

SOPHOS

Security made simple.

SafeGuard Enterprise

User help

Product version: 7

Document date: December 2014



Contents

1	About SafeGuard Enterprise 7.0.....	5
2	SafeGuard Enterprise on Windows endpoints.....	7
3	Security best practices	9
4	SafeGuard Power-on Authentication.....	11
4.1	First logon after SafeGuard Enterprise installation.....	11
4.2	Logging on at the SafeGuard Power-on Authentication.....	13
4.3	Register further SafeGuard Enterprise users.....	14
4.4	Temporary password in the SafeGuard POA.....	14
4.5	Logging on at the SafeGuard Power-on Authentication with smartcards or tokens.....	15
4.6	SafeGuard POA autologon with a token.....	18
4.7	Virtual keyboard.....	19
4.8	Keyboard layout.....	19
4.9	Supported hotkeys/function keys in the SafeGuard Power-on Authentication.....	20
4.10	Password synchronization.....	22
5	Logging on to Windows.....	23
5.1	Log on with SafeGuard Enterprise.....	23
5.2	Log on with the Windows authentication method.....	23
6	Logging on with the Lenovo Fingerprint Reader.....	24
6.1	Requirements.....	24
6.2	Enroll fingerprints.....	25
6.3	Log on to SafeGuard Power-on Authentication with a fingerprint.....	26
6.4	Changing your password.....	29
6.5	Fingerprint logon recovery.....	30
7	Disk encryption.....	31
7.1	SafeGuard full disk encryption.....	31
7.2	BitLocker Drive Encryption.....	34
8	SafeGuard Data Exchange.....	39
8.1	Settings for handling removable media	40
8.2	Single media passphrase for all removable media connected to the computer.....	40
8.3	Encrypting removable media.....	41
8.4	Exchanging data using SafeGuard Data Exchange.....	44

8.5	Writing files to CDs using the Windows CD Writing Wizard.....	45
8.6	SafeGuard Portable.....	46
9	SafeGuard File Encryption.....	51
9.1	Encrypt according to policy.....	51
9.2	SafeGuard File Encryption Wizard.....	52
9.3	Persistent encryption.....	52
10	SafeGuard Cloud Storage.....	53
10.1	Cloud Storage auto-detection.....	53
10.2	Cloud Storage initial encryption.....	53
10.3	Set default keys	53
10.4	SafeGuard Portable for Cloud Storage.....	54
11	SafeGuard Enterprise and self-encrypting, Opal-compliant hard drives.....	55
11.1	Encryption of Opal-compliant hard drives.....	55
11.2	System Tray Icon and Explorer extensions on endpoints with Opal-compliant hard drives.....	55
12	System Tray Icon and tool tips.....	56
12.1	Create local keys.....	58
12.2	Overlay icons.....	59
13	Accessing functions via Explorer extensions.....	60
13.1	Explorer extensions for file-based encryption.....	60
13.2	Explorer extensions for volume-based encryption.....	62
14	Recovery options.....	63
15	Recovery with Local Self Help.....	64
15.1	Activate Local Self Help.....	64
15.2	Activate Local Self Help - reminder.....	66
15.3	Edit questions.....	67
15.4	Changes of question parameters.....	68
15.5	Changes of conditions or parameters for Local Self Help during editing processes.....	69
15.6	Log on at the SafeGuard POA with Local Self Help.....	71
15.7	Failed logon attempts.....	72
15.8	Reactivate questions and answers after password changes on several machines.....	72
16	Recovery with Challenge/Response or recovery key.....	73
16.1	Challenge/Response for SafeGuard POA users.....	73
16.2	Challenge/Response for BitLocker users.....	79
16.3	BitLocker recovery key.....	80

17	SafeGuard Enterprise and Lenovo Rescue and Recovery.....	82
17.1	Overview.....	82
17.2	Requirements.....	82
17.3	Installation.....	83
17.4	Upgrade.....	83
17.5	Uninstallation.....	84
17.6	Boot environment and recovery options.....	84
17.7	Create a backup.....	84
17.8	Restore file backups.....	85
17.9	Restore the SafeGuard Enterprise system.....	85
17.10	Service and factory recovery partitions.....	86
17.11	Disabled SafeGuard POA and Lenovo Rescue and Recovery.....	86
18	Technical support.....	87
19	Legal notices.....	88

1 About SafeGuard Enterprise 7.0

This version of SafeGuard Enterprise supports Windows 7 and Windows 8 on endpoints with BIOS or UEFI.

- For BIOS platforms administrators can choose between SafeGuard Enterprise full disk encryption and BitLocker encryption managed by SafeGuard. The BIOS version comes with the BitLocker-native recovery mechanism.

Note: If SafeGuard Power-on Authentication or SafeGuard full disk encryption is mentioned in this manual, it refers to Windows 7 BIOS endpoints only.

- For UEFI platforms BitLocker managed by SafeGuard Enterprise is the component for disk encryption. For these endpoints SafeGuard Enterprise offers enhanced Challenge/Response capabilities. For details on the supported UEFI versions and restrictions to SafeGuard BitLocker Challenge/Response support, please see the Release Notes at http://downloads.sophos.com/readmes/readsgn_7_eng.html.

Note: Whenever the description only refers to UEFI, it is mentioned explicitly.

The table shows which components are available.

	SafeGuard full disk encryption with SafeGuard Power-on Authentication (POA)	BitLocker with pre-boot authentication (PBA) managed by SafeGuard	SafeGuard C/R recovery for BitLocker pre-boot authentication (PBA)
Windows 7 BIOS	YES	YES	
Windows 7 UEFI		YES	YES
Windows 8 BIOS		YES	
Windows 8 UEFI		YES	YES
Windows 8.1 BIOS		YES	
Windows 8.1 UEFI		YES	YES

Note: SafeGuard C/R recovery for BitLocker pre-boot authentication (PBA) is only available on 64 bit systems.

SafeGuard full disk encryption with SafeGuard Power-on Authentication (POA) is the Sophos module for encrypting volumes on endpoints. It comes with a Sophos implemented pre-boot authentication named SafeGuard Power-on Authentication (POA) which supports logon options like smartcard and fingerprint and a Challenge/Response mechanism for recovery.

BitLocker with pre-boot authentication (PBA) managed by SafeGuard is the component that enables and manages the BitLocker encryption engine and the BitLocker pre-boot authentication.

It is available for BIOS and UEFI platforms:

- The UEFI version additionally offers a SafeGuard Challenge/Response mechanism for BitLocker recovery in case users forget their PINs. The UEFI version can be used when certain platform requirements are met. For example the UEFI version must be 2.3.1. For details, see the Release Notes.
- The BIOS version does not offer the recovery enhancements by the SafeGuard Challenge / Response mechanism and serves also as fallback option in case the requirements for the UEFI version are not met. The Sophos installer checks whether the requirements are met, and if not automatically installs the BitLocker version without Challenge/Response.

Mac endpoints

For Mac endpoints the following products are available. They are also managed by SafeGuard Enterprise or at least report to the management center.

	Sophos SafeGuard File Encryption 7.0	Sophos SafeGuard Native Device Encryption (FileVault 2 management) 7.0
OS X 10.8	YES	YES
OS X 10.9	YES	YES
OS X 10.10	YES	YES

The description in this manual refers to the Windows platform only. For the Mac versions, see the respective product manuals.

Sophos Mobile Encryption

With **Sophos Mobile Encryption** you can read files encrypted by the SafeGuard Enterprise modules **SafeGuard Cloud Storage** or **SafeGuard Data Exchange**. They allow you to encrypt files using a local key. These local keys are derived from a passphrase that is entered by the user. You can only decrypt a file when you know the passphrase that was used to encrypt the file. For details on Sophos Mobile Encryption please visit www.sophos.com.

2 SafeGuard Enterprise on Windows endpoints

SafeGuard Enterprise is a modular security suite that enforces security for endpoints on a cross-platform basis, using administrator-defined policies. SafeGuard Enterprise is easy to use. System administration is carried out centrally in the SafeGuard Management Center.

The main protection functions of SafeGuard Enterprise on an endpoint are data encryption and protection against unauthorized access through external media.

SafeGuard Enterprise modules

- **SafeGuard full disk encryption**

- **SafeGuard Power-on Authentication**

- Logon is performed immediately after you switch on the computer. After successful SafeGuard Power-on Authentication (POA), you are automatically logged on to the operating system. You can also deactivate the SafeGuard POA. In this case, authentication is performed by the operating system.

- **Volume-based encryption**

- All data on volumes (including boot files, swap files, idle files/hibernation files, temporary files, directory information etc.) are encrypted transparently without the user having to change the normal operating procedure or consider security.

- **BitLocker with pre-boot authentication managed by SafeGuard Enterprise**

- SafeGuard Enterprise manages the Microsoft BitLocker encryption engine. On UEFI platforms BitLocker pre-boot authentication comes with a SafeGuard Challenge / Response mechanism whereas the BIOS version allows to retrieve the recovery key from the management center.

- **SafeGuard Data Exchange**

- SafeGuard Data Exchange offers easy data exchange with removable media on all platforms without re-encryption.
 - File-based encryption
 - All mobile writable media, including external hard disks and USB memory sticks, are encrypted transparently.

- **SafeGuard File Encryption**

- SafeGuard File Encryption offers file-based encryption, mainly for workgroups to securely store data on network shares.

- Files in locations covered by File Encryption policies will be encrypted on-the-fly, with no user interaction.

- **SafeGuard Cloud Storage**

SafeGuard Cloud Storage offers file-based encryption of data stored in the cloud. It makes sure that the local copies of your cloud data are encrypted transparently and remain encrypted when they are stored in the cloud.

Note: Some features described in this user help may not be available on your computer. This is because the features available depend on the policies set by your security officer.

3 Security best practices

By following the simple steps described here, you can keep data on your computer secure and protected at all times.

Shut down your computer completely or put it into hibernation mode when it is not in use

On SafeGuard Enterprise protected computers, encryption keys might be accessible to attackers in certain sleep modes where the computer's operating system is not shut down properly and background processes are not terminated completely. Protection is enhanced when the operating system is always shut down or hibernated properly.

When your computer is not in use or left unattended:

- Avoid Sleep (Stand-by/suspend) mode. Avoid Hybrid Sleep mode. Hybrid Sleep mode combines hibernation and sleep.
- Do not simply lock the desktop and switch off the monitor (or close the lid of your laptop), if this is not followed by a proper shut down or hibernation. Setting an additional prompt for a password when you resume working does not provide sufficient protection.
- Always shut the computer down properly or put it into hibernation mode.

Note: It is important that the hibernation file resides on an encrypted volume. Typically it resides on C:\.

Follow these steps in particular when you use a laptop in public locations like airports.

When the computer is hibernated or shut down properly, SafeGuard Power-on Authentication is always activated the next time it is used, thus providing full protection.

Ensure that all volumes have a drive letter assigned

Only volumes that have a drive letter assigned are encrypted. Consequently, volumes without a drive letter assigned may be abused to leak confidential data in plaintext.

To mitigate this threat:

- If you find a volume without a drive letter assigned on your computer, contact your system administrator.
- Do not change drive letter assignments.

Choose strong passwords

Strong passwords are a vital part of protecting your data. Use strong passwords, especially for securing the logon to your computer.

A strong password follows these rules:

- It is long enough to be secure: A minimum of 10 characters is recommended.
- It contains a combination of letters (upper and lower case), numbers and special characters/symbols.
- It does not contain a commonly used word or name.
- It is hard to guess but easy for you to remember and type accurately.

Change your passwords at regular intervals. Do not share them with anyone and do not write them down.

4 SafeGuard Power-on Authentication

SafeGuard Power-on Authentication (POA) requires you to authenticate before the computer's operating system is started. After you do this, Windows starts and you are logged on automatically. The procedure is the same when the computer is switched back on from hibernation (Suspend to Disk).

SafeGuard POA look and feel

The look and feel of the SafeGuard POA can be customized according to your company's requirements. Your security officer does this in the policy settings in the SafeGuard Management Center.

The following adjustments are possible:

- **Logon image**

The default logon image displayed in the SafeGuard POA is a SafeGuard design. This screen is customizable by policy to show your company logo, for example.

- **Dialog text**

All text in the SafeGuard POA is displayed in the default language set in the Windows Regional and Language Options. You can change the language used in the POA by changing the default language. The language of the dialog text can also be specified by the security officer in a policy.

4.1 First logon after SafeGuard Enterprise installation

If SafeGuard Enterprise has been installed with SafeGuard Power-on Authentication, the startup procedure is different during the first system start after the installation of SafeGuard Enterprise. A number of new start messages (for example, the autologon screen) are displayed because SafeGuard Enterprise has been incorporated into the startup procedure. Afterwards, the Windows operating system starts.

Note:

SafeGuard Enterprise uses certificate-based logon. However, user-specific keys and certificates are only created after a successful Windows logon.

When you log on for the first time after installation, you must first log on successfully to Windows as usual using your credentials. Afterwards, you are registered as a SafeGuard Enterprise user. This registration process is required to make sure that your credentials are recognized in the SafeGuard POA the next time the system is started.

A tool tip displays to inform you about the successful registration and receipt of all required data.

When you restart the computer, the SafeGuard POA is activated. From now on, you enter your Windows credentials at the SafeGuard POA. You are then logged on to Windows automatically without any further password entry (if automatic logon to Windows is activated).

You can log on at the SafeGuard POA by using your user name and password.

Note: The settings for the computers which SafeGuard Enterprise is installed on are defined centrally by the security officer in the SafeGuard Management Center and distributed to the endpoints in policy files.

First logon procedure

This section describes the procedure for the first logon to your computer after SafeGuard Enterprise has been installed. The procedure will only correspond to the one described here if the SafeGuard POA has been installed and activated for your computer.

4.1.1 SafeGuard Autologon

1. The computer starts, and the SafeGuard Autologon dialog is displayed.
 - A SafeGuard autouser is logged on.
 - If a connection to the SafeGuard Enterprise Server exists, the computer is automatically registered on the SafeGuard Enterprise Server.
 - The machine key is sent to the SafeGuard Enterprise Server and stored in the SafeGuard Enterprise database.
 - Machine policies are sent to the computer.

4.1.2 Windows logon

1. The Windows logon dialog is displayed.
2. SafeGuard Enterprise offers the SafeGuard Enterprise and the Windows authentication method. Windows provides two icons for the two methods:
 - Click **Other User** to open a dialog for entering credentials.
 - Click the second icon (with a user name displayed below it) to open a dialog that contains the user information of the last user who has logged on to the system. You only have to enter the password.

If your user name is displayed below a SafeGuard Enterprise icon, click that icon. If this is not the case, select the SafeGuard Enterprise icon with **Other User** below it.

3. Enter your Windows user credentials as usual.
 - Your user ID and a hash of your credentials are sent to the server.
 - User policies, certificates, and keys are created and sent to the endpoint.

The user data will become available in the SafeGuard Power-on Authentication after all data has been successfully synchronized between the SafeGuard Enterprise server and your computer.

This means that **the next time the system is started** you only have to enter your Windows user credentials (user name and password) in the SafeGuard POA and you are logged on automatically.

You must restart the computer to activate SafeGuard Power-on Authentication fully. After the restart, the SafeGuard Power-on Authentication protects your computer against unauthorized access.

4.1.3 SafeGuard Power-on Authentication logon after restart

1. When you restart your computer, the SafeGuard Power-on Authentication logon dialog is displayed.

Certificates and keys are available, and you can log on at the SafeGuard POA using your Windows user credentials.

2. Enter your user name and password, and click **OK**.

Your user credentials are evaluated. After the system has verified your credentials, you are automatically logged on to Windows.

Note: Logon pass-through to Windows may be deactivated by a policy setting. In this case, the Windows logon dialog is displayed and you have to enter your user credentials.

4.2 Logging on at the SafeGuard Power-on Authentication

After successful activation of the SafeGuard Power-on Authentication (initial synchronization and restart), you log on by entering your Windows user credentials in the SafeGuard POA logon dialog. You are logged on to Windows automatically.

Note: You can deactivate automatic logon to Windows by clicking the **Options** button in the logon dialog and clearing the **Pass through logon to Windows** check box. Deactivating the automatic logon is, for example, necessary to enable other users to use SafeGuard Power-on Authentication on the computer, see [Register further SafeGuard Enterprise users](#) (page 14). The security officer defines, in the relevant policies, whether logon pass-through to Windows is activated or deactivated and whether you are allowed to change this setting in the logon dialog.

Logon delay on failed logon attempt

If logon at the SafeGuard Power-on Authentication fails, for example, due to an incorrect password, an error message is displayed, and a delay is imposed before the next logon attempt. The delay period is increased with each failed logon attempt. Failed attempts are logged.

Machine lock

After a set number of failed logon attempts, your computer will be locked. To unlock your computer, initiate a Challenge/Response procedure, see [Recovery with Challenge/Response or recovery key](#) (page 73).

4.2.1 Logon recovery

For logon recovery for example, if you have forgotten your password, SafeGuard Enterprise offers different options that are tailored to different recovery scenarios. The recovery methods available

on your computer depend on the settings specified by the security officer. For further information, see [Recovery options](#) (page 63).

4.3 Register further SafeGuard Enterprise users

To allow another Windows user to log on to your computer:

1. Switch on the computer.

The SafeGuard POA logon dialog is displayed. The second Windows user cannot log on at the SafeGuard POA because they do not have the necessary keys and certificates.

2. For the second user to log on at the SafeGuard POA, the computer's owner must allow it.

Note: The default setting specifies that the first user to log on after installation is registered as the owner of the computer. The security officer can also define the owner of a computer with a policy setting.

