SOPHOS

Cybersecurity made simple.

SafeGuard Enterprise

user help

product version: 8.3

Contents

1 About SafeGuard Enterprise

Sophos SafeGuard runs on Windows endpoints to protect them. It consists of several modules.

You may not have all the features described in this Help. This depends on your license and the policies you received from your security officer.

Sophos SafeGuard is configured and managed centrally from the Sophos SafeGuard Management Center.

To access general information on your installation of Sophos SafeGuard, click the Sophos SafeGuard icon in the Sophos SafeGuard system tray (page 7).

The most important options for encrypting and decrypting files are available in a right-click menu in the Windows Explorer.

This document relates to Windows endpoints only. For Mac endpoints, see the SafeGuard Enterprise for Mac user help.

Modules:

Full disk encryption

- **Full disk encryption with BitLocker (page 2)**

Synchronized Encryption

- **SafeGuard File Encryption (application-based) (page 2)**

File encryption

- **SafeGuard File Encryption (location-based) (page 3)**
- **SafeGuard Cloud Storage (page 3)**
- **SafeGuard Data Exchange (page 4)**

2 Modules

2.1 Full disk encryption with BitLocker

Full disk encryption with BitLocker builds on the BitLocker Drive Encryption technology included in your operating system. It encrypts the entire hard disk, so that your data is safe even if the computer is lost or stolen.

When you log on to your endpoint, you have to enter user credentials to unlock BitLocker. For more information, see Encrypt a computer with BitLocker (page 10).

Sophos SafeGuard allows you to manage BitLocker on endpoints with one of the following operating systems:

- Windows 8.1 Professional / Enterprise
- Windows 10 Professional / Enterprise

2.2 SafeGuard File Encryption (application-based)

Application-based file encryption encrypts files created or modified with specific applications (for example, Microsoft Word). A policy defines a list of applications for which file encryption is executed automatically. This encryption is persistent, so your file is safe even if you move it to another location, upload it to a cloud storage provider, or send it via email.

If your security officer has specified Microsoft Word as an application for which file encryption is active, every file you create and/or save with Microsoft Word is encrypted with a defined key. Anyone whose key ring includes this key can access your file.

- New files created with defined apps or file extensions 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, you cannot read its content.
- If you access an encrypted file from a computer where File Encryption is not installed, you cannot read its content.
- Files that are copied or moved from a plain folder to a folder where an encryption rule applies are encrypted.
- Files that are copied or moved from an encrypted folder to a plain folder are decrypted.
- Files that are copied or moved from an encrypted folder to a folder with a different encryption rule are encrypted according to the rule of the target folder.
- Files that are created by applications for which File Encryption is not active, but there is an encryption rule for the file extension, the file is encrypted and cannot be opened with the application that created the file. For example, if you create a .doc file with OpenOffice and OpenOffice is not specified in **Application Lists**.

Important
If copying or moving files is interrupted, for example due to a restart, the operation will not be resumed automatically. This can result in unintentionally unencrypted files. To ensure that files are always encrypted correctly, see Encrypt all files according to policy (page 12).

To find out which locations on a computer are encrypted, see See where files are encrypted (page 14).

To find out about the encryption state of one or more files, right-click the file(s) and select **SafeGuard File Encryption > Show encryption state**.

In Windows Explorer, encrypted files are marked with a green lock symbol. If there is no lock symbol displayed even though the file is encrypted, see Sophos knowledgebase article 108784.

2.3 SafeGuard File Encryption (location-based)

Location-based file encryption allows your security officer to define locations where files are encrypted, for example, **Documents**.

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

- New files in a location that is specified for encryption 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, you cannot read its content.
- If you access an encrypted file from a computer where File Encryption is not installed, you cannot read its content.

To find out which locations on your computer are encrypted, see See where files are encrypted (page 14).

To find out about the encryption state of one or more files, right-click the file(s) and select **SafeGuard File Encryption > Show encryption state**.

In Windows Explorer, encrypted files are marked with a green lock symbol. If there is no lock symbol displayed even though the file is encrypted, see Sophos knowledgebase article 108784.

2.4 SafeGuard Cloud Storage

SafeGuard Cloud Storage offers location-based encryption of files stored in the cloud. It does not change the way you work with your files, but it makes sure that the local copies of your cloud data are encrypted transparently and remain encrypted when stored in the cloud.

SafeGuard Cloud Storage automatically detects your cloud storage provider (if supported) and applies the encryption policy to the synchronization folder.

SafeGuard Cloud Storage does not perform an initial encryption of your data. Files that were stored before SafeGuard Cloud Storage was installed or activated by a policy remain unencrypted. If you want to encrypt these files, you have to remove them from the cloud first and then add them again.

