SOPHOS

Security made simple.

SafeGuard Enterprise quick start and best practice guide

Product version: 8

Document date: July 2016

Contents

1 About this guide

This guide contains two parts:

- Introducing Synchronized Encryption (page 4) helps you get started with the new Synchronized Encryption module.

  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.

- Best practices and recommendations (page 13) provides tips and recommendations for a smooth rollout, administration and use of SafeGuard Enterprise.

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

2 Introducing Synchronized Encryption

Synchronized Encryption is the new file encryption module of Sophos SafeGuard Enterprise. The key changes compared with file encryption in previous versions of SafeGuard Enterprise are:

- Automatic encryption of files created or edited by defined applications (In-Apps).
- Only defined applications can decrypt files.
- Encryption does not depend on the location of the file.
- Encryption keys can be exchanged with mobile devices running iOS or Android.

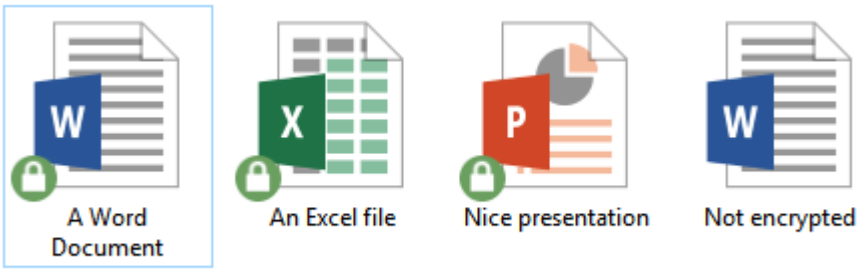
  Note: You must set the Sophos Mobile Control environment to communicate with SafeGuard Enterprise.
- Encryption keys can be automatically removed from the users' devices if a security threat is suspected.

  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 Mac OS X endpoints.
- Users can retrieve the recovery key for their volume-based encryption (BitLocker Drive Encryption on Windows machines or FileVault2 on Mac OS X machines) via their mobile device.

2.1 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.



2.2 Sharing information within the company

There is only one encryption key that is used in this version of SafeGuard Enterprise (SGN 8). This makes it easy to share information internally. Every SafeGuard Enterprise user will be able to read the information.

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 Mac OS X users.

2.3 Sharing information with external parties

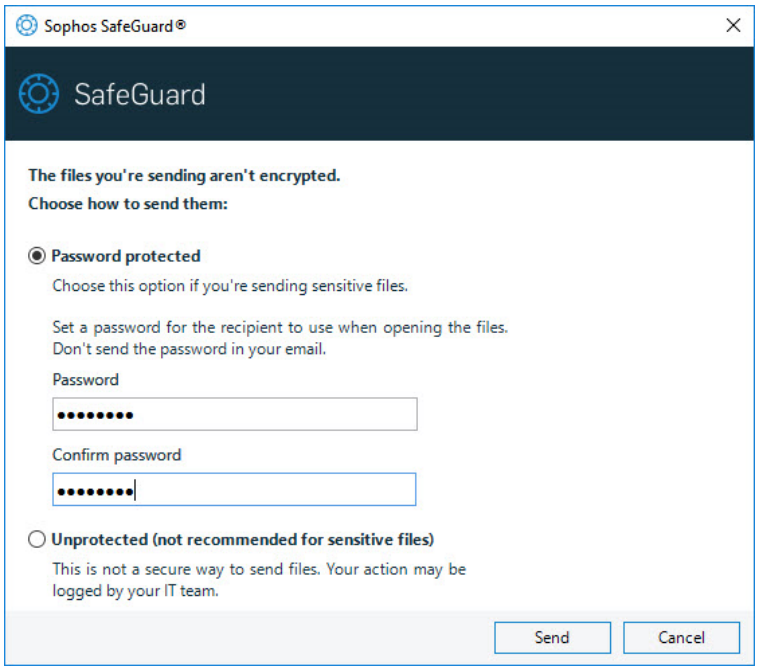
The reason for encrypting information is to restrict access to sensitive data. A document with financial information or the latest intellectual property is not something you want to make widely available. However, there are cases where you want to share this information with the outside world. Sometimes 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