3. In the SafeGuard POA logon dialog, click **Options** and clear the **Pass through logon to Windows** check box. Log on with your credentials as the computer's owner.

The Windows logon dialog is displayed.

4. The second user enters their Windows credentials.
5. If the second user's certificate, and key are all available on the computer (evident from the relevant balloon tool tip), an entry for the second user is created in the SafeGuard Enterprise.

The next time the computer is started, the second user can log on at the SafeGuard Power-on Authentication.

Note: Security officers can assign users to the SafeGuard POA on a new machine in the SafeGuard Management Center. Users assigned in this way can log on at the SafeGuard Power-on Authentication on the relevant computer.

4.4 Temporary password in the SafeGuard POA

SafeGuard Enterprise allows you to change the password temporarily in the SafeGuard POA. Changing the password temporarily is recommended if you suspect that somebody has watched you enter your password.

Example: You start your notebook in a public place, for example at the airport. You think that somebody watched you enter your password at the SafeGuard POA. Since you are not connected to Active Directory (AD), you cannot change your Windows password.

Solution: You temporarily change your SafeGuard POA password to ensure that no unauthorized person knows your password. As soon as you are connected to AD again, you are automatically prompted to change the temporary password.

1. In the SafeGuard POA logon dialog, enter the existing password.
2. Press **F8**.

Note: If you do not enter the existing password before you press **F8**, the system interprets this as a failed logon, and an error message is displayed.

3. In the dialog, enter the new password and confirm it.

The system reminds you that the password change is only temporary.

4. Click **OK**.

Note: If you cancel this dialog, you will be logged on with your old password.

The Windows logon dialog is displayed.

Note: Logon will not be passed through to Windows, even if your system is configured that way. Enter the "old password" here. The temporary password is only valid for logging on at the SafeGuard POA.

5. Click **OK**.

You are logged on to Windows.

For logging on at the SafeGuard POA, you can now only use the temporary password. The temporary password is valid until the password is changed at the Windows logon. Only after you do that can logon be passed through from SafeGuard POA to Windows again.

Changing the temporary password

The password changed temporarily in the SafeGuard POA has to be changed later to synchronize passwords again.

When you log on to Windows, SafeGuard Enterprise automatically prompts you to change your password as soon as you are connected to Active Directory again.

You can close the dialog prompting you to change the password without actually changing the password. In this case, the dialog is shown each time you log on until you change the password.

Note: The SafeGuard POA password can also be changed temporarily while you are connected to Active Directory. In this case, the dialog for changing the password is shown immediately after changing the password temporarily in the SafeGuard POA. You can close this dialog without any changes and use the "old password" for logging on. You can change the password later.

4.5 Logging on at the SafeGuard Power-on Authentication with smartcards or tokens

There are two possible types of logon with smartcards or tokens:

- Logon is *only allowed with smartcards or tokens*.
- Logon is *allowed either with user name and password or with smartcard or token*.

The security officer defines the allowed logon type in a policy.

The security officer issues your smartcard/token and provides it to you. You can also put your Windows user credentials on your smartcard/token yourself.

Note: SafeGuard Enterprise handles smartcards and tokens in the same way. So the terms "token" and "smartcard" mean the same in the product and the manual. In the following sections, the term "token" is used.

4.5.1 First logon with token after installation

The first logon with a token is identical to the logon procedure without a token.

If an issued token is available, you can use it to log on to Windows by entering the token PIN.

Note: We recommend that you configure your token with Windows user credentials before you restart the computer, see [Store Windows user credentials on your token](#) (page 17). The security policies that apply to you may require using a token at the SafeGuard POA. If your token does not contain your credentials, you cannot log on at the SafeGuard Power-on Authentication.

4.5.2 SafeGuard POA logon with token

Prerequisites: Make sure that USB support is activated in the BIOS. Token support has to be initialized, and the token has to be issued for you.

1. Plug in the token.
2. Switch on the computer.

The dialog for token logon is displayed.

Note: If your policy allows you to log on with your user credentials and you disconnect the token, you are prompted to enter your user credentials for logging on. If the dialog for logging on with a user ID and password is not displayed, you can only log on at the SafeGuard Power-on Authentication with a token.

3. Enter your token PIN.

You are logged on at the SafeGuard Power-on Authentication and to Windows (if the **Pass through to Windows** check box is selected in the logon dialog).

4.5.3 Change the PIN

You can change your token PIN in the Windows logon dialog.

If **Pass through logon to Windows** is selected at the SafeGuard Power-on Authentication (POA), the Windows logon dialog is usually not displayed. To display the Windows logon dialog, you have to clear this check box during SafeGuard POA logon.

Note: You are automatically prompted to change the PIN if the security officer has defined rules requiring a PIN change (for example, at specific time intervals).

1. In the **PIN** dialog for Windows logon, select the **Change PIN** check box.
2. Enter your token PIN and click **OK**.

The **PIN Change** dialog is displayed.

3. Enter the new PIN and confirm it.
4. Click **OK**.

The token PIN is changed and Windows logon continues.

4.5.4 Store Windows user credentials on your token

If your token does not contain your Windows user credentials, you can store them on the token yourself.

Note: We recommended that you configure your token during first logon. The security policies that apply to you may require using a token at the SafeGuard POA. If your token does not contain any user information, you cannot log on at the SafeGuard Power-on Authentication.

1. During the first logon after installation, connect your token with the system when the Windows logon dialog is displayed.

If the system detects an empty token, the **Issue Token** dialog is displayed automatically.

2. Enter your Windows user name and password.
3. Confirm your password.
4. Select or enter the domain, and click **OK**.

The system tries to log you on to Windows with the data entered. If logon is successful, the data is written to the token.

You are logged on to Windows.

If token logon is defined as optional for your user (that is you have already logged on once at the SafeGuard POA with your user name and password), you can also issue the token later.

To do so, click **Options** in the SafeGuard POA logon dialog and clear the **Pass through logon to Windows** check box. The Windows logon dialog is displayed, and you can store your credentials on the token as described.

4.5.5 Token logon recovery

If you use a non-cryptographic token and you have forgotten your PIN, you can regain access to your computer with one of the following recovery methods:

- [Recovery with Local Self Help](#) (page 64).
- [Recovery with Challenge/Response or recovery key](#) (page 73).

The recovery methods available on your computer depend on the settings specified by the security officer.

To initiate recovery, click the **Recovery** button in the token logon dialog.

Note: These recovery methods are not available for cryptographic tokens. If logon problems occur, contact your security officer.

4.5.6 Unblock tokens

If you enter your PIN incorrectly several times, your token is blocked. The security officer can configure SafeGuard Enterprise to display the **Unblock Token** dialog in this case.

The security officer has to provide you with the administrator PIN defined for your token.

1. In the **Unblock Token** dialog, enter the administrator PIN.
2. Enter a new PIN and confirm it.

The PIN you enter is subject to the rules defined for PINs (for example, specific character combinations may be required, PINs already used may be banned from being used again).

3. Click **OK**.

The token is unblocked and logon continues.

Note: If this function is not available on your computer, you can regain access to your computer with Challenge/Response. But you cannot change the PIN or your user credentials with Challenge/Response.

4.5.7 Cryptographic tokens - Kerberos

If you use a cryptographic token, you are authenticated at the SafeGuard POA by the certificate stored on the token.

For this type of logon, you need a fully issued token. The security officer or any other authorized person has to provide this token. To log on to the system, you only have to enter the token PIN. If this type of logon is the only type valid for your computer, you cannot log on without the token.

Note: If you use a token of this type neither Challenge/Response nor Local Self Help is available in case of logon problems. If logon problems occur, contact your security officer.

4.5.8 Change the certificate for token logon

To change or renew the certificate used for logging on with a token, your security officer can assign a new certificate to your computer. After synchronization between your computer and the SafeGuard Enterprise Server, the status dialog in the SafeGuard Enterprise System Tray Icon indicates that your computer is **Ready for certificate change**.

The security officer provides you with the new token.

To change the certificate on your computer:

1. Log on at the SafeGuard Power-on Authentication with your old authentication method (token or user name/password) without automatic logon to Windows.

Click **Options** and clear the **Pass through logon to Windows** check box or log off again after automatic logon to Windows has been performed.

2. Log on to Windows with the new token.

The new token is valid for SafeGuard POA logon. The old token is no longer valid for logon.

4.6 SafeGuard POA autologon with a token

Prerequisites:

- USB support is activated in the BIOS.

- Token support is initialized, and the token is issued.
- The security officer has assigned the relevant policy to your computer.

If a policy with a defined default PIN has been assigned to your computer, you can automatically log on at the SafeGuard Power-on Authentication by using a token. You do not have to enter any credentials or PIN, but are passed through at the SafeGuard POA. Depending on your policy settings, you may also be passed through to Windows.

To automatically log on at the SafeGuard Power-on Authentication using a token:

1. Plug in the token.
2. Switch on the computer.

You are automatically logged on at the SafeGuard Power-on Authentication. Depending on your policy settings, you may also be passed through to Windows.

- If autologon has been successful, Windows is started.
- If autologon has failed, you are prompted to enter your token PIN. You are then logged on at the SafeGuard Power-on Authentication.

4.7 Virtual keyboard

At the SafeGuard POA, you can show/hide a virtual keyboard on the screen, and click the on-screen keys to enter credentials, etc.

Prerequisite: The security officer has activated the display of the virtual keyboard by policy.

To show the virtual keyboard in the SafeGuard POA, click **Options** in the POA logon dialog and select the **Virtual Keyboard** check box.

The virtual keyboard supports different layouts. It is also possible to change the layout using the same options used for changing the SafeGuard POA keyboard layout, see [Change the keyboard layout](#) (page 20).

4.8 Keyboard layout

Almost every country has its own keyboard layout. The keyboard layout in the SafeGuard POA is very important when entering user names, passwords, and response codes.

By default, SafeGuard Enterprise adopts the keyboard layout which is set in the Windows Regional and Language Options for the Windows default user at the time SafeGuard Enterprise is installed.

The language of the keyboard layout being used is displayed in the SafeGuard POA, for example "EN" for English. Apart from the default keyboard layout, you can also use the US keyboard layout (English).

4.8.1 Change the keyboard layout

The SafeGuard Power-on Authentication keyboard layout (including the virtual keyboard layout) can be changed.

1. Select **Start > Control Panel > Regional and Language Options > Advanced**.
2. On the **Regional Options** tab, select the required language.
3. On the **Advanced** tab, under **Default user account settings**, select **Apply all settings to the current user account and to the default user profile**.
4. Click **OK**.

The SafeGuard POA recognizes the keyboard layout used for the last successful logon and automatically enables it for the next logon. This requires two restarts. If the previous keyboard layout is deselected in the **Regional and Language Options**, it is still maintained unless you select a different one.

Note: You must also change the language of the keyboard layout for non-Unicode programs.

If the language you want is not available on your system, Windows may prompt you to install it. After you have done so, you need to restart your computer twice so that, first, the new keyboard layout can be read in by the SafeGuard POA and, secondly, the POA can set the new layout.

You can change the required keyboard layout for the SafeGuard POA by using the mouse or keyboard (**Alt+Shift**).

To see which languages are installed and available on your system, select **Start > Run > regedit: HKEY_USERS\.DEFAULT\Keyboard Layout\Preload**.

4.9 Supported hotkeys/function keys in the SafeGuard Power-on Authentication

Certain hardware functionality and settings can lead to problems when starting computers, causing the system to no longer respond. The SafeGuard Power-on Authentication supports a number of hotkeys for modifying these hardware settings and deactivating functionality. Furthermore, a greylist of hardware settings and functionalities that are known to cause these problems is integrated in the .msi file installed on the computer.

We recommend that you install an updated version of the SafeGuard POA configuration file before any significant deployment of SafeGuard Enterprise. The file is updated on a monthly basis and made available to download from here:

<http://www.sophos.com/en-us/support/knowledgebase/65700.aspx>.

You can customize this file to reflect the hardware of a particular environment.

Note: When you define a customized file, this will be used instead of the one integrated in the .msi file. Only when no SafeGuard POA configuration file is defined or found will the default file be applied.

To install the SafeGuard POA configuration file, enter the following command:

```
MSIEXEC /i <Client MSI package> POACFG=<path of the POA configuration file>
```

The SafeGuard Power-on Authentication also supports a number of function keys.

4.9.1 Hotkeys

Shift - F3 = USB Legacy Support (on/off)

Shift - F4 = VESA graphic mode (off/on)

Shift - F5 = USB 1.x and 2.0 support (off/on)

Shift - F6 = ATA Controller (off/on)

Shift - F7 = USB 2.0 support only (off/on) USB 1.x support remains as set by **Shift - F5**.

Shift - F9 = ACPI/APIC (off/on)

Hotkeys dependency matrix

Shift - F3	Shift - F5	Shift - F7	Legacy	USB 1.x	USB 2.0	Comment
off	off	off	on	on	on	3.
on	off	off	off	on	on	Default
off	on	off	on	off	off	1., 2.
on	on	off	on	off	off	1., 2.
off	off	on	on	on	off	3.
on	off	on	off	on	off	
off	on	on	on	off	off	
on	on	on	on	off	off	2.

1. **Shift - F5** disables both USB 1.x and USB 2.0.

Note: Pressing **Shift - F5** during startup will considerably reduce the time it takes to launch the SafeGuard POA. However, if your computer uses a USB keyboard or USB mouse, they might be disabled when pressing **Shift - F5**.

The POA may use the USB keyboard via BIOS SMM. There is no USB token support.

2. If no USB support is active, the SafeGuard POA tries to use BIOS SMM instead of backing up and restoring the USB controller. The Legacy mode may work in this scenario.
3. Legacy support is active, USB is active. The SafeGuard POA tries to back up and restore the USB controller. The system might hang depending on the BIOS version used.

Note: The changes that can be carried out using the hotkeys may already have been specified during SafeGuard Enterprise Client installation using an `.mst` file.

When you change hardware settings by using the hotkeys in the SafeGuard POA, a dialog is displayed prompting you to save the changed settings. This dialog shows an overview of the

configuration that will be saved. To save your changes, click **Yes**. When you restart your computer, the new settings become active. If you click **No**, your changes are not saved, and the old configuration remains active when you restart your computer.

By pressing **F5** in any SafeGuard POA dialog, you can open a dialog showing the hotkeys configuration used to start the POA. If hotkeys were changed during the startup, the relevant key states are shown in blue. Blue means that the key was used in this state to start the SafeGuard POA, but it has not been saved yet. Unchanged values are shown in black. To close the dialog, press **F5** again or press **Return**.

For details see <http://www.sophos.com/en-us/support/knowledgebase/107785.aspx>.

4.9.2 Function keys in the logon dialog

Note: The function keys are not hotkeys.

F2 = abort Autologon.

F5 = displays a dialog showing the hotkey configuration used to start the SafeGuard POA.

F8 = change password in the SafeGuard POA. Use instead of the **Enter** key to trigger a password change in the SafeGuard POA after logging on.

Alt + Shift (left-hand **Alt** and left-hand **Shift** keys) = change keyboard from German to English (or the reverse).

Cancel and prepare SafeGuard POA for shutdown

Ctrl + Alt + Del = if authentication has failed but you need to shut down the computer safely. This key combination has the same function as the **Shutdown** button.

Note: If fingerprint logon is activated, you can use **Ctrl + Alt + Del** to change to the SafeGuard POA dialog for logging on with a user name and password. For further information, see [Logging on with the Lenovo Fingerprint Reader](#) (page 24).

4.10 Password synchronization

SafeGuard Enterprise automatically detects when the Windows password has been changed and no longer corresponds to the one stored in the SafeGuard Enterprise Database. This may happen if the Windows password has been changed through a VPN on another computer, or in Active Directory.

If SafeGuard Enterprise detects this situation, you are prompted to enter the old password. Afterwards, the password stored by SafeGuard Enterprise is updated with the new Windows password.

Password synchronization will take place in the following two situations:

- During the logon process.
- During a Windows lock/unlock procedure.

5 Logging on to Windows

SafeGuard Enterprise offers an additional authentication method.

If you clear the **Pass through logon to Windows** check box in the logon dialog of the SafeGuard Power-on Authentication, the Windows logon dialog is displayed. In this dialog, you can also select a different authentication method.

Note: Using a different authentication method does not mean that SafeGuard Enterprise is inactive on your computer. In this case, the logon at SafeGuard Enterprise is not done during the Windows logon, but after the Windows logon.

5.1 Log on with SafeGuard Enterprise

Usually, you are automatically logged on to Windows after entering your password at the SafeGuard Power-on Authentication (POA). If you clear the **Pass through logon to Windows** check box in the SafeGuard POA logon dialog, and use the SafeGuard Enterprise method for logging on to Windows, SafeGuard Enterprise is available with its complete functionality after you log on to Windows.

The required keys are available, and all data is encrypted and decrypted according to the policies defined.

5.2 Log on with the Windows authentication method

In the Windows logon dialog, you can select an alternative authentication method for logging on to Windows instead of the SafeGuard Enterprise authentication method.

If you use the Windows authentication method, the logon to SafeGuard Enterprise is performed after the logon to the operating system.

After logging on to Windows, the SafeGuard Enterprise authentication application is started automatically, if necessary, to achieve full SafeGuard Enterprise functionality.

Depending on the logon settings in central administration, either a dialog for entering user credentials or a PIN entry dialog is displayed.

1. Enter your credentials or the PIN, and click **OK**.

Now the SafeGuard Enterprise functionality is available and you can, for example, access encrypted data, if you have the necessary key.

6 Logging on with the Lenovo Fingerprint Reader

Note: Logon with the Lenovo Fingerprint Reader is only supported for Windows 7 (BIOS) endpoints.