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 plain text. To make sure that files are encrypted, 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.

2.5 SafeGuard Data Exchange

SafeGuard Data Exchange offers location-based encryption of files stored on removable media so you can exchange them with other users. Only users who have the appropriate keys can read the contents of the encrypted data. All encryption and decryption processes are run transparently and involve minimum user interaction.

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.

Your 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.

2.5.1 Overlay icons

Overlay icons are small icons displayed on elements in Windows Explorer. Their purpose is to give you quick information on the encryption state of files. The appearance of the icons depends on the module you have installed.

The Data Exchange overlay icons are only displayed on files and volumes.

- 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.

Note
If there are no overlay icons displayed, see Sophos knowledgebase article 108784.

2.5.2 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.

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.

2.5.3 Media passphrase for removable media

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.

For instructions on how to define a media passphrase, see Use a media passphrase (page 18).

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.

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

Blu-ray discs and dual-layer DVDs are not supported.

3 Sophos SafeGuard system tray

You can access all Sophos SafeGuard functions on your computer using the Sophos SafeGuard system tray icon on the Windows taskbar. The availability of specific functions depends on the modules you have installed.

Right-click the Sophos SafeGuard system tray icon to display the following:

- **Display**:
  - **Key ring**: Displays all keys available to you.

    Note
    If your endpoint computer has been migrated from an unmanaged to a managed environment, a second logon to SafeGuard Enterprise may be necessary to display your user-defined local keys in your key ring.

  - **User Certificate**: Displays information concerning your certificate.
  - **Company Certificate**: Shows information concerning your company certificate.
- **Reset BitLocker credentials**: Opens a dialog for changing your BitLocker PIN.
- **Create new key**: Opens a dialog for creating a new key that is used for SafeGuard Data Exchange (page 4) or SafeGuard Cloud Storage (page 3). Only available, if either module is installed on your computer.
- **Change Media Passphrase**: Opens a dialog for changing the media passphrase, see SafeGuard Data Exchange (page 4).
- **Synchronize**: Starts synchronization with the SafeGuard Enterprise Server. Tool tips show the progress of the synchronization. You can also double-click the system tray icon to start synchronization.
- **Status**: Opens a dialog showing information on the current status of the SafeGuard Enterprise protected computer:

Field	Information
Last policy received	Date and time when the computer last received a new policy.
Last key received	Date and time when the computer last received a new key.
Last certificate received	Date and time when the computer last received a new certificate.
Last server contact	Date and time of the last server contact.

Field	Information
SGN user state	Status of the user who is logged on to the computer (Windows logon): — **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** 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. — **unconfirmed user** Unconfirmed users have no access to the keyring due to one of the following reasons: – User provided wrong credentials. – User is a local user. – AD authentication server is not reachable. – Authentication failed. – See also Sophos knowledgebase article 124328. The user must be confirmed by the security officer in order to gain access to the keyring. — **unknown** Indicates that the user status could not be determined.

Field	Information
SGN machine state	Indicates the safety level of the endpoint. — **not applicable** The related feature is inactive. — **machine is safe** The machine's health state is safe. — **machine is compromised** The machine's health state is unsafe. Therefore, keys have been revoked and you cannot access encrypted files.
Policy Cache State **Data packets prepared for transmission**	Indicates whether there are any packages to be sent to the SafeGuard Enterprise Server.
Local Self Help (LSH) State **Enabled** **Active**	Indicates whether Local Self Help has been enabled in a policy and whether it has been activated by the user on the computer.
Ready for certificate change	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. For more information, see the SafeGuard Enterprise 8.0 user help.

- **Help**: Opens the SafeGuard Enterprise user help.
- **About SafeGuard Enterprise**: Displays information about your SafeGuard Enterprise version.

4 How to ...

4.1 Encrypt a computer with BitLocker

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 the USB flash drive is not available or accessible, you will be asked to store the external key on a different 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 starts.

If you select **Postpone**, encryption will not be started and you will not 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.

4.1.1 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. We recommend using an unencrypted USB flash drive to store the key. The valid target drives for the startup key are listed in the dialog. Later, you will have to insert the storage device with the key each time you start the computer.

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

4.1.2 Set password

If your security officer specified **Password** as the logon mode, you are asked to enter and confirm your new password. 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
Be careful when setting a PIN or password. The pre-boot environment only supports the US-English keyboard layout. If you set a PIN or password now with special characters, you might have to use different keys when you enter it to log on later.