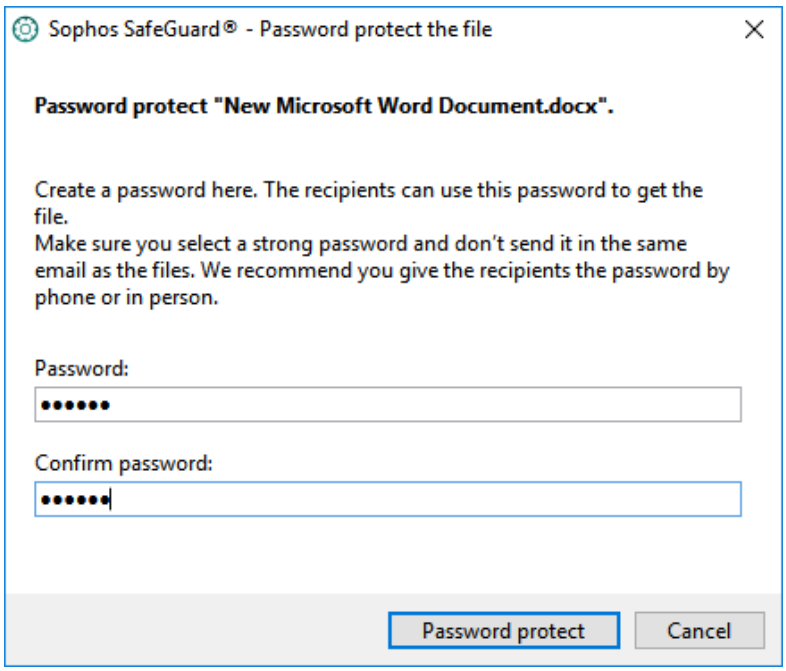
For Windows machines with Microsoft Outlook (32-bit version of Office only), users do not have to think about encryption. You can configure Synchronized Encryption so that a message pops up, asking what to do with the file, when users send an email with at least one external recipient and one file attached.



Other users

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

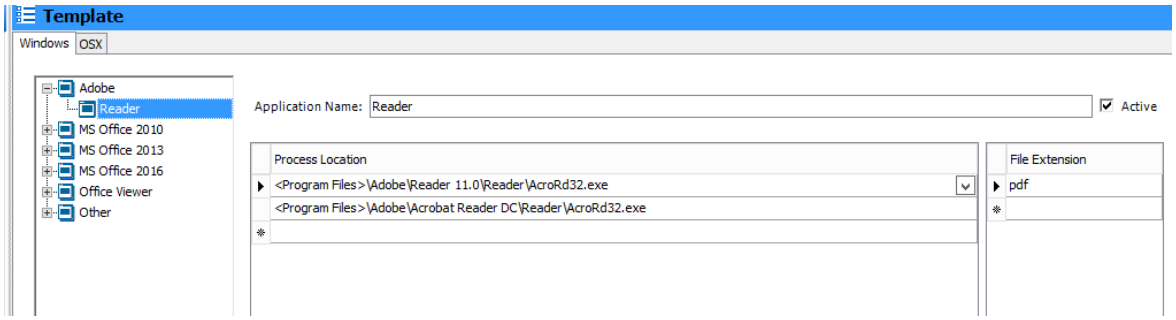
They can right-click a file, select **SafeGuard File Encryption**, and then **Decrypt selected file**. Or they can right-click the file, click **SafeGuard File Encryption**, and choose **Create password protected file**. In this case a new file is created with the extension HTML and the recipient can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

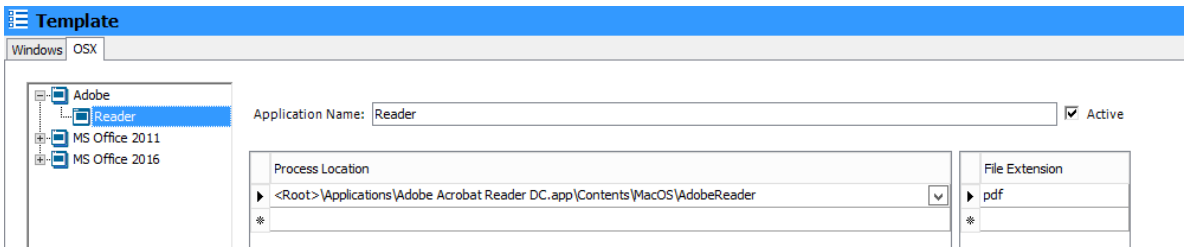


For detailed information, see the SafeGuard Enterprise user help, Securely sending email attachments.

2.4 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 Mac OS X.





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.

2.4.1 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, and also .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.

2.4.2 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 Mac OS X, it may be useful to include mail programs, because there is no Outlook add-in available, see Policies for Mac OS X endpoints (page 16).