Users must remember many different passwords and PINs in order to access their computers, applications, and networks. With a fingerprint reader, all you need to do is swipe your finger over the reader to log on instead of using a password or token.

You cannot lose or forget your credentials. Nor can unauthorized individuals guess this information. Using fingerprint readers thus simplifies the logon process and increases security.

SafeGuard Enterprise supports fingerprint logon for SafeGuard Power-on Authentication as well as the Windows logon phase. For example, you can log on to a Lenovo notebook simply by swiping your finger over the fingerprint reader integrated into the notebook. The rest of the logon procedure then runs automatically. You can also lock and unlock your desktop in Windows by swiping your finger over the fingerprint reader.

Fingerprint readers are integrated directly into certain Lenovo notebooks. You can also use an external USB keyboard for fingerprint logon.

Note:

- Only one fingerprint reader may be connected to a computer at any given time.
- Token and fingerprint logon procedures cannot be combined on the same computer.
- Remote fingerprint logon is not supported.

6.1 Requirements

The following requirements must be satisfied in order to use fingerprint logon.

General requirements

- Lenovo hardware
- Lenovo Fingerprint Reader in the notebook or a USB keyboard with a fingerprint reader
- The latest BIOS (recommended)
- SafeGuard Enterprise
- The recommended vendor-specific software version must be installed before SafeGuard Enterprise:
 - ThinkVantage Fingerprint for AuthenTecor
 - ThinkVantage Fingerprint for UPEK.

- The security officer must have activated fingerprint logon by policy.

System requirements

- Windows 7, 32 bit, 64 bit
- Windows 8, 32 bit, 64 bit

Supported hardware

For information on supported fingerprint logon hardware, refer to <http://www.sophos.com/en-us/support/knowledgebase/108789.aspx>.

Supported software

For information on supported fingerprint software, refer to <http://www.sophos.com/en-us/support/knowledgebase/111626.aspx>.

6.2 Enroll fingerprints

In order to log on to your notebook/PC with a fingerprint, you must first enroll one or more fingerprints using the recommended vendor-specific software. The enrollment process links your enrolled fingerprint with your credentials (user name and password).

Prerequisites: The following procedure assumes that both the recommended vendor-specific software and SafeGuard Enterprise are installed.

1. Log on at the SafeGuard Power-on Authentication (POA) by entering your user name and password.
2. Register one or more of your fingerprints by using the installed vendor-specific software. This registration links your fingerprint with your Windows credentials.
 - a) Refer to the documentation for the ThinkVantage Fingerprint software for instructions on how to enroll a fingerprint.
 - b) Enable the option **POA password in BIOS**. (UPEK only. For AuthenTec this step is not necessary.)
 - c) To use fingerprint logon in the SafeGuard POA, you first have to log on to Windows once with your fingerprint to transfer your credentials to the fingerprint reader. For UPEK you only have to swipe an enrolled fingerprint over the fingerprint reader. For AuthenTec you also have to enter your Windows password at first logon.
3. Restart your computer.
4. To test your enrolled fingerprint, swipe your finger over the fingerprint reader after restarting the computer.

If your fingerprint matches the enrolled one, you are automatically logged on to Windows.

6.3 Log on to SafeGuard Power-on Authentication with a fingerprint

Prerequisites:

- The security officer must have set up the fingerprint option in the relevant **Authentication** policy.
- You must have enrolled one or more fingerprints.

1. Restart your computer.

The SafeGuard POA dialog for logging on with a fingerprint is displayed.

2. Swipe one of your enrolled fingers over the reader.

If the software recognizes your fingerprint, SafeGuard Power-on Authentication reads your credentials and sends them to Windows.

Note: The logon procedure uses icons with short text messages as prompts, notifications, and warnings, see [Icons used in the logon process](#) (page 26).

You are automatically logged on to Windows without any further requests for your data.

Note:

- If the enrollment process in Windows was not completed successfully (for example, after enrolling fingerprints, you have not logged off from and logged on again to Windows) a match with the fingerprints enrolled will be found in the SafeGuard POA.

However, there will not be any credentials. In this case, an error message is displayed, prompting you to log on with your user name and password, although this does not pass you through to Windows. Your credentials are transferred to the fingerprint reader.

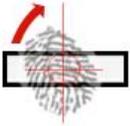
- In the policies that apply to you, the security officer specifies whether pass-through to Windows has been enabled or disabled and whether you can change these settings in the SafeGuard POA dialog for logging on with a user name and password, see [Log on with a user name and password](#) (page 29).

6.3.1 Icons used in the logon process

When you log on at the SafeGuard Power-on Authentication with a fingerprint, the system uses icons as prompts, notifications, and warnings. These icons are displayed during the logon process, along with a short text message.

	Prompts you to swipe your finger over the fingerprint reader.
---	---

	<p>Indicates that fingerprint logon is not currently enabled. This can occur, for example, if the fingerprint logon module has not yet been initialized.</p>
	<p>Indicates that the fingerprint reader is working and is busy.</p>
	<p>Indicates that the fingerprint was read successfully and a match was found.</p>
	<p>Indicates that the fingerprint was read successfully, but no match was found.</p>
	<p>Indicates that the fingerprint could not be read. Swipe your finger across the fingerprint reader again.</p>
	<p>Indicates that you have placed your finger too far to the left (or too far to the right). Move your finger to the center of the fingerprint reader.</p>
	<p>Indicates that your finger swipe was too skewed. Swipe your finger across the fingerprint reader again.</p>

	
	<p>Indicates that you moved your finger too fast. Swipe your finger across the fingerprint reader again.</p>
	<p>Indicates that your finger swipe was too short. Swipe your finger across the fingerprint reader again.</p>

6.3.2 Failed logon attempts

If the system is unable to read your fingerprint after five attempts, it considers this to be a failed logon attempt and logs it as an event. In this case, a logon delay goes into effect.

If the system was able to read your fingerprint without errors, but did not find a match with the registered fingerprint after five attempts, it also considers this to be a failed logon attempt and logs it as an event. In this case, a logon delay also goes into effect.

The logon delay period increases with every failed logon attempt.

6.3.3 Log on with a user name and password

Even if fingerprint logon is enabled, you can still log on at the SafeGuard Power-on Authentication with your user name and password, for example, if your fingerprint reader does not work.

1. Press the **Esc** key or **Ctrl+Alt+Del** in the SafeGuard POA dialog for logging on with a fingerprint.

The SafeGuard POA dialog for logging on with a user name and password is displayed.

Note: If you press **Ctrl+Alt+Del** in the SafeGuard POA dialog for logging on with a user name and password, the computer shuts down. In this dialog, **Ctrl+Alt+Del** corresponds to the **Shutdown** button.

The SafeGuard POA dialog for logging on with a user name and password is also displayed automatically if a fingerprint reader is unavailable or if the system does not find any user data on the fingerprint reader.

Note: Logging on with a user name and password is also enabled automatically if the local cache is corrupt. If this happens, your computer will be locked, and you must log on using a Challenge/Response procedure.

2. Optionally, press **Esc** again to return to the SafeGuard POA dialog for logging on with a fingerprint.

If you pressed **Esc** to switch to the SafeGuard POA dialog for logging on with a user name and password, you can still log on by swiping your finger over the fingerprint reader without having to return to the SafeGuard POA fingerprint logon dialog first.

6.4 Changing your password

1. If fingerprint logon is enabled in SafeGuard Power-on Authentication, you can change your password in Windows by pressing **Ctrl+Alt+Del**.

When you change your password, the system prompts you to swipe your finger over the fingerprint reader in order to transfer your new password to the fingerprint reader.

Note: Whenever you change your password, the change applies to all your enrolled fingerprints.

6.4.1 Synchronize your password

If your Windows password no longer matches the password stored on the fingerprint reader, for example in cases where you changed your password, but the new password was not transferred to the fingerprint reader, you can synchronize your password:

1. Restart your computer.
2. Press the **Esc** key or **Ctrl+Alt+Del** in the SafeGuard POA dialog for logging on with a fingerprint.

The SafeGuard POA dialog for logging on with a user name and password is displayed.

3. Click **Options**, and clear the **Pass through logon to Windows** check box.

Note: In the policies that apply to you, the security officer specifies whether pass-through to Windows has been enabled or disabled and whether you can change these settings in the SafeGuard POA dialog for logging on with a user name and password.

4. Log on with your password.
5. The Windows logon dialog is displayed. Swipe one of your enrolled fingers over the fingerprint reader.
6. The system recognizes the fingerprint, but Windows rejects the password linked to the fingerprint. This is not viewed as a failed logon attempt, however, so no logon delay goes into effect.

A message indicating that the password was changed is displayed, and the system prompts you to enter your current Windows password.

7. Enter the correct Windows password.

Note: If you enter an incorrect Windows password here, a failed logon attempt is logged, and a logon delay goes into effect. If you close the input prompt without entering a password, a failed logon attempt is likewise logged, and a logon delay goes into effect.

A successful transfer of the password completes the password synchronization process and you can then use the password for your logon.

6.5 Fingerprint logon recovery

If fingerprint logon does not work and you have forgotten the password required to log on, SafeGuard Enterprise offers the following recovery methods:

- [Recovery with Local Self Help](#) (page 64).
- [Recovery with Challenge/Response or recovery key](#) (page 73).

The recovery methods available on your computer depend on the settings specified by the security officer.

To initiate recovery, click the **Recovery** button in the fingerprint logon dialog.

Note: Due to a recovery procedure, you may have to change your password when you start your computer, for example if you have forgotten your password. In this case, the system also offers to update your fingerprint credentials.

7 Disk encryption

For disk encryption, SafeGuard Enterprise offers the following depending on the operating system in use on the endpoints:

- **Windows 7 endpoints:**
 - SafeGuard full disk encryption with SafeGuard Power-on Authentication, see [SafeGuard full disk encryption](#) (page 31)
 - BitLocker Drive Encryption with Windows logon, see [BitLocker Drive Encryption](#) (page 34)
- **Windows 8 endpoints:** BitLocker Drive Encryption with Windows logon, see [BitLocker Drive Encryption](#) (page 34).

7.1 SafeGuard full disk encryption

SafeGuard Enterprise provides transparent full disk encryption in a volume-based manner. In the security policies, your security officer defines the volumes that are to be encrypted.

7.1.1 Transparent encryption

The files on an encrypted volume are encrypted transparently. You do not see any prompts for encryption or decryption when opening, editing, and saving files. When you open the files, they are decrypted and you can edit them. When you close or save the files, they are encrypted again.

If you copy or move files (also with **Save as**) from an encrypted volume to an unencrypted file location on your computer, they are decrypted. The files are stored in the new file location in plaintext.

7.1.2 Initial encryption

During initial configuration of SafeGuard Enterprise protected computers encryption policies may be created and distributed in a configuration package to the computers.

After the first encryption policy has been deployed to your computer, initial encryption is performed according to the policy settings received.

7.1.2.1 Initial encryption for volume-based encryption

As soon as your computer receives a policy for volume-based encryption after SafeGuard Enterprise installation, initial volume-based encryption is started automatically.

Volume-based initial encryption runs in the background and you can continue working with your computer.

Note: During initial encryption of the system partition (that is the partition where the hiberfil.sys file is located) do not hibernate the computer. After initial encryption of the system partition is completed, restart the computer to make sure that hibernation works properly again.

7.1.2.2 Restrictions for initial encryption of SafeGuard Enterprise protected computers

During initial configuration of SafeGuard Enterprise protected computers encryption policies may be created and distributed in a configuration package to the computers. When the SafeGuard Enterprise Client is not connected to a SafeGuard Enterprise Server immediately after the configuration package is installed, but is temporarily offline, only encryption policies with the following specific setting become immediately active on the SafeGuard Enterprise protected computer:

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

For all other policies involving encryption with user-defined keys to become active on a SafeGuard Enterprise protected computer, the respective configuration package also has to be reassigned to the computer. The user-defined keys will then only be created after the SafeGuard Enterprise Client has been connected to SafeGuard Enterprise Server again.

This is because the **Defined Machine Key** is created on the SafeGuard Enterprise protected computer at the first restart after installation, whereas the user-defined keys can only be created on the computer after it has been registered at the SafeGuard Enterprise Server.

7.1.3 Volume-based full disk encryption

Volume-based encryption for a volume on the SafeGuard Enterprise protected computer starts automatically if the security officer has defined the policy accordingly.

1. A dialog is displayed, and you are prompted to select a key enabling you to access the volume.

Note: Every user whose key ring includes this key can access this volume. The security officer defines the scope of keys offered. If the security officer has defined a specific key, you cannot select a key.

2. Click **OK** to start encryption.

During the encryption process, an Encryption Viewer shows the encryption progress of the volume to be encrypted. If available, it also shows existing encrypted volumes. The Encryption Viewer is shown in minimized view on the Windows taskbar. You can open it by clicking the icon. If you want the Encryption Viewer minimized, you can request a notification that encryption has been completed by selecting **Show notify before close**. The viewer automatically closes when encryption is complete. You can use the encrypted volume like any unencrypted volume on your computer.

Note:

- Volume-based encryption/decryption is not supported for volumes without a drive letter assigned.
- For Windows 7 Professional, Enterprise and Ultimate, a system partition is created on endpoints without a drive letter assigned. This system partition cannot be encrypted by SafeGuard Enterprise.
- If an encryption policy exists for a volume or a volume type and encryption of the volume fails, the user is not allowed to access it.
- Endpoints can be shut down and restarted during encryption/decryption.
- If decryption is followed by an uninstallation, we recommend that the endpoint is not suspended or hibernated during decryption.
- If after volume encryption a new policy is applied to an endpoint that allows decryption, the following applies: After a complete volume-based encryption, the endpoint must be restarted at least once before decryption can be started.

Note:

In contrast to SafeGuard BitLocker Drive Encryption, SafeGuard volume-based encryption does not support GUID partition table (GPT) disks. Installation will be aborted if such a disk is found. If a GPT disk is added to the system later, volumes on the disk will get encrypted. Please be aware that the SafeGuard recovery tools - such as BE_Restore.exe and recoverkeys.exe - cannot handle such volumes and Sophos strongly recommends to avoid encrypting GPT disks. To decrypt volumes that were accidentally encrypted, please change your SGN policies accordingly and have the user decrypt them.

7.1.3.1 Volume access restrictions

SafeGuard Enterprise denies access to volumes in the following cases:

Volumes with failed encryption

If a policy exists that specifies that a volume or a volume type is to be encrypted, and the encryption process fails, access to the volume is denied.

When you try to access the volume, a relevant message is displayed.

Unidentified File System Objects

Unidentified File System Objects are volumes that cannot be clearly identified as plaintext or encrypted by SafeGuard Enterprise.

If a policy exists that specifies that a volume of this type is to be encrypted and the encryption process fails, access to this volume is denied. When you try to access the volume, a relevant message is displayed.

If there is no encryption policy for an Unidentified File System Object, you can access the volume.

7.2 BitLocker Drive Encryption

BitLocker Drive Encryption is a full disk encryption feature with pre-boot authentication that is included with Windows operating systems. It is designed to protect data by providing encryption for boot and data volumes. SafeGuard Enterprise manages BitLocker Drive Encryption and provides additional features.

7.2.1 Encryption policies for BitLocker

The security officer can create a policy for encryption in the SafeGuard Management Center and distribute it to the BitLocker endpoints where it is executed.

The BitLocker clients are managed transparently in the SafeGuard Management Center. The same encryption policy can be used for Mac, SafeGuard full disk encryption and BitLocker clients. SafeGuard Enterprise knows the status of the clients and selects BitLocker encryption accordingly.

7.2.2 Authentication with BitLocker

BitLocker offers a range of authentication options. The security officer can set the various logon modes in a policy in the SafeGuard Management Center and distribute it to the BitLocker endpoints.

The following logon modes exist for SafeGuard Enterprise BitLocker users:

- TPM
- TPM + PIN
- TPM + Startup Key
- Startup Key (without TPM)
- Password (without TPM)

You must provide these credentials when you start your BitLocker endpoint.

Trusted Platform Module (TPM)

The TPM is a smartcard-like module on the motherboard performing cryptographic functions and digital signature operations. It can create, store and manage user keys. It is protected against attacks.

Startup Key on USB memory stick

The external keys can be stored on an unprotected USB memory stick. You must insert the USB memory stick for authentication at startup.

7.2.3 Encryption on a BitLocker-protected computer

When the encryption policy is sent to a BitLocker-protected computer and before the computer restarts and performs the initial encryption, the encryption keys are generated by BitLocker. Depending on the system used the behavior differs slightly.

Endpoints with TPM

Your security officer can define TPM, TPM + PIN, TPM + Startup Key, Startup Key or Password as the logon mode for BitLocker. If a logon mode with TPM is set, BitLocker stores its own encryption keys in a hardware device called the Trusted Platform Module (TPM) security hardware. The keys are not stored on the computer's hard disk. The TPM must be accessible by the basic input/output system (BIOS) during startup. When you start your computer, BitLocker will get these keys from the TPM automatically.

Endpoints without TPM

If your computer is not equipped with a TPM, you will either be prompted for a password or asked to create a BitLocker startup key using a USB memory stick to store the encryption keys. A dialog appears displaying valid target drives on which to store the startup key. You will have to insert the memory stick each time you start the computer.

Note: For **boot volumes** it is essential that you have the startup key available when you start your endpoint. Therefore the startup key can only be stored on removable media.

For data volumes the BitLocker startup key can be stored on a boot volume that is already encrypted. This will be done automatically, if the security officer specified **Auto-Unlock** as the logon mode for non-boot volumes. Otherwise, select a removable device that is displayed under **Valid target drives** as storage location.

