SOPHOS

Cybersecurity made simple.

SafeGuard Enterprise

quick start & best practice guide

product version: 8.3

Contents

1 About this guide

This guide helps you get started with the new features of SafeGuard Enterprise:

- Multi-key support for Synchronized Encryption
- Improvements with protecting files with a password
- Outlook Add-in for location-based encryption

It provides an overview of the features, how they work, and how to implement them in your environment. For more information about the Synchronized Encryption module, see the SafeGuard Enterprise administrator help.

This guide is not a comprehensive installation guide, but is mainly intended for users who are already familiar with the product. For more information on installation and administration, see the SafeGuard Enterprise administrator help.

2 Best Practice: multi-key support for Synchronized Encryption

SafeGuard Enterprise allows you to configure additional encryption keys for specific locations when using Synchronized Encryption.

These instructions work through the following example:

- Your company has selected **Application-based (Synchronized Encryption)** for encrypting all files created by commonly used applications with the default **Synchronized Encryption key**.
- Encrypt files in the users' `Documents` folder with their **Personal Key**.
  - The users' `Documents` folder should contain the `/unencrypted` folder where users can store files in plain.
- To make sure that all files on endpoints are encrypted according to your company's policy, you should turn on initial encryption.

2.1 Creating a multi-key file encryption policy

1. In the Management Center, select the **(Default) File Encryption** policy and select **Application-based (Synchronized Encryption)** under **Encryption type**.
2. Under **Application list**, select **Template**.

   The default application list is called **Template**. It contains the most commonly used applications.
3. Under **Encryption scope**, select **Everywhere**. This is the most secure option, generally used for Windows endpoints.

   This creates a rule to encrypt files in all locations with the **Synchronized Encryption key**. The rule is added to the list of locations where application-based encryption is applied.

   You can now add specific rules for locations that you want to be encrypted with different encryption keys. These locations can be local or on the network. You can use predefined values to specify them.

   In our example, we want to encrypt the users' `Documents` folder.
4. To add a rule click in the **Path** edit field and select **<Documents>** from the drop-down menu.

   Note
   You cannot change the encryption scope.

   The default key is the **Synchronized Encryption Key**, but you can choose any other encryption key. For example, the domain key, or the key of an organizational unit. You can also select the **Personal Key** which is unique to every user.
5. Click the **Personal Key** symbol in the **Key** edit field to select the users' personal keys to encrypt the `Documents` folder. You can hover over the key symbols to display their function.

   To have an unencrypted folder you need to define an exception rule for that specific folder.
6. Click in the **Path** edit field, select **<Documents>** from the drop-down menu and enter `\unencrypted` after the **<Documents>** placeholder.
7. In the **Mode** column, select **Exclude** from the drop-down menu.

8. To turn on initial encryption on the endpoints, set the **Stored on local disks** option under **Initial encryption: Automatically encrypt existing files** to **Yes**.
9. Save the policy and deploy it.

Note
When you assign such a policy, with only specific rules for locations and different keys, to endpoints that have SafeGuard Enterprise 8.0 installed, these rules are applied correctly. All specified locations are encrypted with the selected keys. However, if a rule with **Encryption scope** set to **Everywhere** is part of the policy, only the **Synchronized Encryption Key** is used. Files in all specific locations are encrypted with the **Synchronized Encryption Key** as well.

2.2 Application-based encryption with multiple keys on endpoints

The endpoint has the SafeGuard Enterprise Encryption software installed, but no policy applied.

When you click **Synchronize** on the SafeGuard Enterprise system tray, the endpoint receives the updated policies. The policy changes include the list of applications for which all new files must be encrypted. This list includes Microsoft Office, so all new Microsoft Office files are encrypted.

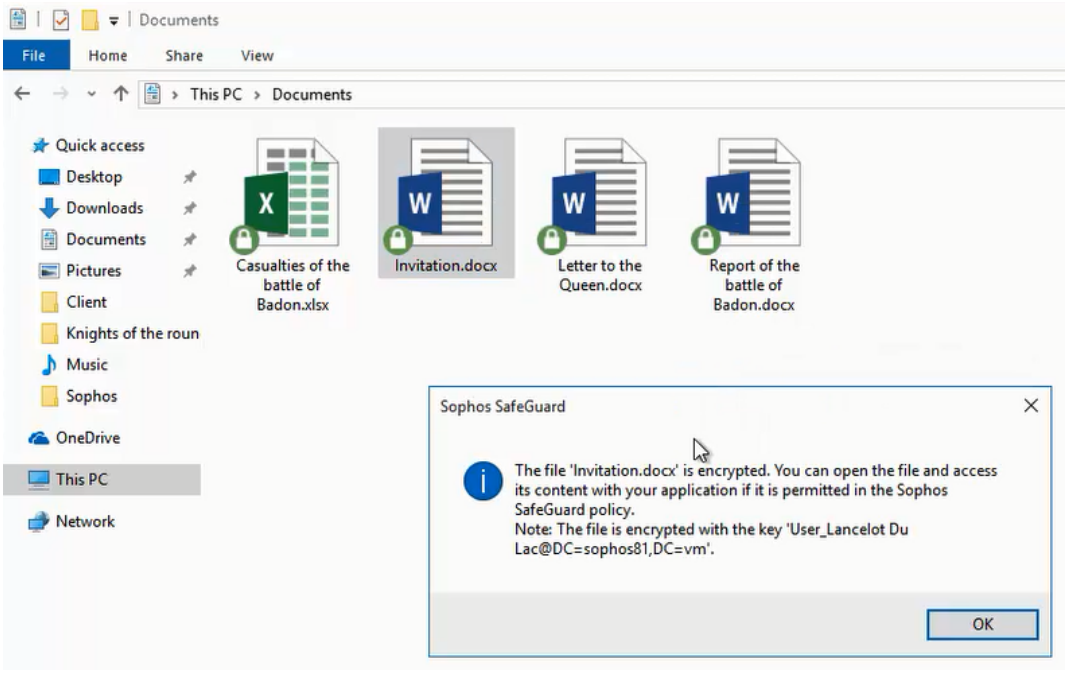
As you turn on initial encryption for all local drives, all files that are already on the computer are encrypted as well.