2.5 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 10).

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

2.5.1 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 8 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 they can read the encrypted content.

2.5.1.1 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.

2.5.2 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.

2.5.3 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 upon 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.

2.5.4 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 Mac OS X 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.

2.5.5 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 Mac OS X this is possible (and done by default) as this is a separate application.

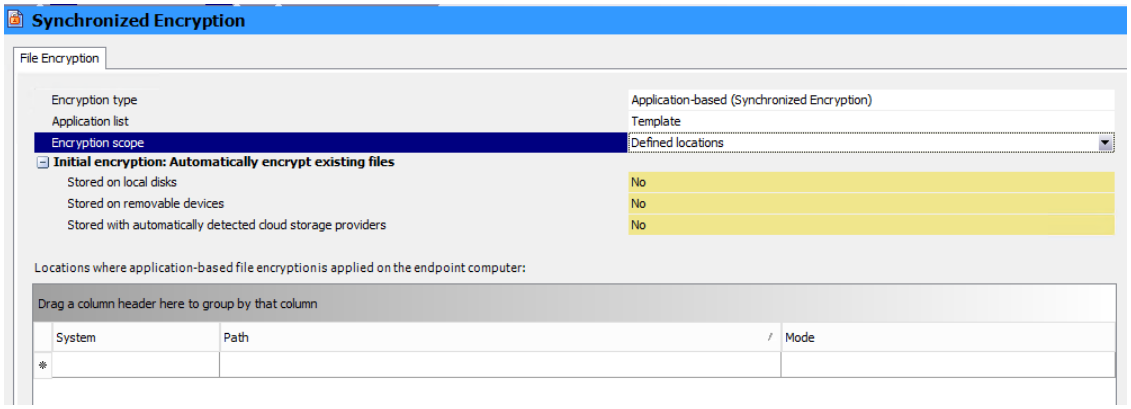
2.6 Creating read-only policies

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

Mac OS X

Mac OS X behaves differently to Windows. On Mac OS X computers, reading encrypted files only works in defined locations.

This means that the read-only policy for Windows users cannot be used for Mac OS X users.

For Mac OS X 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 OS X 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.

2.7 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.

2.7.1 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 device. 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 Mac OS X:** 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 device. 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

Mac OS X:

- 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,

3 Best practices and recommendations

3.1 Rollout

Note: SafeGuard Enterprise Server and SafeGuard Management Center require .NET 4.5.

General suggestions

- Try to avoid a mixed rollout of the new Synchronized Encryption and the legacy File Encryption modules of SafeGuard Enterprise.
- A gradual rollout plan requires a test-run or verification of each step, especially for complex nested AD group memberships.
- User training is the key to a smooth rollout and operation.
- Clear communication about who is participating and the consequences is essential.
- IT and support teams have to be staffed adequately.

Prerequisites

- All endpoints should have installed SafeGuard Enterprise 8. Otherwise sharing of encrypted files will be not transparent and the usual workflow is affected.
- If you want to read encrypted files on mobile devices (a new feature of SafeGuard Enterprise 8), you have to roll out the Sophos Secure Workspace app as well.

  Note: To read encrypted files on mobile devices you have to use Sophos Secure Workspace managed by Sophos Mobile Control.
- Make sure that travelling users connect to the SafeGuard Enterprise backend regularly via VPN or "Direct Access" (Windows) to make sure that latest encryption policies are applied.

3.1.1 Prepare endpoints for Synchronized Encryption

For the Synchronized Encryption module to work properly, the Microsoft runtime **`vstor-redist.exe`** must be installed. The file installs Microsoft Visual Studio 2010 Tools for Office Runtime and is included in the installation package.

We recommend installing the components in the following order:

1. **`vstor-redist.exe`**
2. **`SGNClient.msi`**
3. configuration package

Note: You cannot deploy the configuration package before the installation of **`vstor-redist.exe`** is finished.

3.1.2 Partial rollout

In many situations the new **Synchronized Encryption** module cannot be rolled out and activated for all employees in one step within a short period of time. In these cases it is important to give users read-access to encrypted files even if they are on SafeGuard Enterprise endpoints without activated **Synchronized Encryption**. Therefore, a read-only policy is required.

For giving users read access, you need the following:

- The **Synchronized Encryption** key.

  It is assigned to the root node in the Management Center by default and all employees of a company should get this key automatically.

- An **Application list** and a specific read-only policy.