BitLocker recovery keys

For BitLocker recovery, SafeGuard Enterprise offers a Challenge/Response procedure that allows information to be exchanged confidentially and the BitLocker recovery key to be retrieved from the helpdesk, see [Challenge/Response for BitLocker users](#) (page 79) and [BitLocker recovery key](#) (page 80).

To enable recovery with Challenge/Response, the required data has to be available to the helpdesk. The data required for recovery is uploaded and saved in the SafeGuard Enterprise database.

Note: If a BitLocker-encrypted volume in a computer is replaced by a new BitLocker-encrypted volume, and the new volume is assigned the same drive letter as the previous volume, SafeGuard Enterprise only saves the recovery key of the new volume. You need to back up the key of the previous volume using the backup mechanisms offered by Microsoft.

Managing volumes already encrypted with BitLocker

If there are any volumes already encrypted with BitLocker on your computer when SafeGuard Enterprise is installed, SafeGuard Enterprise takes over the management of these volumes.

Encrypted boot volumes

- Depending on the SafeGuard Enterprise BitLocker support used, you may be prompted to reboot the computer. It is important that you reboot the computer as early as possible.
- If a SafeGuard Enterprise encryption policy applies for the encrypted volume:
 - **BitLocker Challenge/Response** is installed: Management is taken over and SafeGuard Challenge/Response is possible.
 - **SafeGuard BitLocker** is installed: Management is taken over and SafeGuard recovery is possible.
- If no SafeGuard Enterprise encryption policy applies for the encrypted volume:
 - **BitLocker Challenge/Response** is installed: Management is not taken over and SafeGuard Challenge/Response is not possible.
 - **SafeGuard BitLocker** is installed: SafeGuard recovery is possible.

Encrypted data volume

- If a SafeGuard Enterprise encryption policy applies for the encrypted volume:
Management is taken over and SafeGuard recovery is possible.
- If no SafeGuard Enterprise encryption policy applies for the encrypted volume:
SafeGuard recovery is possible.

Important: If a BitLocker-encrypted volume in a computer is replaced by a new BitLocker-encrypted volume, and the new volume is assigned the same drive letter as the previous volume, SafeGuard Enterprise only saves the recovery key of the new volume. You need to back up the key of the previous volume using the backup mechanisms offered by Microsoft.

Note: It may happen that SafeGuard Enterprise is not able to take over the management of a volume that is already encrypted. In such a case, you cannot use SafeGuard Enterprise for recovery. Contact your security officer.

7.2.4 Initial encryption on a BitLocker-protected endpoint

Depending on the logon mode the security officer specified for your endpoint, the behavior of SafeGuard Enterprise BitLocker support differs slightly.

In any case you will be presented with a dialog that offers you the option to proceed with encryption or to postpone it.

If you confirm that you want to save, restart and/or encrypt, encryption still does not start right away. A hardware test is performed to make sure that your endpoint meets the requirements for SafeGuard Enterprise BitLocker encryption. The system performs a reboot and checks whether all hardware requirements are met. If for example the TPM or USB memory stick is not available or accessible you will be asked to store the external key on another device. The system also

checks whether you are able to provide the credentials correctly. If you cannot provide your credentials, the computer boots anyway, but encryption will not start. You will be asked again for your PIN or password. After a successful hardware test BitLocker encryption will start.

If you select **Postpone**, encryption will not be started and you won't be asked again to encrypt this volume until:

- a new policy arrives,
- the BitLocker encryption status of any volume changes, or
- you log on to the system again.

Note: If BitLocker Drive Encryption is managed by SafeGuard Enterprise for your operating system drive or fixed data volumes, do not turn on BitLocker manually for these volumes.

7.2.4.1 Save startup key

If your security officer specified **TPM + Startup Key** or **Startup Key** as the logon mode, you will have to specify the location where the startup key is saved. Insert a USB memory stick to store the key. Do not use an encrypted USB memory stick. The valid target drives for the startup key are listed in the dialog. Later you will have to insert the key each time you start the computer.

Select the target drive and click **Save and Restart**.

7.2.4.2 Set password

If your security officer specified **Password** as the logon mode, you are asked to enter and confirm your new password. Later you will need this password each time you start your computer. The length and complexity that are required for the password depend on group policy objects your security officer specified. You are informed about password requirements in the dialog.

Note: If you use special characters in your password, take into account that the keyboard layout you use might be different from the EN-US keyboard layout supported by BitLocker. Consider setting your keyboard layout temporarily to EN-US for the purpose of setting the password.

7.2.4.3 Set PIN

If your security officer specified **TPM + PIN** as the logon mode, you are asked to enter and confirm your new PIN. Later you will need this PIN each time you start your computer. The length and complexity that are required depend on group policy objects your security officer specified. You are informed about PIN requirements in the dialog.

Note: If your security officer enabled so-called enhanced PINs you can use special characters in your PIN. Take into account that the keyboard layout you use might be different from the EN-US keyboard layout supported by BitLocker. Consider setting your keyboard layout temporarily to EN-US for the purpose of setting the PIN.

7.2.4.4 Dialog for TPM-only

If your security officer specified **TPM** as the logon mode, you just need to confirm the restart and encryption of your endpoint.

7.2.5 Decryption with BitLocker

Computers encrypted with BitLocker cannot be decrypted automatically. Decryption must be carried out using either **BitLocker Drive Encryption** in the **Control Panel** or the Microsoft command-line tool "Manage-bde".

8 SafeGuard Data Exchange

SafeGuard Data Exchange allows you to encrypt data stored on removable media that are connected to your computer, and exchange it with other users. All encryption and decryption processes are run transparently and involve minimum user interaction.

Only users who have the appropriate keys can read the contents of the encrypted data. All subsequent encryption processes are run transparently. Transparent encryption means that data that has been encrypted and saved is automatically decrypted by an application when the data is accessed again.

When you save the relevant file, it is automatically encrypted again. During daily work you will not notice that the data is encrypted. However, when you disconnect the removable media, the data remains encrypted and is protected against unauthorized access. Unauthorized users can access the files physically, but they cannot read them without SafeGuard Data Exchange and the relevant key.

Note: The behavior of SafeGuard Data Exchange on your computer is centrally defined by the security officer.

In central administration, the security officer defines how data on removable media is handled. The security officer can, for example, define encryption as mandatory for files stored on any removable media. In this case, all unencrypted files existing on the device are initially encrypted. In addition, all new files saved to removable media are encrypted. If existing files are not to be encrypted, the security officer can choose to allow access to existing unencrypted files. In this case, SafeGuard Data Exchange does not encrypt the existing unencrypted files. However, new files are encrypted. So you can read and edit the existing unencrypted files, but as soon as you rename them, they are encrypted. The security officer can also specify that you are not allowed to access unencrypted files, and they remain unencrypted.

There are two ways to exchange encrypted files stored on removable media:

- **SafeGuard Enterprise is installed on the recipient's computer:** You can use keys available to both of you, or you can create a new key. If you create a new key, you have to provide the data recipient with the passphrase for the key.
- **SafeGuard Enterprise is *not* installed on the recipient's computer:** SafeGuard Enterprise offers SafeGuard Portable. This utility can be automatically copied to the removable media in addition to the encrypted files. Using SafeGuard Portable and the relevant passphrase, the recipient can decrypt the encrypted files and encrypt them again without SafeGuard Data Exchange being installed on their computer.

Important: When extracting a ZIP archive using the built-in archiver of Microsoft Windows the process stops as soon as an encrypted file is encountered for which the key is not available. The user receives a message that access was denied, but is not informed that there are files that have not been processed and hence are missing. Other archivers, for example 7-Zip, work fine with ZIP archives containing encrypted files.

8.1 Settings for handling removable media

If SafeGuard Data Exchange is installed on your computer, removable media will be handled as predefined by your security officer. A security officer can define the following settings for SafeGuard Data Exchange (a combination of several settings is also possible):

- **Initial encryption of all files:** In this case, encryption of all data on removable media starts as soon as the device is connected to your computer. This setting ensures that the removable media contain only encrypted data. When encryption starts, you are asked to select a key, or a predefined key will be used.
- **User may cancel initial encryption:** When initial encryption starts, a dialog is displayed that allows you to cancel initial encryption.
- **User is allowed to access unencrypted files: No:** In this case, SafeGuard Data Exchange only accepts encrypted data on removable media. If unencrypted data exists on removable media, the system will not allow you to access it. Only after encrypting the files will you be able to access the data.
- **User may decrypt files:** In this case, you can explicitly decrypt files on removable media. A file that has been explicitly decrypted remains as plaintext on the removable storage medium, if it is, for example, transferred to a third party.
- **User may define a media passphrase for devices:** You are prompted to enter a media passphrase the first time you connect removable media.
- **Plaintext folder:** The security officer may define a plaintext folder that will be created on all of your removable media. Files in this folder are not encrypted by SafeGuard Data Exchange.
- **User is allowed to decide about encryption:** When you connect removable media to your computer, a message box is displayed asking you whether you want to encrypt the files on the attached media. In addition and if activated by policy, you can select if this setting should be remembered and always be applied to the relevant media. If you select **Remember setting and do not show this dialog again**, the message box will not be displayed again for the relevant media. In this case, the new command **Re-activate encryption** becomes available in the context menu of the relevant device in Windows Explorer. Select this command to revert your decision about encryption for the relevant device. If this is not possible, for example because you do not have the relevant rights for the device, an error message is displayed. After you have reverted your decision, you are prompted to decide about encryption for the relevant device again.

8.2 Single media passphrase for all removable media connected to the computer

SafeGuard Data Exchange supports the definition of a single media passphrase that will give you access to all removable devices connected to your computer. This is independent of the key that is used for encrypting the individual files.

If specified, access to encrypted files can be granted by entering only one media passphrase. The media passphrase is bound to computers for which you have logon permission. This means that you use the same media passphrase on each computer.

The media passphrase can be changed and will be synchronized automatically on each computer you are working on, as soon as you connect removable media to this computer.

A media passphrase is useful in the following scenarios:

- You want to use encrypted data on removable media on computers where SafeGuard Enterprise is not installed (SafeGuard Data Exchange in combination with SafeGuard Portable).
- You want to exchange data with external users: By providing them with the media passphrase, you can give them access to all files on the removable media with one single passphrase, regardless of which key was used for encrypting the individual files.

You can also restrict access to all files by only providing the external user with the passphrase of a specific key (a "local key," which can be created by a SafeGuard Data Exchange user). In this case the external user will only have access to files that are encrypted using this key. All other files will not be readable.

Note: A media passphrase is not necessary if you use SafeGuard Enterprise group keys to exchange data on removable media within a workgroup where the members share such a key. In this case - if specified by your security officer - access to encrypted files on removable media is fully transparent. You do not have to enter a passphrase or password. This is because group keys and media passphrases for removable media can be used simultaneously. Since the system automatically detects an available group key, access for users sharing this key is fully transparent. If no group key is detected, SafeGuard Data Exchange displays a dialog prompting the user to enter a media passphrase or the passphrase for a local key.

Supported media

SafeGuard Data Exchange supports the following removable media:

- Startup Keys
- External hard disks connected by USB or FireWire
- CD RW drives (UDF)
- DVD RW drives (UDF)
- Memory cards in USB card readers

8.3 Encrypting removable media

Encryption of unencrypted data on removable media either starts automatically as soon as you connect the media to the system, or you have to start the process manually. All subsequent encryption and decryption processes run transparently with nearly no user interaction.

8.3.1 Initial encryption

Encryption of unencrypted data on removable media either starts automatically as soon as you connect the media to the system, or you have to start the process manually. If you are entitled to decide whether files on removable media should be encrypted, you are prompted to do so when you attach removable media to your computer.

To start the encryption process manually:

1. Select **File encryption > Start encryption** from the right-click menu in Windows Explorer. If no specific key has been defined, a dialog is displayed for key selection.
2. Select a key, and click **OK**. All data contained on the removable media is encrypted.

The default key is used as long as no other key is set as the default. If you change the default key, the new one is used for initial encryption of removable media that are connected to the computer afterwards.

Note: To exchange data with users who have SafeGuard Enterprise installed on their computers but do not use the same key as you do, local user-generated keys or a media passphrase are required. These keys are also required for secure data exchange with users who do not use SafeGuard Enterprise. You can identify local keys by their prefix (Local_).

If **Encrypt plain files and update encrypted files** is selected, encrypted files with an existing key will be decrypted and encrypted again using the new key.

Cancelling initial encryption

If initial encryption is configured to start automatically, you may have the right to cancel initial encryption. In this case, the **Cancel** button is activated, a **Start** button is displayed, and the start of the encryption process is delayed for 30 seconds. If you do not click the **Cancel** button during this time period, initial encryption starts automatically after 30 seconds. If you click **Start**, initial encryption is started immediately.

Initial encryption for users with a media passphrase

If the usage of a media passphrase has been defined in a policy, you are prompted to enter the media passphrase before initial encryption. The media passphrase is valid for all of your removable media and is bound to your computer or to all computers for which you have logon permission.

Initial encryption will start automatically when you enter the media passphrase.

When you have entered the media passphrase once, initial encryption will start automatically when you connect a different device to your computer.

Note: Initial encryption does not start on computers where your media passphrase is not set.

8.3.2 Manual encryption

If you are entitled to decide whether files on removable media should be encrypted, you can start the encryption process manually. Doing so you can also encrypt files already encrypted using a different key.

To start the encryption process manually:

1. Select **File encryption > Start encryption** from the context menu in Windows Explorer. If no specific key has been defined, a dialog is displayed for key selection.
2. Select a key, and click **OK**. All data contained on the removable media is encrypted.

The default key is used as long as no other key is set as the default. If you change the default key, the new one is used for initial encryption of removable devices that are connected to the computer afterwards.

Note: To exchange data with users who have SafeGuard Enterprise installed on their computers but do not use the same key as you do, local user-generated keys or a media passphrase are required. These keys are also required for secure data exchange with users who do not use SafeGuard Enterprise. You can identify local keys by their prefix (Local_).

If **Encrypt plain files and update encrypted files** is activated, encrypted files with an existing key will be decrypted and encrypted again using the new key.

8.3.3 Transparent encryption

If the settings defined for your computer specify that files have to be encrypted on removable media, all encryption and decryption processes run transparently.

The files are encrypted when they are written to removable media and decrypted when they are copied or moved from removable media to another file location.

Note: The data is only decrypted if it is copied or moved to a location for which no other encryption policy applies. The data is then available at this location in plaintext. If a different encryption policy applies to the new file location, the data is encrypted accordingly.

8.3.3.1 Media passphrase

If specified by a policy, you are prompted to enter the media passphrase when you connect a removable device for the first time after the installation of SafeGuard Data Exchange.

If the dialog is displayed, specify a media passphrase. You can use this single media passphrase to access all encrypted files on your removable media, regardless of the key that was used to encrypt them.

The media passphrase is valid for all devices you connect to the computer. The media passphrase can also be used with SafeGuard Portable and allows you to access all files, regardless of the key that was used to encrypt them.

8.3.3.2 Change/reset media passphrase

You can change your media passphrase at any time using **Change Media Passphrase** from the System Tray Icon menu. A dialog is displayed in which you enter the old and new media passphrases and confirm the new one.

If you have forgotten your media passphrase, this dialog also provides an option to reset it. If you select the **Reset Media Passphrase** option and click **OK**, you are informed that your media passphrase will be reset at the next logon.

Log off immediately and log on again. You are informed that there is no media passphrase on your computer and prompted to enter a new one.

8.3.3.3 Media passphrase synchronization

The media passphrase on your devices and on your computer will be synchronized automatically. If you change the media passphrase on your computer and connect a device that still uses an old version of the media passphrase, you will be informed that the media passphrases have been synchronized. This is true for all computers for which you have logon permission.

Note: After you have changed your media passphrase, you should connect all your removable media with your computer. This ensures that the new media passphrase is used on all your devices immediately (synchronization).

8.4 Exchanging data using SafeGuard Data Exchange

The following are typical examples of secure data exchange with SafeGuard Data Exchange:

- Exchanging data with SafeGuard Enterprise users who have at least one key that is also included in your key ring.

In this case, encrypt the data on the removable media using a key that is also included in the recipient's key ring (for example, on his/her notebook). The recipient can use the key to access the encrypted data transparently.

- Exchanging data with SafeGuard Enterprise users who do not have the same keys as you do.

In this case, create a local key and encrypt the data using this key. Keys created locally are secured by a passphrase and can be imported by SafeGuard Enterprise. You provide the data's recipient with the passphrase. Using the passphrase, the recipient can import the key and access the data.

- Exchanging data with users without SafeGuard Enterprise

For users who do not have SafeGuard Enterprise installed on their machines, SafeGuard Portable is available. To exchange data using SafeGuard Portable, local keys must also be used in combination with a passphrase.

In addition, SafeGuard Portable has to be copied to the removable storage medium. You also have to provide the recipient of encrypted data with the relevant passphrase. Using the passphrase and SafeGuard Portable, the user can decrypt the encrypted files, edit them, for example, and save them encrypted again on the removable storage medium. As SafeGuard Portable is a self-sufficient application, no additional software needs to be installed on the computer in order to access encrypted data.

Note: The security officer determines whether SafeGuard Portable is copied to removable media in the security policy that applies to you.

8.4.1 Import keys from a file

If you have received removable media containing encrypted data or want to access Cloud Storage data in a shared folder which has been encrypted using user-defined local keys, you can import the key required for decryption to your private key ring.

To import the key, you need the relevant passphrase. The person who encrypted the data has to provide you with the passphrase.

1. Select the relevant file on the removable media and click **File encryption > Import key from file**.
2. Enter the passphrase in the dialog that is displayed.

The key is imported, and you can access the file.

8.4.2 Create local keys

1. Right-click the SafeGuard Enterprise System Tray Icon on the Windows taskbar or right-click a volume/folder/file.
2. Click **Create new key**.
3. In the **Create Key** dialog, enter a **Name** and a **Passphrase** for the key.

The internal name of the key is displayed in the field below.

4. Confirm the passphrase.

If you enter a passphrase that is not secure, a warning message is displayed. To increase the level of security, we recommend that you use complex passphrases. You can also decide to use the passphrase despite the warning message. The passphrase also has to correspond with the company policies. If it does not, a warning message is displayed.

5. If you opened the dialog using a right-click menu it contains the **Use as new default key for path** option. With the **Use as new default key for path** option, you can set the new key immediately as the default key for a volume or Cloud Storage synchronization folder.

The default key you specify here is used for encryption during normal operation. It will be used until a different one is set.

6. Click **OK**.

The key is created and becomes available as soon as the data has been successfully synchronized with the SafeGuard Enterprise Server.

If you define this key as the default key, all data copied to a removable storage medium or a Cloud Storage synchronization folder from now on is encrypted using this key.

For a recipient to be able to decrypt all data contained on a removable storage medium, you may have to re-encrypt the data on the device using the key created locally. To do so, select **File encryption > Start encryption** from the device's context menu in Windows Explorer. Select the required local key and encrypt the data. This is not necessary if you use a media passphrase.

8.5 Writing files to CDs using the Windows CD Writing Wizard

SafeGuard Data Exchange allows you to write encrypted files to CDs using the Windows CD Writing Wizard.

To do so, an encryption rule has to be specified for the CD recording drive. SafeGuard Data Exchange adds a dialog to the CD Writing Wizard. There you can specify how the files are written to CD (encrypted or plaintext).

Note: If there is no encryption rule for the CD recording drive, files are always written to the CD in plaintext. The SafeGuard Data Exchange dialog, where the encryption state of files to be written to the CD can be specified, is not displayed.

After you have entered a name for the CD, the SafeGuard Removable Disk Burning Extension is displayed.

Under **Statistics**, the following information is displayed:

- how many files are selected to be written to CD
- how many of the selected files are encrypted
- how many of the selected files are plaintext files

Under **Status**, the keys used for encrypting previously encrypted files are displayed.

For encrypting files that will be written to CD, the key that is specified in the encryption rule for the CD recording drive is always used.

Files to be written to CD may be encrypted with different keys if the encryption rule for the CD recording drive has been changed. If the encryption rule was deactivated when files were added, the relevant plaintext files can be found in the folder for files to be copied to CD.

Encrypt files on CD

If you want to encrypt the files when writing them to CD, click **(Re)Encrypt all files**.

If necessary, previously encrypted files are re-encrypted, and plaintext files are encrypted. On the CD, the files are encrypted using the key that was specified in the encryption rule for the CD recording drive.

Write files to CD in plaintext

If you select **Decrypt all files**, the files are first decrypted and then written to the CD.

Copy SafeGuard Portable to optical media

If you select this option, SafeGuard Portable will also be copied to the CD. This allows the reading and editing of files encrypted with SafeGuard Data Exchange without having SafeGuard Data Exchange installed.

8.5.1 Write CDs/DVDs

Windows provides a CD Writing Wizard for CDs/DVDs.

The SafeGuard Disc Burning Extension for the CD Writing Wizard is only available for burning CDs/DVDs in **Mastered** format. The wizard is only displayed if files are to be written on CDs/DVDs in **Mastered** format.

For the Live File System, no Recording Wizard is required. In this case, the recording drive is used like any other removable media. If there is an encryption rule for the recording drive, the files are encrypted automatically when they are copied to a CD/DVD.

8.6 SafeGuard Portable

Using SafeGuard Portable, you can exchange encrypted data on removable media with recipients who do not have SafeGuard Data Exchange installed on their machines. Data encrypted with SafeGuard Data Exchange can be encrypted and decrypted using SafeGuard Portable. This is achieved by automatically copying a program (SGPortable.exe) to the removable media.

Note: SafeGuard Portable only encrypts or decrypts files encrypted with AES 256.

Using SafeGuard Portable in combination with the relevant media passphrase gives you access to all encrypted files, regardless of which local key was used for encrypting them. The passphrase of a local key only gives you access to files that have been encrypted using this specific key. The recipient can decrypt encrypted data and encrypt it again.

Note: The media passphrase or the passphrase of a local key has to be communicated to the recipient beforehand.

The recipient can use existing keys created with SafeGuard Data Exchange for encryption, or create a new key with SafeGuard Portable (for example, for new files).

SafeGuard Portable does not have to be installed on or copied to your communication partner's computer. It remains on the removable media.

Note: As a SafeGuard Enterprise user, you usually do not need SafeGuard Portable. The following description assumes that users do not have SafeGuard Enterprise installed on their computer and therefore have to use SafeGuard Portable to edit encrypted data.

8.6.1 Editing files using SafeGuard Portable

You have received removable media containing files encrypted with SafeGuard Data Exchange, along with a folder named **SGPortable**. This folder contains the file **SGPortable.exe**.

1. Start SafeGuard Portable by double-clicking **SGPortable.exe**.

Using SafeGuard Portable, you can decrypt the encrypted data on the removable media and then re-encrypt it. SafeGuard Portable offers functionality that is similar to Windows Explorer.

In addition to the file details known from Windows Explorer (name, size, etc), SafeGuard Portable shows the **Key** column. This column indicates whether the relevant data is encrypted. If a file is encrypted, the name of the key used is displayed.

Note: You can only decrypt files if you know the relevant passphrase for the key used.

- To edit files on the removable media, click on the relevant file and choose the relevant command from the context menu (with a right-click) or from the **File** menu.

The following menu commands are available from the context menu:

Set Encryption Key	Opens the Enter Key dialog. In this dialog, you can generate an encryption key with SafeGuard Portable.
Encrypt	Encrypts the activated file on your removable media. The last-used key is used for encryption.
Decrypt	Opens the Enter Passphrase dialog. Enter the passphrase for decrypting the selected file in this dialog.
Encryption State	Displays a dialog and shows the file's encryption state.
Copy to	Copies the file to a folder of your choice and decrypts it.
Delete	Deletes the activated file from your removable media.

You can also select the commands **Open**, **Delete**, **Encrypt**, **Decrypt** and **Copy** with the icons shown on the toolbar.

8.6.1.1 Set encryption keys

To encrypt a file on removable media, and create an encryption key:

- From the context menu or from the **File** menu, select **Set Encryption Key**.

The **Enter Key** dialog is displayed.

- Enter a **Name** and a **Passphrase** for the key. **Confirm** the passphrase, and click **OK**.

The passphrase has to correspond to the company policies. If it does not, a warning message is displayed.

The key is created and will be used for encryption from now on.

8.6.1.2 Encrypt files on removable media

1. In SafeGuard Portable Explorer, select the file and, using the context menu, select **Encrypt**.

The file is encrypted with the key last used by SafeGuard Portable.

When saving new files on removable media using a drag-and-drop procedure in SafeGuard Portable Explorer, you are asked if you want to encrypt the files.

If this is the case, and there has been no encryption using SafeGuard Portable before, a dialog for setting the key opens. Enter the name of the key and the passphrase (and confirm the passphrase) in this dialog. Click **OK**.

2. Select the file to be encrypted with the key you have just set, and select **Encrypt** from the context menu or from the **File** menu.

The file is encrypted, and a message is displayed upon completion.

Note: The key last used and set by SafeGuard Portable is used for all subsequent encryption processes you perform with SafeGuard Portable, unless you set a new key.

8.6.1.3 Decrypt files on removable media

1. Select the file in SafeGuard Portable Explorer, and select **Decrypt** from the context menu.

The dialog for entering the media passphrase or the passphrase of a local key is displayed.

2. Enter the relevant passphrase (the sender has to provide you with this passphrase), and click **OK**.

The file is decrypted.

The media passphrase gives you access to all encrypted files on the removable media, regardless of which local key was used to encrypt them. If you only have the passphrase of a local key, you will only have access to files which are encrypted using this key.

When decrypting a file that has been encrypted using a key you have generated in SafeGuard Portable, this file is decrypted automatically.

After decrypting files on removable media and entering the key's passphrase, you do not have to enter it again the next time you encrypt or decrypt files that have been encrypted with the same key.

SafeGuard Portable stores the passphrase for as long as the application is running. The last key used by SafeGuard Portable is used for encryption.

After you decrypt the files, they are available in plaintext on the removable media. Files that have been decrypted are encrypted again when you close SafeGuard Portable.

8.6.1.4 Encrypt new files using SafeGuard Portable

You can also copy your own files in encrypted form onto removable media using SafeGuard Portable.

1. Drag the required files into SafeGuard Portable Explorer.

The system asks you whether you want to encrypt the relevant file.

2. Confirm that you want to encrypt the file. The file is encrypted with the key last used and copied to the removable media.

8.6.1.5 Determine the encryption state of a file

1. Select the file, and select **Encryption State** from the context menu or from the **File** menu.
The encryption state is also indicated in the **Key** column next to the file name in SafeGuard Portable Explorer.

8.6.2 Other operations using SafeGuard Portable

The following operations are also available:

- **Open:** This menu command is only available from the SafeGuard Portable **File** menu.
When you open an encrypted file with this menu command, you are prompted to enter your passphrase. Enter your passphrase, and click **OK**. The file is decrypted and opened.
- **Delete:** Deletes the selected file.
- **Copy to:** This menu command is only available in the context menu that you can open using your right mouse button in SafeGuard Portable Explorer.
Using this command, you can copy files from removable media to another volume on your computer.
- **Exit:** This menu command is only available from the SafeGuard Portable **File** menu.
Exit closes SafeGuard Portable.

9 SafeGuard File Encryption

The SafeGuard Enterprise module File Encryption offers file-based encryption on local drives and network locations. It was especially designed for work groups, to securely store data on network shares.

After a **File Encryption** policy has been assigned to your computer, files in the locations covered by the policy are transparently encrypted without user interaction:

- New files in the relevant locations are encrypted automatically.
- If you have the key for an encrypted file, you can read and modify the content.
- If you do not have the key for an encrypted file, access is denied.
- If you access an encrypted file on a computer where File Encryption is not installed, the encrypted content is shown.
- You can check the encryption state of your files with the SafeGuard Enterprise Explorer extensions for file-based encryption, see [Explorer extensions for file-based encryption](#) (page 60).

9.1 Encrypt according to policy

After a **File Encryption** policy has been assigned to your computer, existing files in the locations covered by the encryption policy are not encrypted automatically. An initial encryption has to be performed.

We recommend that you perform this initial encryption as soon as your computer receives a File Encryption policy although your security officer may automatically initiate this encryption task. This is to ensure that your data is encrypted according to the policy as soon as possible after you received a File Encryption policy.

Some applications create a new file after modifying the content of a file and delete the old one. Only for these applications it is true that the file is encrypted after modification. All other applications leave the file unencrypted if it was unencrypted before modification.

To start the encryption process manually:

1. Select **File encryption > Encrypt according to policy** from the context menu of the *My Computer* node in Windows Explorer.
2. The **SafeGuard File Encryption Wizard** is displayed.

All files in folders and subfolders covered by encryption rules are encrypted with the key defined in the relevant rule.

9.2 SafeGuard File Encryption Wizard

The SafeGuard File Encryption Wizard starts when you select the **Encrypt according to policy** command in the context menu of the *Computer* node or the **Start encryption** command from the context menu of folders and files in Windows Explorer.

It checks all folders that are defined in an encryption rule for the user:

- Plain files that should be encrypted will be encrypted with the key defined in the rule.
- Encrypted files that should be encrypted with a different key will be re-encrypted with the key defined in the rule.
- An error is shown when the user does not own the current key.
- Encrypted files that should be plaintext according to the encryption policy that applies remain encrypted.

A status image indicates overall state of the operation:

- **Green:** the operation has been finished successfully.
- **Red:** the operation has been finished with errors.
- **Yellow:** the operation is in progress.

Four tab pages provide detailed information on the processed files:

- The **Summary** tab page shows counters about the found/encrypted/re-encrypted/ ... files. The **Export...** button can be used to create XML reports containing the processed files and the results.
- The **Errors** tab page shows files that could not be handled as required.
- The **Modified** tab page shows files that have been modified successfully.
- The **All** tab page shows all processed files and their results.

Clicking the **Stop** button in the upper right corner cancels the operation. The **Stop** button changes to **Restart** to restart the operation.

When the operation is finished with errors, the **Stop** button changes to a **Retry** button. Clicking the **Retry** button starts the operation again but only for files that failed.

9.3 Persistent encryption

The content of files encrypted by File Encryption is being decrypted on-the-fly if you own the necessary key. When the content is saved as a new file in a location that is not covered by an encryption rule, the resulting file will not be encrypted.

With persistent encryption, copies of encrypted files will be encrypted, even when they are saved in a location not covered by an encryption rule.

Note: Security officers can disable this behavior. If disabled, files are created in plaintext when they are copied/moved to a location not covered by an encryption rule.

10 SafeGuard Cloud Storage

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

It does not change the way you work with data stored in the cloud. But Cloud Storage makes sure that the local copies of your cloud data is encrypted transparently and remains encrypted when it is stored in the cloud.

Note: Do not add files to your Dropbox folder by dropping them onto the Dropbox icon on the Windows desktop. These files will be copied to your Dropbox folder in plaintext. To encrypt files transparently copy them directly to your Dropbox folder.

Important: When extracting a ZIP archive using the built-in archiver of Microsoft Windows the process stops as soon as an encrypted file is encountered for which the key is not available. The user receives a message that access was denied, but is not informed that there are files that have not been processed and hence are missing. Other archivers, for example 7-Zip, work fine with ZIP archives containing encrypted files.

10.1 Cloud Storage auto-detection

SafeGuard Cloud Storage automatically detects your cloud storage provider. It will automatically set the encryption policy to the folder to be synchronized.

10.2 Cloud Storage initial encryption

SafeGuard Cloud Storage does not perform an initial encryption of your data. Files which have been stored before SafeGuard Cloud Storage was installed or was activated by a policy remain plaintext.

If you want to encrypt these files, you have to remove them from the cloud first and then add them again.

10.3 Set default keys

SafeGuard Cloud Storage allows you to set default keys for encrypting data in your cloud storage. Using default keys allows you to encrypt different subfolders of your cloud storage using different keys by setting a separate default key for each folder. You set default keys using the **File encryption > Set default key ...** command from the SafeGuard Explorer Extensions, see [Define a default key](#) (page 61).

Note: To do so, your security officer has to explicitly allow the use of default keys for Cloud Storage. If allowed, you can select a default key from a predefined set of keys and use it for encrypting folders of your cloud storage.

Note: If you intend to read encrypted files on Android and iOS devices with Sophos Mobile Encryption, you must use local keys for encryption. For further information on Sophos Mobile Encryption, see the *Sophos Mobile Encryption Help*.

Imagine you want to use Dropbox to provide secured data for different partners. Each partner should have access to one subfolder of your dropbox. To do so, you only have to set a separate default key for each of the subfolders. SafeGuard Enterprise will then automatically add a copy of SafeGuard Portable, which gives partners without SafeGuard Cloud Storage access to encrypted data, to each subfolder. You provide your partners with the respective passphrases for the keys. Using SafeGuard Portable and the passphrase they can decrypt data in the folder you created for them, but they do not have access to data stored in other subfolders, because it is encrypted with a different key.

10.4 SafeGuard Portable for Cloud Storage

You may want to access your cloud storage from home or exchange encrypted data in the cloud by using a shared folder in your cloud storage. SafeGuard Portable allows access to encrypted data stored in the cloud without having SafeGuard Cloud Storage installed.

Data encrypted with SafeGuard Cloud Storage can be encrypted and decrypted using SafeGuard Portable. This is achieved by automatically copying a program (SGPortable.exe) to your synchronization folder.

The passphrase of a local key only allows access to files that have been encrypted using this specific key. You or any recipient can decrypt encrypted data and encrypt it again.

Note: The passphrase of a local key has to be communicated to the recipient beforehand.

The recipient can use existing keys or create a new key with SafeGuard Portable (for example, for new files).

SafeGuard Portable does not have to be installed on or copied to your communication partner's computer. It remains in the cloud storage.

For a detailed description of how to use SafeGuard Portable, see [Editing files using SafeGuard Portable](#) (page 47).

Note: Double-clicking a file or selecting the open command will not cause in-place decryption of the file since decrypted files in cloud storage synchronization folders would automatically be synchronized to the cloud. When doing so a dialog appears asking you to choose a safe location for the file. Decrypted files are not wiped automatically when SafeGuard Portable is closed. Changes in files decrypted using SafeGuard Portable for Cloud Storage will not be done in the encrypted original.

Note: Do not store cloud storage synchronization folders on removable media or the network. If you do, SafeGuard Portable creates decrypted files in those folders. SafeGuard Portable should not be used in such cases. Consider moving the synchronization folders to fixed disks instead.

11 SafeGuard Enterprise and self-encrypting, Opal-compliant hard drives

Self-encrypting hard drives offer hardware-based encryption of data when they are written to the hard disk. The Trusted Computing Group (TCG) has published the vendor-independent Opal standard for self-encrypting hard drives. Different hardware vendors offer Opal-compliant hard drives. SafeGuard Enterprise supports the Opal standard and offers management of endpoints with self-encrypting, Opal-compliant hard drives. For details, see <http://www.sophos.com/en-us/support/knowledgebase/113366.aspx>.

11.1 Encryption of Opal-compliant hard drives

Opal-compliant hard drives are self-encrypting. Data are encrypted automatically when they are written to the hard disk.

Opal-compliant hard drives are locked by an AES 128/256 key used as an Opal password. This password is managed by SafeGuard Enterprise through an encryption policy. Your security officer defines this encryption policy in the SafeGuard Management Center and deploys it to your computer.

11.2 System Tray Icon and Explorer extensions on endpoints with Opal-compliant hard drives

When SafeGuard Enterprise is installed on your computer, the SafeGuard Enterprise product icon is displayed in the system tray of the computer taskbar. You can centrally access all important functions provided by SafeGuard Enterprise on your computer. Note that the features available depend on the settings defined in the SafeGuard Management Center. The security officer specifies these settings centrally in the SafeGuard Management Center, and distributes them to the endpoint computers.

If the security officer has allowed you by policy to decrypt Opal-compliant hard drives, the SafeGuard Enterprise **Decrypt** command is available in the Windows Explorer context menu.

12 System Tray Icon and tool tips

You can easily access all of the important SafeGuard Enterprise Client functions on your computer. The SafeGuard Enterprise System Tray Icon is placed on the Windows taskbar to allow access to these functions.

Note: The System Tray Icon's behavior on your computer is defined by the security officer. The security officer specifies in a policy whether the icon is displayed on your computer. It can also be set to "silent". In this case, balloon tool tips are not displayed on your computer.

With the System Tray Icon, you can view information or perform specific actions. By clicking the icon with your right mouse button, you can show a menu with the following entries:

- **Display:**
 - **Key ring:** Shows all keys available for you.
Note: If your endpoint computer has been migrated from an unmanaged to an managed environment, a second logon to SafeGuard Enterprise may be necessary to display your user-defined local keys in your key ring.
 - **User Certificate:** Shows information concerning your certificate.
 - **Company Certificate:** Shows information concerning the company certificate used.
- **Create new key:** Opens a dialog for creating a new key that is used for data exchange with removable media or SafeGuard Cloud Storage, see [SafeGuard Data Exchange](#) (page 39) and [SafeGuard Cloud Storage](#) (page 53).
- **Local Self Help:**

If Local Self Help is activated for your computer in the relevant policy, the Local Self Help command is shown on the right-click menu of the System Tray Icon. Using this command, you can launch the Local Self Help Wizard. Local Self Help is a logon recovery method that does not require any helpdesk assistance. For further information, see [Recovery with Local Self Help](#) (page 64).
- **Change Media Passphrase:** Opens a dialog for changing the media passphrase, see [SafeGuard Data Exchange](#) (page 39).
- **Synchronize:** Starts data synchronization with the SafeGuard Enterprise Server. Tool tips show the data synchronization's progress and result.
Note: You can also start synchronization by double-clicking the System Tray Icon.
- **Status:** Opens a dialog showing information on the current status of the SafeGuard Enterprise protected computer:

Field	Information
Last policy received	Shows the date and time when the computer last received a new policy.
Last key received	Shows the date and time when the computer last received a new key.
Last certificate received	Shows the date and time when the computer last received a new certificate
Last server contact	Shows the date and time of the last server contact.
SGN user state	<p>Shows the status of the user who is logged on to the computer (Windows logon):</p> <ul style="list-style-type: none"> ▪ Pending: The replication of the user in the SafeGuard POA is pending, this means the initial user synchronization has not yet been completed. This information is especially important after your first logon to SafeGuard Enterprise as you can only log on at the SafeGuard Power-on Authentication after initial user synchronization has been completed. ▪ SGN user: The user logged on to Windows is a SafeGuard Enterprise user. An SGN user is allowed to log on at the SafeGuard Power-on Authentication, is added to the UMA (User Machine Assignment) and is provided with a user certificate and a key ring to access encrypted data. ▪ SGN user (owner): Provided that the default settings have not been changed, an owner has the right to enable other users to log on to the endpoint and become SGN users. ▪ SGN guest: SGN guest users are not added to the UMA, are not provided with rights to log on to the SafeGuard POA, are not assigned a certificate or a key ring and are not saved to the database. ▪ SGN guest (service account). The user logged on to Windows is a SafeGuard Enterprise guest user who has logged on using a service account for administrative tasks. ▪ SGN Windows user

Field	Information
	<p>A SafeGuard Enterprise Windows user is not added to the SafeGuard POA, but has a key ring for accessing encrypted files, just as a SafeGuard Enterprise user does. The users are added to the UMA. This means that they are allowed to log on to Windows on that endpoint.</p> <ul style="list-style-type: none"> ▪ Unknown: Indicates that the user status could not be determined.
<p>Policy Cache State Data packets prepared for transmission</p>	<p>Indicates whether there are any packages to be sent to the SafeGuard Enterprise Server.</p>
<p>Local Self Help (LSH) State Enabled Active</p>	<p>Indicates whether Local Self Help has been enabled in a policy and whether it has been activated by the user on the computer.</p>
<p>Ready for certificate change</p>	<p>This text is displayed if the security officer has assigned a new certificate for token logon to your computer. You can now change the certificate for token logon, see Change the certificate for token logon (page 18).</p>

- **Help:** Opens the SafeGuard Enterprise Online Help.
- **About SafeGuard Enterprise:** Shows information about your SafeGuard Enterprise version.

12.1 Create local keys

1. Right-click the SafeGuard Enterprise System Tray Icon on the Windows taskbar or right-click a volume/folder/file.
2. Click **Create new key**.
3. In the **Create Key** dialog, enter a **Name** and a **Passphrase** for the key.

The internal name of the key is displayed in the field below.

4. Confirm the passphrase.

If you enter a passphrase that is not secure, a warning message is displayed. To increase the level of security, we recommend that you use complex passphrases. You can also decide to use the passphrase despite the warning message. The passphrase also has to correspond with the company policies. If it does not, a warning message is displayed.

5. If you opened the dialog using a right-click menu it contains the **Use as new default key for path** option. With the **Use as new default key for path** option, you can set the new key immediately as the default key for a volume or Cloud Storage synchronization folder.

The default key you specify here is used for encryption during normal operation. It will be used until a different one is set.

6. Click **OK**.

The key is created and becomes available as soon as the data has been successfully synchronized with the SafeGuard Enterprise Server.

If you define this key as the default key, all data copied to a removable storage medium or a Cloud Storage synchronization folder from now on is encrypted using this key.

For a recipient to be able to decrypt all data contained on a removable storage medium, you may have to re-encrypt the data on the device using the key created locally. To do so, select **File encryption > Start encryption** from the device's context menu in Windows Explorer. Select the required local key and encrypt the data. This is not necessary if you use a media passphrase.

12.2 Overlay icons

Overlay icons are small icons displayed on elements in Windows Explorer. The Data Exchange overlay icons are only displayed on files and volumes. Their purpose is to give you a quick information on the encryption status of a file or whether a volume has an encryption rule applied.

- The red key indicates that you do not have a key to decrypt a file. This icon is only displayed on files.
- The green key is displayed if a file is encrypted and its key is in your key ring. This icon is only displayed on files.
- The grey key is displayed if a file is not encrypted, but an encryption rule for that file is available. This icon is only displayed on files.
- The yellow key is displayed if a drive has an encryption policy defined for it. This icon is only displayed on drives.

Overlay icons will only be displayed on non-boot volumes, removable media and CDs/DVDs. On boot drives overlay icons will be displayed in the burning staging folder (that's the folder where Windows stores the files before they are burned on a CD/DVD). If you specify an unencrypted folder, then no grey key will be displayed on unencrypted files in that folder and its subfolders. Generally speaking, if a file has no encryption rule applied, no grey key is displayed.

13 Accessing functions via Explorer extensions

You can access encryption-related functions from the corresponding entries in Windows Explorer context menus.

Note: The functions displayed depend on the settings defined in the policies. They also depend on whether the relevant function is available for the Explorer node selected. The function scope varies depending on whether file-based or volume-based encryption was used for the relevant volume/folder/file.

13.1 Explorer extensions for file-based encryption

You can access the functions for file-based encryption (Data Exchange, File Encryption, Cloud Storage) from the corresponding entries in Windows Explorer context menus. The functions are available in the context menus of

- the 'My Computer' node
- removable media
- folders
- files

The functions displayed in the menus depend on which components are installed.

The entry **File encryption** is added to the context menu. You can access the individual functions from this menu.

If a file-based encryption policy applies to the selected volume, removable media, folder, or file, encryption-related entries are added to the context menu.

The following functions are available:

- **Encrypt according to policy:** Is only displayed when File Encryption is installed and the 'My Computer' node is selected. If you select this option all files in folders and subfolders covered by encryption rules are encrypted according to the policy valid for your computer.
- **Start encryption:** If you select this option in a context menu, all files can be encrypted or re-encrypted. It starts a file encryption wizard when a File Encryption policy is applicable.
- **Show encryption state:** Indicates whether a volume, removable media, or a file has been encrypted, which key has been used, whether the key is included in your key ring, and whether you have access to this file.
- **Decrypt:** Decrypts the selected files.

Note: It is not possible to decrypt files which are covered by a File Encryption rule.

- **Default key:** Shows the key currently used for new files added to the volume (by saving, copying or moving). You can define the standard key for each individual volume or removable media separately.
- **Set default key:** Opens a dialog for selecting a different default key.
- **Create new key:** Opens a dialog for creating user-defined local keys.
- **Re-activate encryption:** Your security officer can allow you to decide whether files on removable media connected to your computer are to be encrypted. When you connect removable media to your computer, a message box is displayed asking you whether you want to encrypt the files on the attached media. In addition, your security officer can allow you to select whether your choice is to be remembered for the relevant media. If you select **Remember setting and do not show this dialog again**, the message box will not be displayed again for the relevant media. In this case, the new command **Re-activate encryption** becomes available in the context menu of the relevant device in Windows Explorer. Select this command to revert your decision about encryption for the relevant device. If this is not possible, for example because you do not have the relevant rights for the device, an error message is displayed. After you have reverted your decision, you are prompted to decide about encryption for the relevant device again.

13.1.1 Define a default key

By defining a default key you specify the key to be used for encryption during normal operation of SafeGuard Data Exchange and SafeGuard Cloud Storage.

You can define the default key from the context menu

- of a file on removable media
- of removable media
- of a Cloud Storage synchronization folder or sub-folder
- of a file in a Cloud Storage synchronization folder or sub-folder
- additionally, you can set a key as default immediately when you create a new local key in the **Create key** dialog.

To define a default key:

Select **File encryption > Set default key** to open a dialog for key selection.

The key you select in this dialog is used for all subsequent encryption processes on the removable storage medium or in your Cloud Storage synchronization folder. If you want to use a different one, you can define a new default key at any time.

Note: If a local key is selected for encryption of Cloud Storage, SafeGuard Portable will be copied to the Cloud Storage synchronization folder.

By policy, a default key to be used for encryption can be specified. If it is not defined by policy and you are allowed to set default keys, you are prompted to specify an initial default key.

13.1.2 Import keys from a file

If you have received removable media containing encrypted data or want to access Cloud Storage data in a shared folder which has been encrypted using user-defined local keys, you can import the key required for decryption to your private key ring.

To import the key, you need the relevant passphrase. The person who encrypted the data has to provide you with the passphrase.

1. Select the relevant file on the removable media and click **File encryption > Import key from file**.
2. Enter the passphrase in the dialog that is displayed.

The key is imported, and you can access the file.

13.2 Explorer extensions for volume-based encryption

The entry **Encryption** is added to the Windows Explorer context menu.

If the volume is encrypted, a key symbol is displayed next to the menu entry. If a green key symbol is shown, you have the required keys and you can access the volume.

Note: **File encryption > Show encryption state** shows the encryption status of the files on the volume from a file-based encryption point of view. Files on an encrypted volume can also be encrypted in a file-based manner. If this is the case, a dialog will be displayed accordingly.

Add/Remove Keys

You can add/remove keys to/from the encrypted volume if the settings specified in the applicable policies allow it. By doing so, you enable all owners of the relevant key to access the encrypted data on this volume.

You can assign keys to the volume in the volume's **Properties** dialog. This dialog includes the **Encryption** tab (right-click on **Volume > Properties > Encryption**).

Select a key from the lower list, and click **Add Key**. The file is moved upwards from the key selection list. It is included in the list of keys that can be used to access the encrypted volume.

With **Remove Key**, you can remove the key from the list of keys used for accessing the media.

14 Recovery options

For recovery (for example, if you have forgotten your password), SafeGuard Enterprise offers various options that are tailored to different recovery scenarios:

- **Logon recovery with Local Self Help** (available for SafeGuard POA only)

If you have forgotten your password, Local Self Help enables you to log on to your computer without the assistance of a helpdesk. Even in situations where neither telephone nor network connections are available (for example, aboard an aircraft), you can regain access to your computer. To log on, you simply answer a number of predefined questions in the SafeGuard Power-on Authentication.

For further information, see [Recovery with Local Self Help](#) (page 64).

- **Recovery with Challenge/Response or BitLocker recovery key**

The Challenge/Response mechanism is a secure and efficient recovery system that helps you if you cannot log on to your computer or access encrypted data. During the Challenge/Response procedure, you provide a challenge code generated on your computer to the helpdesk officer, who in turn generates a response code that authorizes you to perform a specific action on the computer.

On endpoints which do not support Challenge/Response, recovery keys are provided. This is Microsoft's standard procedure. During the recovery process, you provide the computer name to the helpdesk officer, who in turn provides you with the recovery key you need to start your computer.

For further information, see [Recovery with Challenge/Response or recovery key](#) (page 73).

All the recovery options are enabled for use on your computer by the security officer in policies.

15 Recovery with Local Self Help

Note: Local Self Help is only available for Windows 7 endpoints with SafeGuard Power-on Authentication (POA).

If you have forgotten your password, Local Self Help enables you to log on to your computer without the assistance of a helpdesk.

Using Local Self Help, you can regain access in situations where neither telephone nor network connections are available, and you therefore cannot use a Challenge/Response procedure (for example, aboard an aircraft). You can log on to your computer by answering a specified number of predefined questions in the SafeGuard Power-on Authentication.

The security officer can define the questions to be answered and distribute them to the endpoints. You can also define your own questions, if the relevant policy entitles you to do so. The Local Self Help Wizard helps you provide the initial answers and edit the questions. You can open the Local Self Help Wizard by clicking the SafeGuard Enterprise System Tray Icon on the Windows taskbar.

Prerequisites

To use Local Self Help for logon recovery, the following prerequisites must be met:

- The security officer has enabled Local Self Help in the relevant policy and has defined the settings for this function (for example, the right to define your own questions).
- You have activated Local Self Help on your computer.

15.1 Activate Local Self Help

After the policy entitling you to use Local Self Help has become effective, you have to activate the function by answering the predefined questions received or by defining and answering your own questions.

Local Self Help only becomes active on your computer after you have answered and saved a predefined number of questions. The security officer specifies how many questions you have to answer. The Local Self Help Wizard guides you through the process and shows how many answers are required. Depending on the policy settings, these are the possible scenarios:

- **You have received predefined questions, and you are *not* entitled to define your own questions.**

Answer and save the predefined questions received. The Local Self Help Wizard shows how many answers are required.

- **You have received predefined questions, and you are entitled to define your own questions.**

Answer and save the required number of questions (predefined questions, your own defined questions, or a combination of both).

- **You have not received predefined questions, and you are entitled to define your own questions.**

Define, answer, and save the required number of questions.

Note: To log on at the SafeGuard Power-on Authentication with Local Self Help, you have to answer questions randomly selected from the questions answered in the Local Self Help Wizard. The security officer specifies how many questions you have to answer in the SafeGuard POA.

Prerequisite: After receiving the policy, the tool tip indicates that there are unanswered Local Self Help questions. Restart your computer to add the **Local Self Help** command to the context menu of the System Tray Icon on the Windows taskbar.

To activate Local Self Help:

1. Right-click the SafeGuard Enterprise System Tray Icon on the Windows taskbar.
2. Select **Local Self Help**.

The **Local Self Help Wizard Welcome** dialog is displayed.

For security reasons, you are prompted to enter your password.

3. Enter your password, and click **Next**.

The **Status Overview** dialog is displayed.

This dialog tells you how to activate Local Self Help. It also displays status information (for example the number of answered user-defined questions or the number of answered predefined questions).

4. Click **Next**.

If you have received predefined questions with the effective policy, the **Predefined questions** dialog is displayed.

- If you have received several different question themes, you can choose from the question themes displayed in the drop-down list of the **Theme** field.
- To answer the questions, click on the relevant question, and enter your answer in the **Answers** column.
- After you enter the answer, the text entered is hidden. To view the text, select **Show answers**.

Note: When answering the questions during a recovery process in the SafeGuard Power-on Authentication, you will need to enter the answers exactly as you entered them in the Local Self Help Wizard. For example, answers are case-sensitive in Local Self Help.

Note: Not all characters that can be entered in Windows can be handled by the SafeGuard POA, for example Hebrew or Arabic characters cannot be used. When entering answers in Japanese, you have to use Romaji (Roman) characters. Otherwise the answers will not match when you answer the questions in the SafeGuard POA.

5. After you have finished answering the predefined questions, click **Next**.
6. If you are entitled to define your own questions, the **User defined questions and answers** dialog is displayed.
 - a) To add a new question, click **New Question**.

A new line is added to the list of questions.

- b) Enter your question in the **Questions** column and the answer in the **Answers** column.

After you enter the answer, the entered text is hidden.

- c) To display the text, select **Show answers**.

Note: When answering the questions during a recovery process in the SafeGuard Power-on Authentication, you will have to enter the answers exactly as you entered them in the Local Self Help Wizard. For example, answers are case-sensitive in Local Self Help.

Note:

Not all characters that can be entered in Windows can be handled by the SafeGuard POA, for example Hebrew or Arabic characters cannot be used. When entering answers in Japanese, you have to use Romaji (Roman) characters. Otherwise the answers will not match when you answer the questions in the SafeGuard POA.

7. After you have finished defining and answering your own questions, click **Next**.

The last dialog of the Local Self Help Wizard shows the new status information after you answer the questions. A message indicates whether the prerequisites for activating Local Self Help have been met.

8. Click **Finish**.

The questions and answers are saved. A message is displayed indicating that Local Self Help was activated successfully.

9. Click **OK**.

Local Self Help is active on your computer. You can use Local Self Help for logon recovery in the SafeGuard Power-on Authentication.

15.2 Activate Local Self Help - reminder

It is essential that you activate Local Self Help. For this reason SafeGuard Enterprise will remind you to enroll in Local Self Help.

SafeGuard Enterprise will remind you to set up your Local Self Help questions in three stages:

- **Stage 1**

A balloon tool tip pops up every hour for one calendar day and indicates that Local Self Help needs to be set up. On the following calendar day stage 2 starts.

- **Stage 2**

In addition to stage 1 behavior the Local Self Help Wizard will be started every time you log on to or unlock the computer. You can postpone running the wizard. After 3 calendar days stage 3 starts.

- **Stage 3**

In addition to stage 2 behavior but without a tool tip notification, the Local Self Help Wizard will start every 60 minutes.

The user is immediately notified by a balloon tool tip and stage 1 is entered whenever Local Self Help has to be reactivated due to changes in one of the following:

- Local Self Help parameters
- Windows password
- certificate

15.3 Edit questions

After activating Local Self Help on your computer, you can edit the questions at any time:

- For predefined questions, you can change the answers that were provided when answering the questions initially. However, predefined questions cannot be deleted.
- For user-defined questions, you can change the answers that were provided when answering the questions initially, add new questions, or delete questions.

1. Right-click the SafeGuard Enterprise System Tray Icon on the Windows taskbar.

2. Select **Local Self Help**.

The **Local Self Help Wizard Welcome** dialog is displayed.

For security reasons, you are prompted to enter your password.

3. Enter your password, and click **Next**.

The **Status Overview** dialog is displayed.

This dialog tells you how to activate Local Self Help. It also displays status information (for example, the number of answered user-defined questions, the number of answered predefined questions, etc).

4. Click **Next**. If you have received and answered predefined questions, the **Predefined Questions** dialog is displayed, containing the answered questions.

a) If you have received several different question themes, you can choose between the question themes to be displayed in the drop-down list of the **Theme** field.

b) By default the answers entered are not shown as text. To show the text entered, select the **Show answers** check box.

c) To change the answers, click the relevant questions and enter your new answer in the **Answers** column.

5. Click **Next**. If you are entitled to define your own questions, the **User defined questions and answers** dialog is displayed. By default the answers entered are not shown as text.

a) To show the text entered, select the **Show answers** check box.

b) To change existing answers, click the relevant question and enter your new answer in the **Answers** column.

c) To add a new question, click **New Question**.

A new line is added to the list of questions. Enter your question in the **Questions** column, and the answer in the **Answers** column.

- d) To delete questions, click the relevant question and click **Delete Question**.

A message is displayed, prompting you to confirm that you want to delete the question. Click **Yes**.

6. Click **Next**.

The last dialog of the Local Self Help Wizard shows the new status information after you edit the questions. A message indicates whether the prerequisites required for Local Self Help to remain active have been met.

7. Click **Finish**.

The questions and answers are saved. A message is displayed indicating that the editing procedure was successful, and Local Self Help remains active.

8. Click **OK**.

The modifications take effect.

Next time you launch Local Self Help in the SafeGuard Power-on Authentication, the modified/new questions are selected randomly and displayed. The modified/new answers apply.

Note: If the number of answered questions falls below the minimum number required due to the changes made, a warning message is displayed in the last dialog of the Local Self Help Wizard, indicating that Local Self Help will be deactivated after you close the wizard. If you do not want to deactivate Local Self Help, you can return to **User defined questions** and **Predefined questions** by clicking the **Back** button. You can then add or answer new questions. If you click **Finish** and the number of answered questions has fallen below the minimum number required, another warning message is displayed, indicating that Local Self Help is no longer active on your computer. However, in this case, you can reactivate Local Self Help.

15.4 Changes of question parameters

The security officer can define the following parameters that apply to Local Self Help questions:

- The number of questions you have to answer in the Local Self Help Wizard to activate Local Self Help on your computer. The number of questions specified must be available with answers for Local Self Help to remain active.
- The number of questions you have to answer in the SafeGuard POA to log on with Local Self Help. The questions displayed in the SafeGuard POA are selected randomly from the questions you have answered in the Local Self Help Wizard.

If these two parameters change due to a new policy deployed to your computer, the following scenarios may occur:

Condition	LSH action	User action required
The number of questions you have to answer in the LSH Wizard changes, but there are enough questions available for Local Self Help to remain active on your computer.	Local Self Help remains active on your computer.	None.
The number of questions you have to answer in the LSH Wizard changes and there are not enough questions available for Local Self Help to remain active on your computer.	A message is displayed stating that your Local Self Help settings have changed. The questions available on your computer are no longer valid. Local Self Help is no longer active on your computer.	To reactivate Local Self Help, open the Local Self Help Wizard and follow the Wizard instructions.
The number of questions you have to answer in the SafeGuard POA to log on with Local Self Help changes.	A message is displayed stating that your Local Self Help settings have changed. The questions available on your computer remain valid. The ratio between available questions and valid answers has changed.	Open the Local Self Help Wizard and follow the Wizard instructions.

15.5 Changes of conditions or parameters for Local Self Help during editing processes

Local Self Help parameters and other conditions that are crucial for the usage of Local Self Help may change while you are defining or editing questions in the Local Self Help Wizard.

For example:

- A new user password or certificate may be set.
- A new policy with new Local Self Help settings and/or a new set of Local Self Help questions may be transferred to your computer through the regular update mechanism.

If such changes occur during the editing process, the set of questions and answers you have defined may no longer be valid and there may not be enough questions for Local Self Help to become or stay active on your computer.

Therefore, each time you finish defining or editing questions in the Local Self Help Wizard, the wizard checks whether any of the following conditions apply and initiates the relevant action:

Condition	LSH Wizard action	Result
Local Self Help has been disabled globally by a new policy.	The Local Self Help Wizard shows a message stating that Local Self Help has been disabled globally and closes.	Local Self Help can no longer be used.

Condition	LSH Wizard action	Result
<p>Local Self Help parameters have been changed (for example minimum length of answers, right to define your own questions, the number of questions to be answered) by a new policy. Local Self Help has not been disabled.</p> <p>The questions and answers you have defined are still valid and sufficient for Local Self Help to be active on your computer.</p>	<p>The Local Self Help Wizard shows a message stating that the Local Self Help parameters have changed, saves your changes and closes.</p>	<p>Local Self Help is active on your computer and can be used for logon recovery. But the ratio of available questions and valid answers may have changed. To regain the initial ratio, you may need to add or delete questions and/or answers.</p>
<ul style="list-style-type: none"> ▪ The user password has been changed <p>and/or</p> <ul style="list-style-type: none"> ▪ Local Self Help parameters have been changed (for example minimum length of answers, right to define your own questions, the number of questions to be answered etc.) by a new policy. Local Self Help has not been disabled. <p>The questions and answers you have defined are no longer valid and there are not enough questions for Local Self Help to be active on your computer.</p>	<p>The Local Self Help Wizard shows a message stating that the user password or Local Self Help parameters have changed. Local Self Help will not be active on your computer. You are advised to rerun the wizard. The wizard closes.</p>	<p>To activate Local Self Help, rerun the Local Self Help Wizard and define questions and answers again. Afterwards, you can use Local Self Help for logon recovery.</p>
<p>The user certificate has changed.</p>	<p>The Local Self Help Wizard shows a message stating the user certificate has changed. Local Self Help will not be active on your computer. You are advised to rerun the wizard. The wizard closes.</p>	<p>To activate Local Self Help, rerun the Local Self Help Wizard and define questions and answers again. Afterwards, you can use Local Self Help for logon recovery.</p>

15.6 Log on at the SafeGuard POA with Local Self Help

1. In the SafeGuard POA logon dialog, click the **Recovery** button.
 - If only Local Self Help is activated for logon recovery, Local Self Help is started.
 - 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**.

Note:

If you usually log on to the SafeGuard Power-on Authentication with a token or smartcard, you first have to remove the token/smartcard from your computer. After that the SafeGuard POA logon dialog for logging on with user name and password is displayed. Enter your user ID and click the **Recovery** button.

The **Local Self Help Welcome** dialog is displayed.

This dialog provides a short description of the next steps.

2. Click **Next** to start answering the questions.

The first question is displayed.
3. Enter your answer.

By default, the text entered is not displayed in the input field for security reasons. To display the answer, clear the **Hide answer** check box.
4. After answering the question, click **Next**.

You can only click **Next** and continue with the next question after you have entered an answer.
5. Answer the remaining questions. After answering the last one, click **OK**.

In the next dialog, you can display your current password.
6. To display the password, press **Enter** or **Spacebar** or click the blue box.

Note:

Do NOT click **OK**. After clicking **OK** the startup process will continue WITHOUT showing the password.

The password will be shown for a maximum of five seconds. Afterwards, the startup process continues automatically.

Note: Make sure that no unauthorized person can view the contents of your screen, by chance or on purpose. You can immediately hide your password by pressing the **Spacebar**, **Enter**, or by clicking the blue display box.

7. You can read the password and use it for logging on at the SafeGuard Power-on Authentication and to Windows again.
8. After reading the password, click **OK**. Otherwise, the startup process will continue automatically, five seconds after showing the password.

You are now logged on to the SafeGuard Power-on Authentication and to Windows.

15.7 Failed logon attempts

If you enter a wrong answer for one or several questions, logon fails. In this case, a message indicating the failed logon is displayed. For security reasons, Local Self Help does not indicate which of the answers were wrong.

A failed Local Self Help recovery procedure is considered a failed logon attempt and logged as an event. In this case, a logon delay goes into effect. The logon delay period increases with every failed logon attempt.

If you restart your computer after a failed logon attempt, and select logon recovery with Local Self Help again, questions are randomly selected again.

15.8 Reactivate questions and answers after password changes on several machines

If you use different computers with Local Self Help activated, and you change your Windows password on one machine, the Local Self Help questions and answers are no longer active on the second (or any further) machine after the password change has become effective. But the questions and answers are still available in the Local Self Help Wizard. To use the same set of questions on the second computer again, confirm it in the Local Self Help Wizard.

1. After you have changed your password on one machine, log on to the second machine.

A tool tip indicates that there are unanswered Local Self Help questions.

2. Right-click the SafeGuard Enterprise System Tray Icon on the Windows taskbar and select **Local Self Help**.

The Local Self Help Wizard **Welcome** dialog is displayed.

3. Enter your password, and click **Next**.
4. Confirm all following Local Self Help Wizard dialog pages with **Next** and click **Finish** on the last one.

The questions and answers stored previously on the computer are active again and are used when you log on to the SafeGuard POA with Local Self Help.

16 Recovery with Challenge/Response or recovery key

If you use SafeGuard Enterprise and you have, for example, forgotten your password, you can regain access to your computer very quickly through a central helpdesk.

Note: If you use Windows 7 and the SafeGuard POA, we recommend that you use Local Self Help to recover a forgotten password. You can display the current password in Local Self Help and continue using it, so there is no need to reset the password or involve the helpdesk.

16.1 Challenge/Response for SafeGuard POA users

For recovery, SafeGuard Enterprise offers a **Challenge/Response procedure** that allows information to be exchanged confidentially.

During the Challenge/Response procedure, you generate a challenge code (an ASCII character string), and provide this code to a helpdesk officer. Based on the challenge code provided, the helpdesk officer generates a response code that authorizes you to perform a specific action on your computer.

Recovery with Challenge/Response is available for the following logon methods in the SafeGuard Power-on Authentication:

- Logon with user ID and password
- Logon with fingerprint
- Logon with non-cryptographic token

16.1.1 Typical scenarios for which you may require help desk assistance

- You have forgotten your password.
- You have entered your password incorrectly too often at the SafeGuard POA. The computer has been locked.
- You have forgotten or lost your token/smartcard.
- The SafeGuard Power-on Authentication's local cache is partly damaged.
- A different user has to start the SafeGuard Enterprise protected computer.

16.1.2 Procedures for which a response can be requested and the relevant scenarios

- **Booting the SafeGuard Enterprise Client without user logon:**

Booting the computer without user logon helps if you have entered your password incorrectly (for example due to typing errors, activated CAPS LOCK key, etc), but you know the correct password. The Challenge/Response procedure logs you on to your computer without resetting the password.

If you have entered the password incorrectly too often, the helpdesk automatically generates a response code for booting the client without user logon. The requirement for this specific case is included in the challenge. Afterwards, you can log on with your user name and password again.

- **Booting the SafeGuard Enterprise Client with user logon:**

If you have forgotten your password, do not try to enter a password, but request a challenge right away. The help desk can then generate a response for logon with or without a user name. When you log on with your user name, ask your help desk to have your old password displayed during the Challenge/Response procedure. This avoids the need to reset the password. Otherwise, when you log on with your user name, you have to reset your password for the Windows logon during the Challenge/Response procedure.

Note: For users working offline, that is, not connected to the domain controller, special aspects need to be considered, see [Challenge/Response for offline users](#) (page 77).

- **Restoring the SafeGuard Enterprise policy cache:**

This procedure is necessary if the SafeGuard policy cache is damaged. The local cache stores all keys, policies, user certificates and audit files. By default, logon recovery is deactivated when the local cache is corrupted, that is it will be restored automatically from its backup. In this case, no Challenge/Response procedure is required for repairing the local cache. But logon recovery can be activated by policy if the local cache is to be repaired explicitly with a Challenge/Response procedure. In this case, you are prompted automatically to initiate a Challenge/Response procedure if the local cache is corrupted.

16.1.3 The Challenge/Response procedure

1. SafeGuard Power-on Authentication starts.

Note: When you generate the challenge, a time period of 30 minutes is available for entering the response generated by the helpdesk in a Challenge/Response procedure. After 30 minutes, the response code is no longer valid and can no longer be used.

2. Request a challenge:

Open the **Challenge** dialog in the SafeGuard Power-on Authentication. A challenge code in the form of an ASCII character string is generated and displayed.

3. Contact the helpdesk.

Tell the helpdesk your user data (user ID, computer ID, etc) as shown in the **Challenge** dialog, along with the challenge code.

4. The helpdesk generates a response code in the SafeGuard Management Center.
5. The helpdesk provides the response by phone or SMS.
6. Enter the response code at the SafeGuard Power-on Authentication.

You can now perform the authorized action. For example, resetting the password.

You can resume working.

16.1.4 Request a challenge

1. In the SafeGuard Power-on Authentication (POA) logon dialog, click **Recovery**.

The **Recovery** button is only activated when you enter a user name or at least one character in the PIN dialog.

Note: If you have entered your password/PIN incorrectly too often or if the policy cache is damaged, SafeGuard Enterprise informs you automatically, and offers to solve the problem with Challenge/Response.

Your user data and a randomly generated challenge code are displayed. For better readability, the challenge code is divided into five-character blocks.

2. Call the SafeGuard Enterprise helpdesk, and provide your user data as well as the challenge code to the help desk officer.

If you need help stating the challenge code, you can click the **Spelling Aid** button.

The helpdesk officer can identify the relevant scenario from the challenge code.

3. Click **Next**.

16.1.5 Enter the response

1. Enter the response code received from the helpdesk officer in the **Response** dialog, and click **OK**.

If you enter the response code incorrectly, the character block containing the error will be marked in red.

2. You are logged on at the SafeGuard Power-on Authentication.

If necessary, SafeGuard Enterprise will prompt you to change your Windows user credentials.

16.1.6 Best practice

16.1.6.1 You have entered the password incorrectly too often

You have entered your password incorrectly in the SafeGuard Power-on Authentication too often (typing errors, activated Caps Lock key etc.), but you know the correct password. You are connected to the domain.

1. Your computer is locked. You are prompted to initiate a Challenge/Response procedure to unlock your computer.
2. The helpdesk officer generates a response for booting without user logon.

Booting without user logon means that you do not have to change your password before you log on to Windows.

3. The Windows logon dialog is displayed. Enter your Windows password in this dialog.
Your are logged on to the system.

4. The counter of the maximum number of password entry attempts allowed is reset.

Note: You can also request a response with user logon. In this case you are prompted to change your Windows credentials before logging on to Windows.

16.1.6.2 You have forgotten your password

We recommend that you use the following methods to recover a forgotten password. By using these methods, you avoid having your password reset centrally:

- Use Local Self Help. With recovery by Local Self Help you can have the current password displayed and may continue using this password without having to reset it and without any helpdesk assistance.
- When using Challenge/Response: Ask your helpdesk to generate a response with user logon and to have your old password displayed during the Challenge/Response procedure. This will avoid having to reset it. You may continue working with the old password and change it locally afterwards, if desired.

If you do not use one of these methods, proceed as follows:

1. If you have forgotten your password, you receive a response for booting your computer with user logon. In this case, you have to change your password when you log on to Windows (provided that the domain is accessible).
2. After you have changed your password, use the new password to log on at the SafeGuard Power-on Authentication.

16.1.6.3 You have forgotten or lost your token

In this case, the Challenge/Response procedure with user logon is required.

1. You are prompted to change your password during the Challenge/Response procedure.

Note: The dialog for changing the password is only displayed if a connection to the domain controller is established.

2. If logon with a token and PIN is mandatory, you can decide whether you want to change the password or skip the password change by clicking **Cancel**.

- **You have forgotten your token**

Skipping the password change by clicking **Cancel** in the dialog only makes sense if you have forgotten your token but will have it for future logons. When you click **Cancel**, you are logged on to the system and you can resume working with your computer.

Without a token, you can only log on with Challenge/Response in the SafeGuard Power-on Authentication. Once you have your token again, you can use it to log on at the SafeGuard POA.

- **You have lost your token**

If you have lost your token, enter a new password in the dialog for changing your password. You are logged on to Windows with this password. If the policies on your computer allow it (token logon at the SafeGuard POA is not mandatory), you can also log on at the SafeGuard Power-on Authentication using this password.

Unauthorized use of the token by anyone finding it can be ruled out. Unauthorized users cannot use the token for logon even if they know the PIN - as your password has been changed.

16.1.6.4 You have forgotten your PIN

1. If you have forgotten your token PIN, request a response and enter a new password. You are logged on to Windows with this password. You can also use it to log on at the SafeGuard Power-on Authentication, provided that you are authorized for logging on by using a password.
2. A security officer has to assign a new PIN to the token, and store your new credentials on it. You can then use it for logging on.

16.1.6.5 You cannot access your computer any more

If you cannot access your computer any more, the SafeGuard Power-on Authentication might be corrupted. Even in this critical situation, SafeGuard Enterprise offers a Challenge/Response procedure with helpdesk assistance enabling you to regain access to your encrypted drives. Challenge/Response in this case is carried out through a WinPE environment. When encountering such a critical situation, we recommend that you contact your SafeGuard Enterprise helpdesk. The helpdesk officer will provide you with the necessary files and guide you through the necessary steps to regain access to your computer.

16.1.7 Challenge/Response for offline users

Special aspects need to be considered for Challenge/Response procedure for offline users. For offline users (that is, users who are not connected to the domain controller, for example sales representatives working with their notebooks), an automatic password change cannot be initiated during the Challenge/Response procedure.

16.1.7.1 Challenge/Response for offline users with logon mode user name/password

Example:

You are working offline (you are not connected to the domain controller), and you have forgotten your password. With the Challenge/Response procedure, you can quickly and easily regain access to your computer.

SafeGuard Enterprise can also log you on to Windows automatically during the Challenge/Response procedure. However, as you would not know the password after this procedure, you would have to repeat it each time you start your computer. Furthermore, you would not be able to unlock your computer in case it was locked (for example, a lock on screen saver activation). In this case, you would have to restart your computer risking data loss (and initiate a Challenge/Response procedure again).

Note: For this reason, SafeGuard Enterprise offers the possibility to show the password during a Challenge/Response procedure. As an offline user you should have your password displayed during a Challenge/Response procedure. Tell the helpdesk officer that you would like to have your password displayed. The helpdesk officer has to activate password display explicitly before generating your response code.

Proceed as follows:

1. To initiate the Challenge/Response procedure, click **Recovery** in the SafeGuard POA logon dialog.
2. Call your helpdesk and tell them your challenge code.
3. Tell the helpdesk officer that you would like to boot your computer with user logon and that your password is to be displayed.
4. In the **Challenge/Response** dialog, click **Next** and enter the response.
5. Click **OK**.

You are asked whether your old password is to be displayed on screen

6. Answer **Yes**, and click **OK**.
7. The next dialog informs you that your password will be displayed when you press **Enter** or the **Spacebar** on your keyboard, or when you click in the text.

Note: Do **not** click **OK**. If you click **OK**, the boot process will continue WITHOUT showing the password.

The password is shown for 5 seconds. The boot process then continues automatically.

8. Press **Enter** or the **Spacebar** on your keyboard, or click in the text.

The password is displayed.

Note: Make sure that no unauthorized person can view the contents of your screen, by chance or on purpose. You can immediately hide your password by pressing the **Spacebar**, **Enter**, or by clicking the blue display. The password will only be shown for 5 seconds at the maximum.

9. You can read the password, and use it for logging on at the SafeGuard Power-on Authentication and to Windows.

You can resume working with your computer.

16.1.7.2 Challenge/Response for offline users with logon mode "Only Token"

In this case, if you have forgotten your PIN or forgotten/lost your token, the procedure to be used depends on whether you know your Windows credentials.

- You know your Windows credentials
 - a) If you know your Windows credentials, initiate the Challenge/Response procedure as described. You are automatically logged on to Windows.

Logon mode **Only Token** is reset for the duration of the work session following the Challenge/Response procedure. Consequently, logging on to Windows with your user name and password is also possible.

In case your computer should be locked, you can therefore unlock it by entering your Windows password. But logging on at the SafeGuard Power-on Authentication is only possible with Challenge/Response.

- You do not know your Windows credentials
 - a) If you do not know your Windows credentials and you have forgotten your PIN, you can also start a Challenge/Response procedure during which your password will be displayed.
 - b) Tell your helpdesk officer that your password should be displayed.
As logon mode **Only Token** will be deactivated you can also unlock your computer - should it be locked - with this password. But logging on at the SafeGuard Power-on Authentication, however, is only possible with Challenge/Response.

16.2 Challenge/Response for BitLocker users

General hints on using mouse and/or keyboard

- You can select controls by using the mouse and/or the keyboard. To jump from one control to the next with the keyboard press the **Tab** key. To get back into the previous control use **Shift+Tab**.
- Confirm selections by pressing **Enter**.

Challenge/Response procedure

If you need to get a BitLocker recovery key, proceed as follows:

1. Reboot the PC. After rebooting, a yellow message appears. Press any key within the next three seconds.
2. The Sophos Challenge/Response screen appears.
3. In Step 2 information required to call the helpdesk is provided to you.
4. Provide the following information to the helpdesk:
 - Computer**, for example Sophos\ - Challenge** code, for example ABC12-3DEF4-56GHO-892UT-Z654K-LM321. Hover with the mouse over the characters to display a spelling aid. Or press **F1** several times to display this help box. The code expires after 30 minutes leading to an automatic shutdown of the PC.
5. Then enter the **response code** from the helpdesk (six blocks with two text fields each and five characters required per field).
 - If a text field is completely filled with characters, the focus is automatically switched to the next text field.
 - If you accidentally enter a wrong character in a block, the corresponding block will be highlighted in red. Use the **Delete** or the **Backspace** key to correct entries.
6. After you have successfully entered the response code, click **Continue** or press **Enter** to complete the Challenge/Response action.

Reset BitLocker credentials

As soon as you are logged on to the system again, specify new BitLocker credentials so that you will not need another Challenge/Response procedure for your next logon. Depending on your operating system and BIOS/UEFI version the system will display a dialog for the credential reset.

If this dialog does not appear automatically, right-click the SafeGuard Enterprise icon in the taskbar. A context menu opens. Select **Reset BitLocker credentials** and follow the on-screen instructions.

Note:

If you want to shut down or restart the system, click with the mouse on the shut down button or press the **Tab** key until the shut down button is highlighted:



16.3 BitLocker recovery key

As a BitLocker user on a system that does not support SafeGuard Challenge/Response, you can request a BitLocker recovery key from your helpdesk.

General hints on using mouse and/or keyboard

- You can select controls by using the mouse and/or the keyboard. To jump from one control to the next with the keyboard press the **Tab** key. To get back into the previous control use **Shift+Tab**.
- Confirm selections by pressing **Enter**.

Request the recovery key

If you need to get a BitLocker recovery key from your helpdesk, proceed as follows:

1. Reboot the endpoint. After rebooting, press the **Esc** key in the BitLocker logon screen.
2. The screen for entering a BitLocker recovery key appears.
3. In Step 2 information required to call the helpdesk is provided to you.

For example: <Computer name> C: 9/25/2014

4. Provide the **Computer name** to the helpdesk.
5. Then enter the **BitLocker recovery key** from the helpdesk (eight blocks with six characters required per field).
6. After you have successfully entered the response code, click **Continue** or press **Enter** to complete the recovery action.

Reset BitLocker credentials

As soon as you are logged on to the system again, specify new BitLocker credentials so that you will not need another Challenge/Response procedure for your next logon. Depending on your operating system and BIOS/UEFI version the system will display a dialog for the credential reset.

If this dialog does not appear automatically, right-click the SafeGuard Enterprise icon in the taskbar. A context menu opens. Select **Reset BitLocker credentials** and follow the on-screen instructions.

Note:

If you want to shut down or restart the system, click with the mouse on the shut down button or press the **Tab** key until the shut down button is highlighted:



17 SafeGuard Enterprise and Lenovo Rescue and Recovery

Note: Lenovo Rescue and Recovery is only available for Windows 7 endpoints.

You can restore complete operating system backups on an encrypted partition without decrypting the hard disk first. This saves a lot of time when performing disaster recovery. SafeGuard Enterprise has been officially certified by Lenovo for this functionality.

The main function of Lenovo Rescue and Recovery is to restore data at the press of a key. Even if the primary operating system is damaged and no longer starts, Rescue and Recovery saves data through an emergency environment (WinPE). You can access the rescue tools from the Microsoft Windows Desktop or by pressing the blue "ThinkVantage" key integrated in Lenovo systems.

Lenovo Rescue and Recovery is most useful for mobile users who do not have administrative support. For example, on a business trip, users can restore their computers with Lenovo Rescue and Recovery.

For information on the Lenovo Rescue and Recovery (RnR) versions supported by SafeGuard Enterprise, see <http://www.sophos.com/en-us/support/knowledgebase/108383.aspx>

17.1 Overview

SafeGuard Enterprise is integrated with Rescue and Recovery functionality and supports Lenovo features such as the "ThinkVantage" blue button on the keyboard of Lenovo notebooks, or the blue "Enter" key on Lenovo PC keyboards.

This integrated functionality lets you pair this efficient backup and recovery method with SafeGuard Enterprise encrypted operating system partitions. Backups from encrypted SafeGuard Enterprise systems can be stored on any disk drive used by RnR. Therefore, in an emergency, a system can be restored by loading the backup from a virtual or service partition or from a removable media device such as a CD/DVD or a USB hard disk.

SafeGuard Enterprise is unaffected by a system restore and all the encryption settings are still in place, so there is no need to reinstall any software. You do not have to restart encryption.

In a SafeGuard Enterprise environment, Rescue and Recovery is based on WinPE recovery. WinPE can be started from:

- a virtual or service partition.
- a removable media device such as a CD/DVD or a USB hard disk.

17.2 Requirements

- Latest BIOS for the PC/notebook.

- For information on compatibility of Lenovo Rescue and Recovery versions with SafeGuard Enterprise versions, see: <http://www.sophos.com/en-us/support/knowledgebase/108383.aspx>
- Lenovo Rescue and Recovery can be used to recover SafeGuard Enterprise encrypted volumes. The `SGNClient.msi` installation package must be installed.
- For Rescue and Recovery, volumes must be encrypted with the defined machine key. For volumes encrypted with any other keys, Rescue and Recovery is not supported.

17.3 Installation

When Rescue and Recovery software is installed on a hard disk without a service partition, the following applies:

The Rescue and Recovery environment is installed on a virtual partition on the computer's hard disk "C:" partition (primary partition of the master hard disk).

In the sections that follow, note the sequence in which Rescue and Recovery and SafeGuard Enterprise are installed. We recommend that you install Lenovo Rescue and Recovery first, and SafeGuard Enterprise afterwards.

17.3.1 Install both Rescue and Recovery and SafeGuard Enterprise

The following installation sequence is recommended:

1. Install the latest version of Rescue and Recovery.
2. Install the latest version of the SafeGuard Enterprise Device Encryption module (`SGNClient.msi`).
SafeGuard Enterprise checks if Rescue and Recovery is installed, and adds its own files and configurations to the Lenovo recovery environment.
3. Check that the SafeGuard Power-on Authentication is activated, so no unauthorized backups can be restored.

You activate the SafeGuard Power-on Authentication when you install SafeGuard Enterprise.

17.3.2 Rescue and Recovery is already installed

RnR WinPE is located on the first hard disk on a service or virtual partition.

In this case all necessary drivers and files are copied to the corresponding locations of RnR WinPE, and the necessary registry entries are added to the registry files of WinPE.

Install the latest version of the SafeGuard Enterprise Device Encryption module (`SGNClient.msi`).

SafeGuard Enterprise checks if Rescue and Recovery is installed and adds its own files and configurations to the Lenovo recovery environment (WinPE).

17.4 Upgrade

Upgrade implies that SafeGuard Enterprise and Rescue and Recovery are installed, and you want to upgrade one or both to a newer version.

Upgrade SafeGuard Enterprise

If you upgrade SafeGuard Enterprise, this updates the entire system, so you will not need to set any further configurations.

17.5 Uninstallation

When uninstalling the software products:

- We recommend that you uninstall SafeGuard Enterprise first, and then Rescue and Recovery. If SafeGuard Enterprise is uninstalled while Rescue and Recovery is still installed, all SafeGuard Enterprise specific modifications, such as added drives, files, and registry entries are removed from RnR WinPE.
- Do not uninstall SafeGuard Enterprise immediately after the system has been restored. After a system restore, start the computer once and then uninstall SafeGuard Enterprise.
- If Rescue and Recovery is removed while SafeGuard Enterprise is still installed, then RnR modifications of the MBR boot sector are removed, and the original MBR boot sector is restored.

17.6 Boot environment and recovery options

SafeGuard Enterprise allows you to boot into the Rescue and Recovery environment after successfully having logged on at the SafeGuard Power-on Authentication (POA).

From the local hard disk

- The virtual partition on the local hard disk or the local service partition.
- The volumes must have been encrypted in SafeGuard Enterprise with the defined machine key. All necessary drivers must have been added to RnR WinPE. Then the defined machine key is available in the RnR WinPE environment and the volumes can be accessed again.

Note: SafeGuard Enterprise does not allow you to boot into the Rescue and Recovery environment when booting directly from BIOS.

From a bootable CD/DVD or any bootable removable media

- In this case no authentication at the SafeGuard POA is performed, and there are no keys available, so encrypted volumes cannot be accessed. If Rescue and Recovery is started directly from BIOS, the operating system will be recovered. SafeGuard Enterprise will be removed during the restore process. To secure the system again, SafeGuard Enterprise must be reinstalled.

17.7 Create a backup

You create backups using Rescue and Recovery in Windows. On computers on which Rescue and Recovery is already installed, and on which SafeGuard Enterprise is installed later, a message is displayed prompting the user to create a new backup of the system.

Before creating a backup of your system using Rescue and Recovery, please read the documentation provided by Lenovo.

SafeGuard Enterprise only provides support for saving the backups to:

- local hard disk
- second hard disk
- USB hard disk
- network
- startup key
- CD/DVD

By default the backups are saved in the `C:\RRUbackups` folder. This folder is protected by Rescue and Recovery if it is stored on a local partition on the primary hard disk drive. If so, it cannot be deleted or removed.

17.8 Restore file backups

Rescue and Recovery can restore files or folders from backups in which SafeGuard Enterprise is installed. Simply start Windows, and then Rescue and Recovery, and restore the selected files. You do not have to restart your machine after the restore is completed, you can work with your files immediately.

17.9 Restore the SafeGuard Enterprise system

To restore a system backup that includes SafeGuard Enterprise, boot into the Rescue and Recovery environment. The RnR environment appears as soon as you press one of following keys during the startup process:

- "Thinkvantage" (Lenovo Notebooks)
- Blue "Enter" key (Lenovo Desktop PCs)
- **F11** with other keyboards

1. If you use a Lenovo computer:

- a) Start the Rescue and Recovery environment from a local hard disk by pressing the blue "ThinkVantage" button on the Lenovo notebook keyboard, or the blue "Enter" button on a Lenovo PC keyboard.

The SafeGuard Power-on Authentication is displayed.

- b) Enter the SafeGuard Enterprise credentials.

2. If you do not use a Lenovo computer:

- a) Log in at the SafeGuard POA with your SafeGuard Enterprise credentials.
- b) While the computer continues starting up, press **F11** to start the Rescue and Recovery environment.

The user interface for Rescue and Recovery is displayed. The welcome screen is displayed.

3. Click **Next**.

4. On the left-hand side menu, select **Restore Backup**.
A dialog is displayed in which you can select the backup.
5. Select the backup and restore it.

17.10 Service and factory recovery partitions

Lenovo supplies new computers with special pre-installed partitions:

- **Lenovo service partition:** contains the Rescue and Recovery boot environment.
- **Factory recovery partition:** contains all information about the computer's factory settings and factory recovery functions.

These partitions are visible in Windows under separate drive letters.

Note: When these partitions are available on the computer, they will never be encrypted even if an encryption policy is defined to, for example, encrypt all volumes.

If there are no such partitions on the computer, but you would like to create one, do so before installing SafeGuard Enterprise. For further information, refer to the Lenovo documentation.

17.11 Disabled SafeGuard POA and Lenovo Rescue and Recovery

If the SafeGuard Power-on Authentication is disabled on your computer, the Rescue and Recovery authentication should be enabled for protection against access to encrypted files from the Rescue and Recovery environment.

For details on activating the Rescue and Recovery authentication, refer to the Lenovo Rescue and Recovery documentation.

18 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>.

19 Legal notices

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

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.

Sophos, Sophos Anti-Virus and SafeGuard are registered trademarks 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.

You find copyright information on third party suppliers in the *Disclaimer and Copyright for 3rd Party Software* document in your product directory.