Note
When you create an application list, you have to specify explicitly the file extensions of files to be processed by initial encryption. The **Template** application list includes the most common extensions for each application.

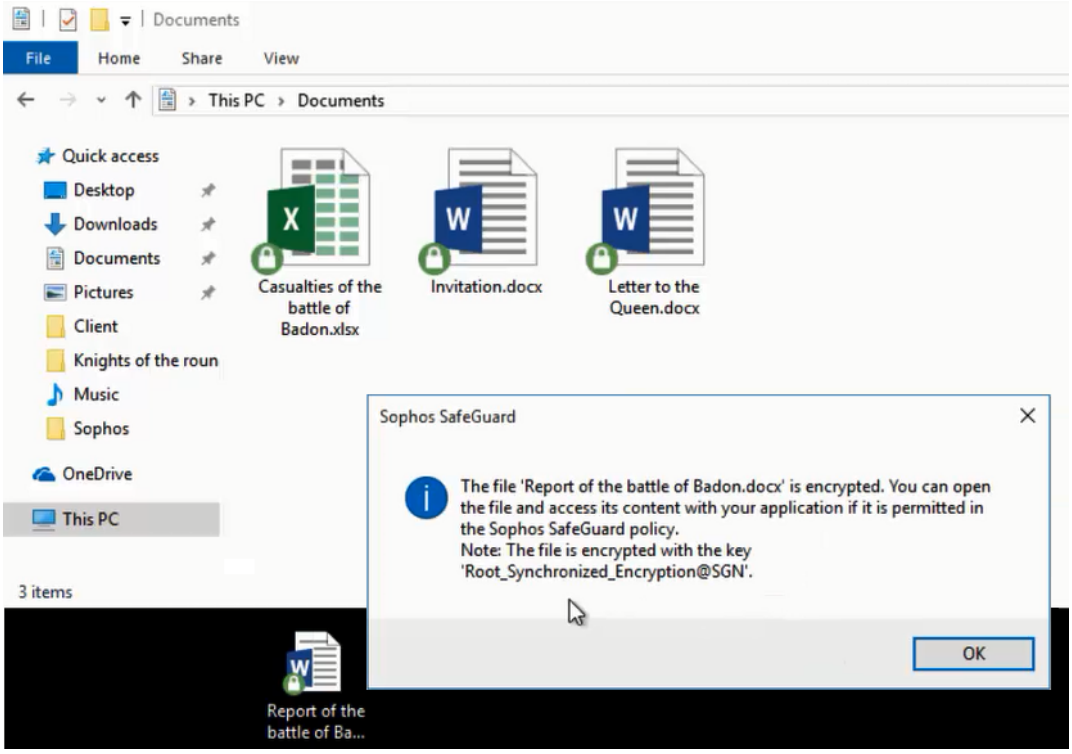
- Files in the `Documents` folder are encrypted with the users' **Personal Key**.
- All other files that need to be encrypted according to the application list are encrypted with the **Synchronized Encryption key**.

Encryption scope Everywhere vs. Defined Locations

You chose to use the **Synchronized Encryption key** everywhere and made an exception for the **<Documents>** folder where the users' **Personal Key** should be used.