  For detailed information on partial rollout of Synchronized Encryption, see the SafeGuard Enterprise administrator help, Partial rollout of Synchronized Encryption.

3.1.3 Synchronized Encryption and SafeGuard Enterprise File Encryption in the same environment

Note: If your environment requires you to use both, Synchronized Encryption and File Encryption, consider the following to achieve a smooth integration.

Synchronized Encryption supports one encryption key for an entire company. This makes administration and rollout easy. For some departments like HR or Finance, there might be the need to have a cryptographic separation from other departments to make their documents accessible only within their department.

For this scenario the SafeGuard Enterprise File Encryption modules (File Share, Cloud Storage, Data Exchange) have to be used. These modules allow using different keys for file encryption. You cannot install the Synchronized Encryption module and the SafeGuard Enterprise File Encryption module on the same machine.

To make use of Synchronized Encryption and the SafeGuard Enterprise File Encryption modules some extra administration tasks are necessary:

1. The rollout of SafeGuard Enterprise must consider that different modules have to be installed for some departments.
2. Departments with special requirements have to get other policies than those assigned on **Synchronized Encryption** endpoints. To make this possible the imported AD structure should allow an easy assignment of these policies to users and machines concerned.
3. The rollout/installation of the SafeGuard Enterprise modules must be carried out according to the policies assigned: the right machines must get the right policies.

   Note: The Outlook add-in is not available for SafeGuard Enterprise File Encryption modules. Therefore Synchronized Encryption and File Encryption endpoints cannot share encrypted attachments transparently.

Recommendations

- Users of SafeGuard Enterprise File Encryption modules need to get the **Synchronized Encryption** key. Users can then read files encrypted with the **Synchronized Encryption** key, transparently.
- Sharing encrypted files:

  For users of SafeGuard Enterprise File Encryption modules, we recommend creating a policy which defines the **Synchronized Encryption** key to be used for a "transfer" share. All files created in or moved to this share will be encrypted with the **Synchronized Encryption** key. **Synchronized Encryption** users are able to read these files.

- Sharing plain files:

  For users of SafeGuard Enterprise File Encryption modules, a policy that excludes a folder from encryption can be used (**Encryption type**: **Location-based**, **Mode**: **Exclude**).

- When users of SafeGuard Enterprise File Encryption modules want to share files with **Synchronized Encryption** users, they need to decrypt the files first. They can then decide to either send the unencrypted files or encrypt them with the Synchronized Encryption key.

3.1.4 Check validity of user certificates

Checking the validity of the user certificates is especially important for companies that used SafeGuard Enterprise BitLocker management only and want to add **Synchronized Encryption**.

You can check the certificates in the SafeGuard Management Center under **Keys and Certificates** > **Certificates** > **Assigned Certificates**.

Expired certificates or certificates that will expire soon are marked red in the **Expires** column. To renew a certificate that will expire soon activate the check-box in the **Renew** column. Users with already expired certificates have to get new ones. You must delete the expired certificates, then the affected users will get new ones automatically the next time they log on to SafeGuard Enterprise.

SafeGuard Enterprise provides the database script **`UserCertficateRenewal.vbs`** to automate these tasks. The script can be used in the SafeGuard Enterprise or Windows **Task Scheduler** to perform these checks regularly and renew certificates if necessary, see Sophos knowledgebase article 118878.

3.1.5 Check if all users are confirmed

In SafeGuard Enterprise new users have to be confirmed in the SafeGuard Management Center or authenticated against Active Directory. Most users will be Active Directory users, who will be confirmed automatically. However, some users have to be confirmed manually, for example local users. Unconfirmed users will not become **SGN Users** and therefore will not get encryption keys for Synchronized Encryption. This is true for Windows and Mac OS X endpoints.

We recommend setting the first policy to be rolled out to **read-only**. After all endpoints/users have received their keys activate the encryption policies. This way you can make sure that all users are confirmed before they receive their encryption policies. Issues with unconfirmed users will be avoided.

3.1.6 Policies for Mac OS X endpoints

For file encryption we recommend using the policy type **Application-based (Synchronized Encryption)** with **Encryption scope** set to **Defined locations** and start with only a few locations where files are encrypted automatically. This way you can reduce the impact on users and their usual workflows.

To be able to distinguish between Windows and Mac OS X endpoints in terms of policy management, use a separate AD or SafeGuard Enterprise group for Mac OS X users and machines. Activate the Mac OS X policy only for Mac OS X users and machines.