4.1.3 Set PIN

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

Note
Be careful when setting a PIN or password. The pre-boot environment only supports the US-English keyboard layout. If you set a PIN or password now with special characters, you might have to use different keys when you enter it to log on later.

4.1.4 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.

4.2 Reset a forgotten BitLocker PIN/password

If you cannot log on to your computer because you have forgotten your PIN, password, or USB key, you need a recovery key. To request a recovery key:

1. Restart your computer and press the **Esc** key in the **BitLocker** logon screen.
2. In the **BitLocker recovery** screen, find the **Recovery key ID**.
   The **Recovery key ID** is displayed for a short time. To display it again, you must restart the computer.
3. Contact your administrator and give them the **Recovery key ID**.
   Your administrator needs to find the recovery key to your computer in the Sophos SafeGuard Management Center and give you the key.
4. In the **BitLocker recovery** screen, enter the recovery key.
   You can now start your computer.

As soon as you are logged on to the system again, specify new BitLocker credentials. Depending on your operating system, a dialog for the credential reset is displayed. If this dialog does not appear automatically, right-click the Sophos SafeGuard icon in the taskbar, select **Reset BitLocker credentials** and follow the on-screen instructions.

4.3 Reset a forgotten BitLocker PIN/password with Challenge/Response

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\<Computer name>
   - **Challenge** code, for example ABC12-3DEF4-56GHO-892UT-Z654K-LM321. Move your 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. Enter the **response code** from the helpdesk (six blocks with two text fields each and five characters required per field).
   - As soon as a text field is completely populated, 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.
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. Depending on your operating system, a dialog for the credential reset is displayed. If this dialog does not appear automatically, right-click the Sophos SafeGuard icon in the taskbar, select **Reset BitLocker credentials** and follow the on-screen instructions.

4.4 Encrypt all files 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.

To start the encryption process manually, right-click the **This PC** node in Windows Explorer and select **SafeGuard File Encryption > Encrypt according to policy**. The SafeGuard File Encryption Wizard (page 12) encrypts all files in folders and subfolders covered by the defined encryption rules.

4.4.1 SafeGuard File Encryption Wizard

To open the SafeGuard File Encryption Wizard, right-click the **This PC** node or a folder in Windows Explorer and select **SafeGuard File Encryption > Encrypt according to policy**.

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 or processed 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.

4.5 Encrypt/Decrypt files manually

SafeGuard File Encryption allows you to encrypt or decrypt individual files manually. Right-click a file and select **SafeGuard File Encryption**. The following functions are available:

- **Show encryption state**: Indicates whether or not the file is encrypted as well as the key used.
- **Encrypt according to policy**: See Encrypt all files according to policy (page 12).
- **Decrypt**: (only for location-based file encryption): Allows you to decrypt a file that is not covered by a File Encryption rule.
- **Decrypt selected file** (only for application-based file encryption): Allows you to decrypt your file and store it in plaintext. We recommend decrypting your file only if it does not contain any sensitive data.
- **Encrypt selected file** (only for application-based file encryption): Allows you to manually encrypt files with the key specified in your policy.
- **Create password protected file**: Here you can define a password to encrypt individual files manually. This is useful if you want to securely share your file with someone outside your corporate network, see Send encrypted files via email (page 15).

If you right-click folders or drives, the following functions are available:

- **Show encryption state**: Displays a list of the included files with icons indicating the encryption state as well as the key used.
- **Encrypt according to policy**: See Encrypt all files according to policy (page 12).

The following options are only available for Cloud Storage and Data Exchange:

- **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.

4.6 See where files are encrypted

If you want to check where files are encrypted on your computer and which keys are used to protect your files, you can use the SafeGuard Enterprise `FETool` tool.

To open the SafeGuard Enterprise `FETool` tool, open a command prompt, go to `C:\Program Files (x86)\Sophos\SafeGuard Enterprise\FileEncryption` and enter `fetool rli -a`.

This command lists all encryption rules that apply to your computer. The list contains the encryption mode, the full path to the appropriate folders, and the keys used.

4.7 Use a password to protect a file

When sending emails to recipients outside your corporate network, we recommend that you encrypt your file with a password. This allows the recipients to access encrypted files without having SafeGuard Enterprise installed.

Do the following:

1. Right-click the file you want to send and select **Create password protected file**.
2. Follow the on-screen instructions and create a password. We recommend that you use a strong password and don't send it in the same email as the files.
   Your file is encrypted and saved as an HTML file. You can now safely attach the HTML file to emails.

   Note
   - You need free disk space for the encryption.
   - The encrypted HTML file is bigger than the original file.
   - The maximum supported file size is 50 MB.
   - To send several files at once, you can compress them into a .zip file and then encrypt the .zip file.

3. Give your recipients the password by phone or through any other means of communication. Recipients can use one of the following browsers to open the password protected attachment:
   - Mozilla Firefox
   - Google Chrome

- Microsoft Internet Explorer 11
- Microsoft Edge

4. Instruct your recipients to double-click the file and follow the on-screen instructions to do one of the following:
   - Enter the password and click **Enter** to access the file.
   - Click **Password protect a new file** to protect a different file with a password.

Recipients can access a file you protected with a password. They can protect the file with a password when sending it back to you. They may use the same password or a new password. They can even protect a new file with a password.

4.8 Send encrypted files via email

When you send encrypted files to recipients in your corporate network, you do not need to worry about encryption and decryption. If your recipient has the appropriate key, they will be able to read the file.

For sending emails to recipients outside your corporate network, SafeGuard Enterprise offers an add-in for Microsoft Outlook that makes encrypting email attachments easy. Whenever you send an email with one or more files attached, the system prompts you to choose how to send the attachments. The available options may vary according to the encryption state of the files you attached to your email.

Note
When you send embedded items such as contacts (.vcf) or emails (.msg) as attachments, you are not prompted to encrypt them. They are sent unencrypted.

- **Password protected**

  Select this option if you are sending sensitive files to recipients outside your organization.

  After you define a password and press send, your file is encrypted and saved as an HTML file. If you password protect several files at once, each file is encrypted separately with the same password. Files that are already encrypted are decrypted automatically before they are password protected.

  Recipients can open the file with their web browser as soon as you communicate the password to them. We recommend that you use a strong password and don't send it in the same email as the files. We recommend that you give the recipients the password by phone or through any other means of communication.

  Recipients can use one of the following browsers to open the password protected attachment:

  — Mozilla Firefox

  — Google Chrome

  — Microsoft Internet Explorer 11

  — Microsoft Edge

  Decryption with other browsers, such as mobile browsers, may work but is not actively supported.

  Recipients can edit the file and send it back using the same password or a new password. They can even protect a new file with a password. They are guided through the procedure by a wizard in their browser. For more information, see Sophos knowledgebase article 124440.

You can also password protect files manually, see Use a password to protect a file (page 14).

- **Unprotected**

  Select this option only if your email attachment does not contain any sensitive data. Any case in which you send email attachments unprotected may be logged and monitored by your security officer.

- **Attachments to be sent unchanged**

  If the email contains attachments that cannot be password protected, you can either send them unchanged or remove them from your email. The dialog contains a list of files that cannot be protected for one of the following reasons:

  — The file is already password protected. You can either decrypt the file first and use a new password, or you send the file unchanged and communicate the relevant password to the recipient.

  — The file has been encrypted with a key that is currently unavailable in your keyring. The key may have been temporarily revoked because of a security issue, or you do not own the key used for encrypting the file. In this case, please ask your security officer.

When you send an email to both internal and external recipients, the system handles the email as if it were sent to external domains only.

4.9 Create a local key

Local keys can be used for encrypting files in specified locations on a removable device or a cloud storage provider. These locations must be included in an encryption policy already.

To create a local key:

1. Right-click the Sophos SafeGuard 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 comply 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 **SafeGuard**

File Encryption > Encrypt according to policy 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.

4.9.1 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 file on the removable media and click **SafeGuard 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.

4.10 Exchange data with 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 their 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

  Users who do not have SafeGuard Enterprise installed on their computer can use SafeGuard Portable to access encrypted files. SafeGuard Portable is not supported on Macs. For more information, see:

  — Exchange data on removable media without SafeGuard Enterprise (page 19)

  — Edit files with SafeGuard Portable (page 23)

4.10.1 Encrypt removable media with SafeGuard Data Exchange

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 allowed 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 **SafeGuard File Encryption > Encrypt according to policy** 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.

Cancel 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.

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

4.10.2 Use a 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.

Note that you cannot use a media passphrase on Macs.

Change/reset a 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.

Synchronize a media passphrase

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 are informed that the media passphrases have been synchronized. This is true for all computers for which you have logon permission. Note that you cannot use a media passphrase on Macs.

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).

4.10.3 Exchange data on removable media without SafeGuard Enterprise

SafeGuard Portable allows you to exchange encrypted data on removable media with recipients who do not have SafeGuard Enterprise.

Note
SafeGuard Portable is not supported on Mac computers or computers with Sophos SafeGuard installed.

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.

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.

Recipients can decrypt encrypted data and encrypt it again as soon as you give them the required media passphrase or the passphrase of a local key. They 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 the recipients' computer. It remains on the removable media.

For more information, see Edit files with SafeGuard Portable (page 23).

4.10.4 Write files to CDs/DVDs with SafeGuard Data Exchange

SafeGuard Data Exchange allows you to write encrypted files to CDs/DVDs with the Windows CD Writing Wizard. Your security officer must define an encryption rule for the CD recording drive. If there is no encryption rule for the CD recording drive, files are always written to the CD in plain text.

The SafeGuard Disc Burning Extension for the CD Writing Wizard is only available for burning 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.

In the CD Writing Wizard, you can specify how the files are written to CD (encrypted or plain text). 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 plain text 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 plain text 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 plain text

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.

4.11 Exchange data in the cloud without SafeGuard Enterprise

SafeGuard Portable allows you to exchange encrypted data in the cloud with recipients who do not have SafeGuard Enterprise.

SafeGuard Portable allows you to access encrypted data in your cloud storage from computers without SafeGuard Enterprise. 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. 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 Edit files with SafeGuard Portable (page 23).

Double-clicking a file or selecting the open command doesn't cause in-place decryption of the file. This is because decrypted files in cloud storage synchronization folders are automatically 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 are not 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 unencrypted files in those folders.

4.12 Use default keys

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.

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 in your cloud storage.

You can define a default key from the context menu in the following locations:

- removable media
- files on removable media
- Cloud Storage synchronization folders or sub-folders
- files 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 **SafeGuard File Encryption > Set default key**.

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.

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

If you intend to read encrypted files on Android and iOS devices with Sophos Secure Workspace, you must use local keys for encryption. For further information, see the Sophos Secure Workspace user help.

Example

You want to use Dropbox to provide secured data for multiple partners and to give each partner access to only one subfolder. To do this, simply set a separate default key for each subfolder. SafeGuard Enterprise will 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.

4.13 Recover encrypted files

If a file is encrypted with a key that is not available in your keyring, you cannot open the file. This might be the case because you are not supposed to access this file according to company policy. However, in some cases, you may be allowed access to the file but you just happen not to have the required key. In this case, you need to find out which key was used and ask your security officer to assign the key to your keyring. Proceed as follows:

1. Right-click the file and then click **SafeGuard File Encryption > Show encryption state**.
   The key used for encrypting this file is displayed.
2. Contact your security officer and provide them with the key name.
3. Ask your security officer to assign the key to your keyring.
4. As soon as your security officer confirms that your user policy has been updated, right-click the Sophos SafeGuard system tray icon in the taskbar of your computer.
5. Click **Synchronize**.
6. Again, right-click the system tray icon and then click **Status**.
   A dialog displays the date when the last key was transferred to your computer. The current date is displayed under **Last key received** when your requested key has been added to your keyring.

You can now access the file.

4.14 Check your connection to the SafeGuard Enterprise Server

If you are having trouble synchronizing your endpoint with the server, you can use the Client/Server Connectivity Check tool to find out why the communication between the endpoint and the SafeGuard Enterprise Server fails.

To open the SafeGuard Enterprise Client/Server Connectivity Check tool, go to `C:\Program Files (x86)\Sophos\SafeGuard Enterprise\Client` and run the `SGNCSCC.exe` application.

For more information, see Sophos knowledgebase article 109662.

4.15 Edit files with SafeGuard Portable

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

You have received 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 and then re-encrypt it.

   In addition to the file details, 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. You can only decrypt files if you know the relevant passphrase for the key used.
2. To edit a file, right-click it and select one of the following commands:

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

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

4.15.1 Set encryption keys for SafeGuard Portable

To set an encryption key for SafeGuard Portable:

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

   The **Enter Key** dialog is displayed.
2. Enter a **Name** and a **Passphrase** for the key.
3. 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.

4.15.2 Encrypt files with SafeGuard Portable

1. In SafeGuard Portable, right-click the file and select **Encrypt**.

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

When saving new files using drag-and-drop, you are asked if you want to encrypt the files.

If no default key is set, a dialog for setting one opens. Enter the name of the key and the passphrase, confirm the passphrase, and click **OK**.

2. To encrypt more files with the key you have just set, select **Encrypt** from the context menu or from the **File** menu.
   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.

4.15.3 Decrypt files with SafeGuard Portable

1. In SafeGuard Portable, right-click the file and select **Decrypt**.

   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, regardless of which local key was used to encrypt them. If you only have the passphrase of a local key, you only have access to the files that 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 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.

Files that have been decrypted are encrypted again when you close SafeGuard Portable.

5 Support

Full release

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

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

6 Legal notices