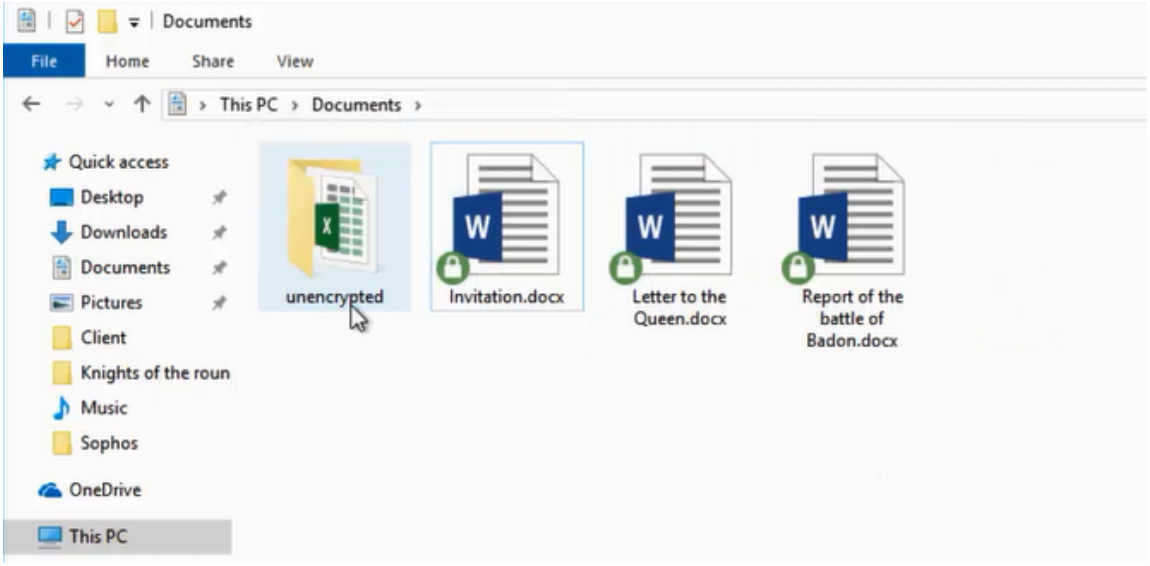
Moving or copying a file changes the encryption key. The new location is part of the **Everywhere** rule and therefore the **Synchronized Encryption key** is used.



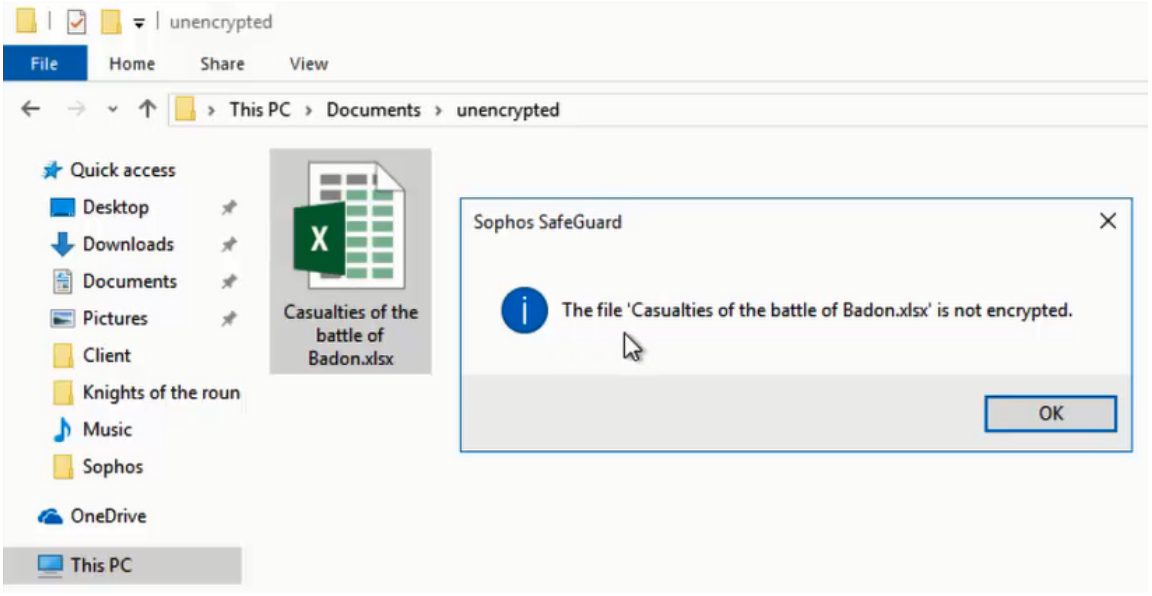
Moving a plain or already encrypted file to the **<Documents>** folder encrypts the file with the user's **Personal Key**.

Folder without encryption

In the policy, you set the **<Documents>**`\unencrypted` folder as a location where you do not want to have files encrypted.



When you move a file to the unencrypted folder, it is decrypted.



SafeGuard Enterprise automatically decrypts files only if you put one or more individual files to a location without encryption. If you move a folder to an exclude folder or if you rename a folder to the name of an exclude folder, files are not decrypted automatically to avoid accidental decryption. You can then decrypt the files manually or use the Encrypt according to policy option from the folder's SafeGuard Enterprise context menu.

3 Outlook Add-in for location-based encryption

Since version 8.1 the SafeGuard Enterprise Outlook Add-In for Windows is available for location-based encryption. It is available on endpoints when you install any location-based File Encryption module.

In general, the functionality for sending external emails is the same as for application-based encryption. However, for sending emails with attachments to white-listed domains, there are some caveats due to the nature of location-based encryption and the multi-key feature of Synchronized Encryption.