3.1.6.1 Suggestions for a Mac OS X Synchronized Encryption policy

In-Apps

Applications that will encrypt their data, to be added to the **Application list**:

- Email

  Note: For Mac OS X, there is no Outlook add-in available. However, you can add Outlook and Apple Mail to the application list to make sure that no encrypted data is sent unintentionally to users who cannot access it. Note that the mail apps you included in the list will send all attachments unencrypted and will save encrypted attachments in encrypted form and plain files in plain text.

  - /Applications/Microsoft Outlook.app/Contents/MacOS/Microsoft Outlook
  - /Applications/Microsoft Office 2011/Microsoft Outlook.app/Contents/MacOS/Microsoft Outlook
  - Applications/Mail.app/Contents/MacOS/Mail

- To enable Mac OS X preview and the preview functionality in Finder and Apple Mail, the following processes need to be added:
  - /Applications/Preview.app/Contents/MacOS/Preview
  - /System/Library/Frameworks/QuickLook.framework/Versions/A/Resources/quicklookd.app/Contents/XPCServices/QuickLookSatellite.xpc/Contents/MacOS/QuickLookSatellite
  - /System/Library/Frameworks/Quartz.framework/Versions/A/Frameworks/QuickLookUI.framework/Versions/A/Resources/QuickLookUIHelper.app/Contents/MacOS/QuickLookUIHelper
  - /System/Library/Frameworks/QuickLook.framework/Versions/A/Resources/quicklookd.app/Contents/MacOS/quicklookd

Paths for Encryption scope: Defined locations

- Encrypt:
  - <Documents>\Encrypted
- If you want users to be able to double-click encrypted documents in their mail clients to open them, you need to add these applications (for example Mail) to the In-App list, and their temporary folders to the list of defined locations.

  The locations you need to define for the mail clients on Mac are:
  - <%TMPDIR%>\com.apple.mail\com.apple.mail
  - <User Profile>\Library\Containers\com.apple.mail\Data\Library\Mail Downloads

  Add the following locations for Outlook for Mac OS X:
  - <User Profile>\Library\Caches\TemporaryItems\Outlook Temp\
  - <%TMPDIR%>com.microsoft.Outlook\Outlook Temp\

3.2 Backend

3.2.1 Read-only user for Active Directory synchronization

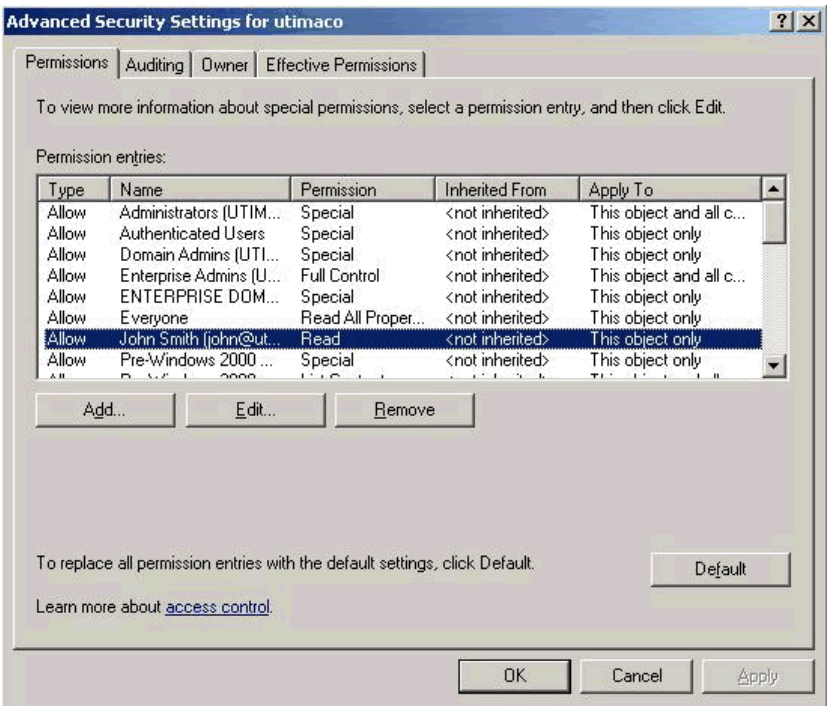
Note: To increase security of the connection, we recommend that you use SSL encryption for the Active Directory synchronization.

The account used for the import and synchronization of the Active Directory should be a **read-only** user. The user needs read access to the domain and all child objects.

To assign the rights:

1. