information, see the *SafeGuard Enterprise administrator help*, chapter *Assign policies*.
5. On the Web Helpdesk server, install the previously created configuration package. Restart the service.

   Logging Web Helpdesk events has been activated.

6. Log on to Web Helpdesk and carry out a Challenge/Response procedure.
7. In the SafeGuard Management Center, click the **Reports** tab. In the **Event Viewer** action area on the right, click the magnifier icon to view the events logged for Web Helpdesk.

13 Technical support

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

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

14 Legal notices