In the **(Default) General Settings** policy, you can configure what happens with attachments to emails sent to white-listed (usually internal) domains. Available options for **Behavior for white-listed domains** are:

- **Encrypted**
- **No encryption**
- **Always ask**
- **Unchanged (Synchronized Encryption)**

No encryption and **Always ask** behave the same for all File Encryption modules.

The options **Encrypted** and **Unchanged (Synchronized Encryption)** behave differently when used with Synchronized Encryption or location-based encryption.

Encrypted

- Synchronized Encryption

  Encrypted files keep their encryption, the encryption key isn't changed. Plain files are encrypted with the **Synchronized Encryption key**, but only if the file extension is defined in the list of In-Apps.

- Location-based encryption

  All attached files are encrypted with the **Synchronized Encryption key**, regardless of their file extensions and encryption status.

Unchanged (Synchronized Encryption)

- Synchronized Encryption

  Encrypted files will be sent encrypted, plain files will be sent in plaintext.

- Location-based encryption

  All files are encrypted with the **Synchronized Encryption key**.

4 Password protected files

Synchronized Encryption introduced the concept of password protected files, where users can create encrypted HTML files that need a password for decryption.

As of SafeGuard Enterprise 8.1, this feature is also available in the location-based encryption module on Windows.

Note
On macOS, this feature has been available since version 8.

4.1 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. Right-click the file you want to send and select **Create Password Protected File**.
   If you receive an error message, select **View > Hide Preview** in the Finder and try again.
3. 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.

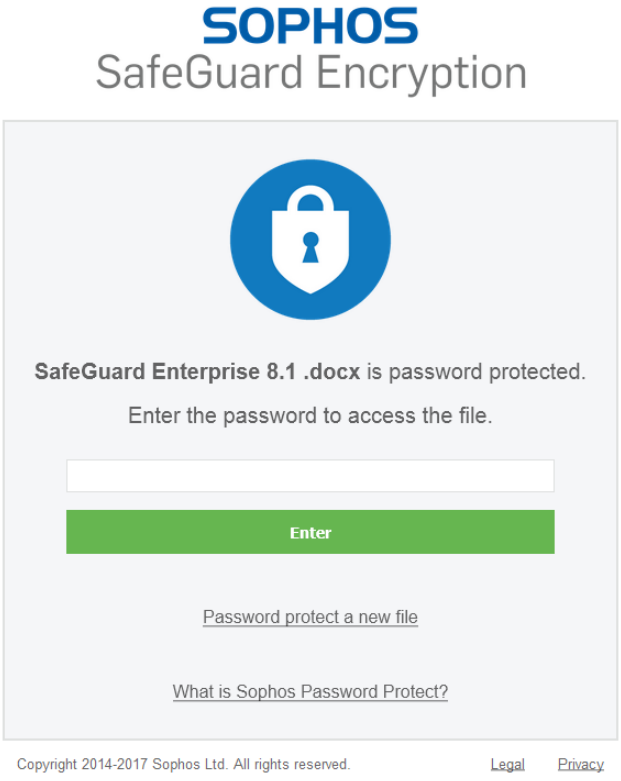
   Note
   - You need free disk space for the encryption.
   - The encrypted HTML file is bigger than the original file.
   - The maximum supported file size is 50 MB.
   - To send several files at once, you can compress them into a .zip file and then encrypt the .zip file.

4. 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
5. 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.

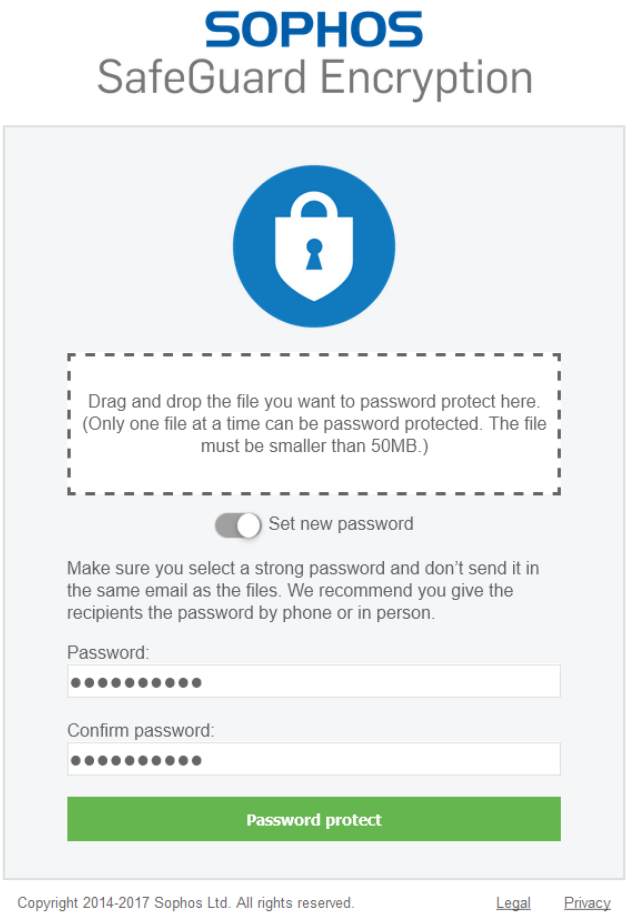
Recipients can access a file you protected with a password. They can protect the file with a password when sending it back to you. They may use the same password or a new password. They can even protect a new file with a password.

4.2 Protecting a new file with a password

With SafeGuard Enterprise 8.1, recipients of a password protected file can encrypt a new file with a password. They don't have to decrypt the original file first. This saves time and works even without entering the original password first.



Users just have to double-click on an encrypted HTML file and then click **Password protect a new file**.



Users need to drag and drop a file to the marked area, enter a strong password, and click **Password protect**.

5 Synchronized Encryption

Synchronized Encryption is the application-based file encryption module of Sophos SafeGuard Enterprise. The differences compared to location-based file encryption are:

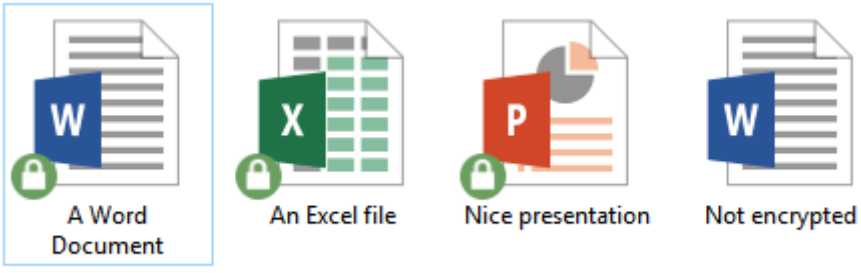
- Automatic encryption of files created or edited by defined applications (In-Apps).
- Only defined applications can read files.
- Encryption does not depend on the location of the file.
- Encryption keys can be automatically removed from the users' devices if a security threat is suspected.

Note
This feature is only available if you use web-based Sophos Central Endpoint Protection together with SafeGuard Enterprise. You need a SafeGuard Enterprise policy set to remove the encryption keys. The feature is available on Windows and macOS endpoints.

5.1 Working with standard applications

With Synchronized Encryption you can work as before and do not have to think about encryption. Only when sharing the information externally you may have to think about who the recipient is, and what the adequate security level is.

For example, you create content in Excel or PowerPoint as before. When you save the document it will be encrypted. Encrypted documents are marked by a little icon on top of the original file icon, showing a padlock.



5.2 Sharing information within the company

Using the SafeGuard Enterprise **Synchronized Encryption Key** makes it easy to share information internally. Every SafeGuard Enterprise user within your company will be able to read the information.

This version of SafeGuard Enterprise (SGN 8.1) allows you to configure additional encryption keys for specific locations. To be able to read files encrypted with a different key than the Synchronized Encryption key users must have this key in their key ring, see Best Practice: multi-key support for Synchronized Encryption (page 2).

Note
Users can display their key ring by right-clicking the SafeGuard Enterprise system tray icon on the Windows taskbar and then clicking on **Display > Key Ring**.

You can share encrypted documents in the usual way: send them by email, put them on a network share, or copy them to a removable storage device.

You need to install the Synchronized Encryption module on the computers of all users who need to access information shared in the company.

Note
Make sure you install SafeGuard Enterprise for both Windows and macOS users.

5.3 Sharing information with external parties

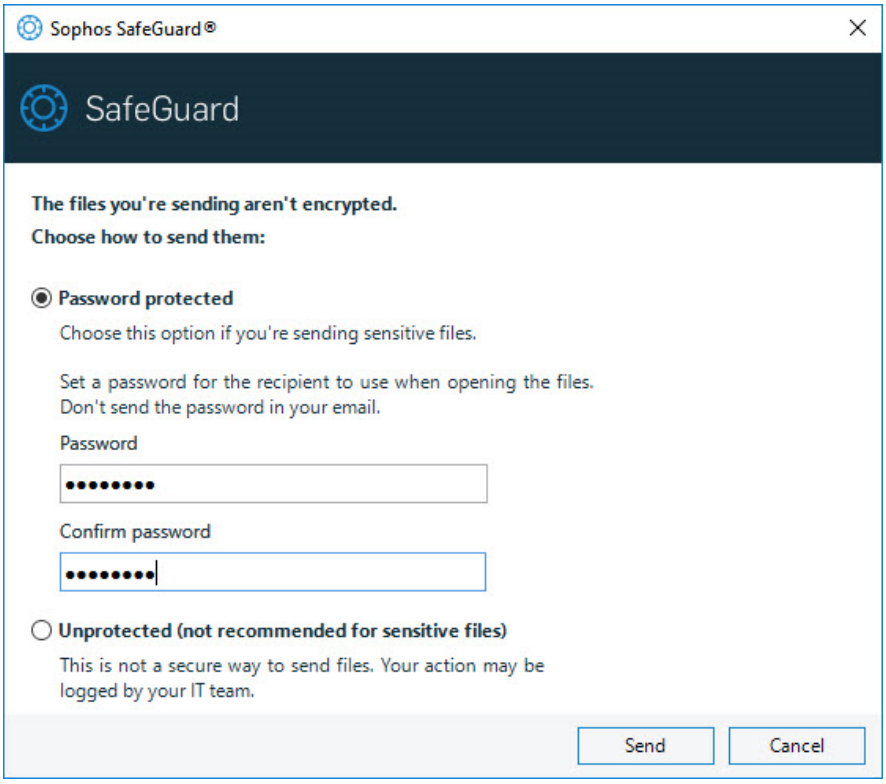
The reason for encrypting information is to restrict access to sensitive data. A document with financial information or the latest intellectual property is not something you want to make widely available. However, there are cases where you want to share this information with the outside world. Sometimes you would want this to be still encrypted, other times you may decide this information is no longer confidential.

Different workflows apply to Outlook users and other users.

Tip
Make the SafeGuard Enterprise user help available to your users.

Outlook users

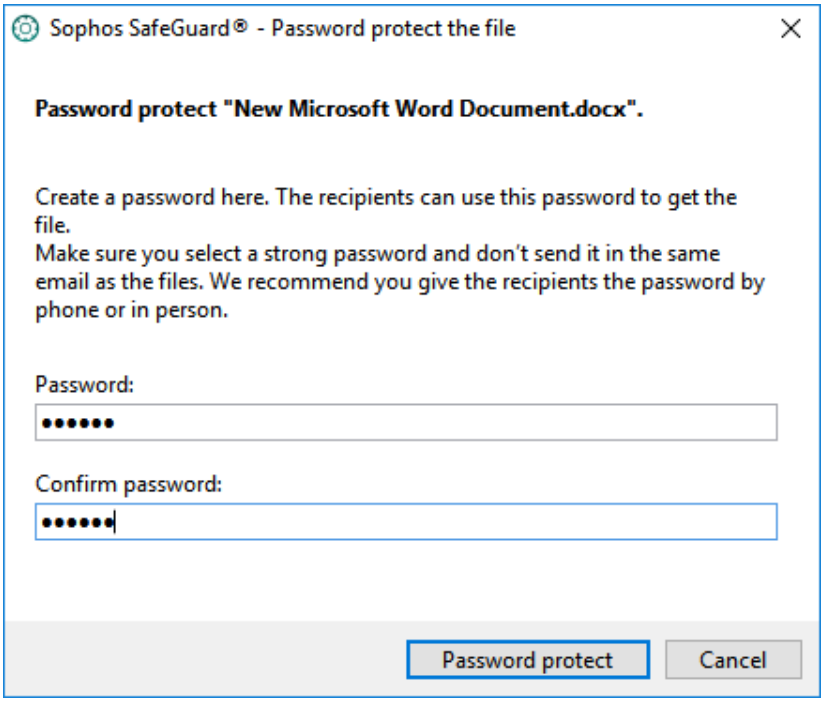
For Windows machines with Microsoft Outlook (32-bit version of Office only), users do not have to think about encryption. You can configure Synchronized Encryption so that a message pops up, asking what to do with the file, when users send an email with at least one external recipient and one file attached.



Other users

Windows and Mac users can decrypt files to send them unencrypted or create a password protected file before sharing it.

They can right-click a file, select **SafeGuard File Encryption**, and then **Decrypt selected file**. Or they can right-click the file, click **SafeGuard File Encryption**, and choose **Create password protected file**. In this case a new file is created with the extension HTML and the recipient can access it with the password the user has defined.



For detailed information, see the SafeGuard Enterprise user help, Send encrypted files via email.

5.4 Specifying In-Apps

In-Apps are applications that can create and access encrypted content. Such applications are defined by a SafeGuard Enterprise security officer using full paths, both on Windows and on macOS.

Tip
Make sure all machines have the applications installed in the same location, or include all different possible installation paths in the definition of the In-Apps.

5.4.1 What should I define as In-App?

In-Apps are the only applications that can create and read encrypted content. You need to include all applications you intend to use for either creating or reading encrypted content.

For content creating applications this typically includes:

- Office suites (Microsoft Office, OpenOffice, FreeOffice, ...)
- Design suites (Adobe Creative Suite, ...)

Reading applications can include:

- Office viewers
- PDF viewers
- Image viewers

Note
You cannot add Windows Store apps to the In-Apps list.

Tip
Consider all file types that can be used by content creating software. For example, for Microsoft Word, you need to include .docx as well as .rtf, .odt, etc.

In some cases, you will be adding applications that are used by certain end users only. This does not mean you have to apply the policy only to those people; if users receive a policy for the application they don't have, that part of the policy will be ignored.

5.4.2 What should I never define as In-App?

As the purpose of encryption is preventing information from leaking to the outside world, the applications that can be used for sending out information should never be defined as an In-App. Otherwise, all content will be decrypted before sending and there would be no protection of the data.

Never define applications such as email clients, internet browsers, backup software, etc. as In-Apps.

Note
For macOS, it may be useful to include mail programs, because there is no Outlook Add-in available.

5.5 Issues to be considered before deployment

Consider deploying Synchronized Encryption to a limited set of people (test group) only. Give all others a policy that does not encrypt, but provides the encryption key, so that they can read the encrypted files created by their colleagues, see Creating read-only policies (page 16).

You may want to consider some of the following issues before deploying Synchronized Encryption.

5.5.1 Opening files created with a particular app in a different app

Several applications can create files in different formats. For example, Microsoft Word can easily create PDF files. When Microsoft Word is defined as an encrypting application (In-App), those resulting PDF files will be encrypted. This is expected behavior as that content may be sensitive.

However, this means that you will need to think about the application used to open and read that file. In our example, this will be a PDF reader, and even though PDF readers are not usually used for creating files, they will need to be defined as In-Apps as well. Otherwise, you won't be able to read the files in PDF readers. For this reason, we already included the most common PDF readers in the application list template that is provided with the SafeGuard Management Center.

Other examples may be:

- In-Apps that export graphics
- In-Apps that export files in different text formats such as .txt, .rtf, .csv and so on.

Tip
Consider default readers for all file types you can create with the defined In-Apps. Make sure those readers are installed on all machines, and make them In-Apps as well so that the encrypted content can be read.

Windows 10 PDF

The default PDF reader for Windows 10 is the new internet browser Edge. You could make Edge an In-App, but this would mean that when you upload files to the internet using Edge, they would be decrypted and uploaded as plaintext.

Important
Deploy Windows 10 machines with a PDF reader other than the default built-in reader Edge, for example Adobe Acrobat Reader or Foxit Reader.

5.5.2 Java applications

Java applications often share the same `java.exe` as executable. Therefore, it is not possible to distinguish between different Java applications through the path to the `java.exe`. If you define `java.exe` as an In-App, consider that all applications that use this executable will create and can access encrypted content.

5.5.3 Web based applications

Groups of people often work with documents that need to be uploaded to a web based application. Encrypted files will stay encrypted so the underlying system will not be able to read them. This means:

- It is impossible to index these files based on content
- When these files have to be accessed externally they will be unreadable.

You may need to have external access to these files. Users can decrypt files before uploading. Alternatively you can create a folder where the files can be saved without encryption.

This exception folder should be used for that purpose only. This should be communicated clearly to the users.

Tip
Create an exception for encrypted files, either by a full path, such as `c:\unencrypted`, or create a relative path (only available on Windows clients). If you use a relative path, users only have to create a folder with an agreed name. If the name of the folder is for example `\unencrypted`, files and sub-folders in every `\unencrypted` folder on the computer, regardless of its location will not be encrypted.

5.5.4 Exchanging information with platforms that don't have SafeGuard encryption

Sometimes users create files for use in another environment. For example files created on a Windows or a macOS workstation are used in a Terminal Server environment. As SafeGuard Enterprise is not supported in Terminal Server environments, these files will stay encrypted and cannot be read by any application there.

The solution here, too, is to create an excluded path in the encryption policy for such locations.

5.5.5 What happens to my previews?

File browsers (Windows Explorer or Finder) can show previews of the different file types such as images, text documents, spreadsheets, PDF files, etc. These previews are typically built when the file is stored or changed. To do so, the application that creates these previews needs to have access to the unencrypted content of the file. So you would have to add it to the list of In-Apps. For macOS this is possible (and done by default) as this is a separate application.

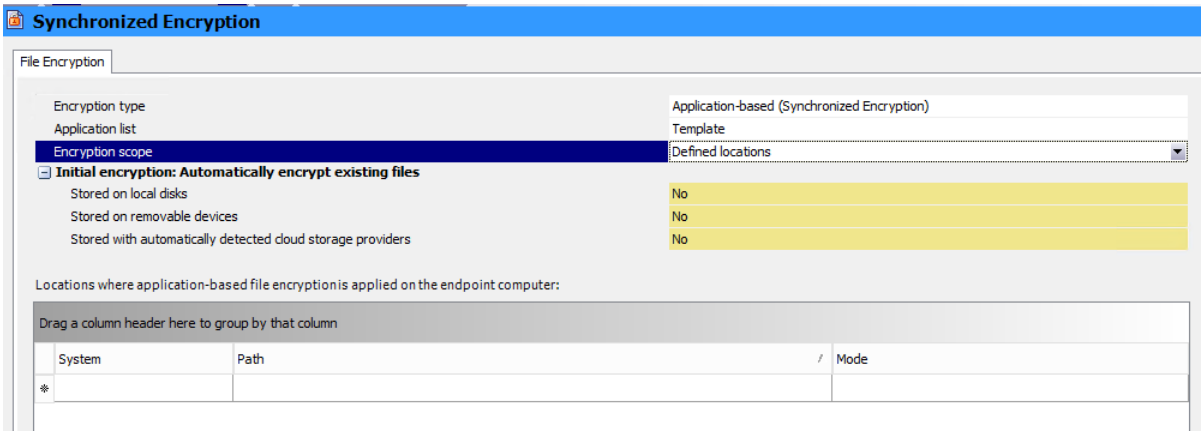
5.6 Creating read-only policies

When you start the deployment of Synchronized Encryption, users should be able to read encrypted documents but not encrypt them. You can then start turning on encryption for dedicated groups, and eventually for everybody.

This first policy is a read-only policy.

Windows

For Windows users this means that you create a Synchronized Encryption policy including all your applications and specify **Defined locations** as the **Encryption scope** but not define locations.



For detailed information, see the SafeGuard Enterprise administrator help, Create read-only policy for Windows endpoints

macOS

Macs behave differently to Windows. On macOS computers, reading encrypted files only works in defined locations.

This means that the read-only policy for Windows users cannot be used for Macs.

For Macs you have to create a policy of type **File Encryption** and select **Location-based** as the encryption type. You need to add at least one location, **exclude** it from encryption and communicate the location to your Mac users. This can for example be `<Documents>/Encrypted`. Users who want to read an encrypted document should then move or copy the file to that location first.

For detailed information, see the SafeGuard Enterprise administrator help, Create read-only policy for Mac endpoints.

5.7 Informing the end users

In many cases encryption is going to be new to the end users. We recommend that you tell your users about your encryption procedure and rules. Especially with synchronized encryption it is important that users know what to expect. For example: which applications are defined as In-Apps?

Knowing this means that a user can immediately spot a missing key application and give feedback to the SafeGuard Enterprise security officer. They can then add that application to the list of In-Apps.

Recommended process:

- Send an email to all users briefly explaining the implemented encryption rules and consequences. Ideally refer to an internal website that you can easily modify, for example when new In-Apps have been added.
- Include a feedback email address in the mail.
- If you have already rolled out SafeGuard Enterprise on all endpoints (for example in read-only mode), you can include a document that has been encrypted with the Synchronized Encryption key, and ask users to verify that they can read it. If not, you know there is a problem with the installation or communication between the endpoint and the SafeGuard Enterprise backend before you enable the encryption for everyone.

5.7.1 Sample communication

This is a sample email you may want to use to inform your users. It contains the most important information, but there may be other items you may wish to add, for instance, when you have created an exception rule for all folders named “unencrypted”, or when you’re using other applications. This sample mail assumes it comes with an attachment of a document that has been encrypted using the Synchronized Encryption key.

= =

To All,

IT has finished rolling out SafeGuard Enterprise to everybody. This is an encryption product by Sophos that will be used by everybody to protect our documents. In general, this will not interfere with your daily work, but there are some exceptions we want to bring to your attention.

We will be enabling Synchronized Encryption for all employees next week. Once enabled, you will be creating encrypted files on your computer. We have gathered some getting started material on our intranet – just go to the intranet home page and click encryption, or go to https://company.internal/encryption.

To check the readiness of your system, please open the attached file.

- **Windows and macOS:** If you can open the document and read the message then you’re all set! If you are not able to see the message within the file correctly, please contact IT Service Desk to get help.
- **iOS and Android:** Open the attachment in the Sophos Secure Workspace application on your device. The native viewer will not be able to open the file as it is encrypted. If you don’t have Sophos Secure Workspace on your mobile device, please contact the IT Service Desk for assistance.

Applications to use

The following applications will automatically create encrypted content on your computer. If you use different applications to access encrypted files, you will only see the encrypted content.

Windows:

- Adobe Reader
- MS Office 2010 (Excel, PowerPoint, Word)
- MS Office 2013 (Excel, PowerPoint, Word)
- MS Office 2016 (Excel, PowerPoint, Word)

- Office Viewers
- Foxit Reader for PDF

macOS:

- Adobe Reader
- Apple Productivity (Keynote, Numbers, Pages, Preview)
- MS Office 2011 (Excel, PowerPoint, Word)
- MS Office 2016 (Excel, PowerPoint, Word)

What about sending files?

When sending an email to an external recipient, note that the file will be sent encrypted. That means your recipient will not be able to read the content. You may want to decrypt the file before sending if the content is not confidential. If it is confidential, or when in doubt, create a password encrypted file. Right-click the file and select "SafeGuard File Encryption". Then either select “Decrypt selected file” or “Create password protected file”.

If you are using **Windows** and are sending the file by **Microsoft Outlook**, you don’t have to do this manually. When the system detects you are sending an encrypted file to an external correspondent it will ask you what you want to do with the file.

And what about uploading files to our web applications?

Whenever you upload encrypted files, they will not be decrypted. This means that they remain encrypted in SharePoint or any other web application you are using. You may want to manually decrypt files first. Note that you won’t be able to see previews, and that indexing of files will not work either.

Problems? Suggestions?

If you have a problem with SafeGuard Enterprise or your computer in general after encryption is enabled, please raise an IT ticket at the IT Service Desk.

Regards,

6 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.

7 Legal notices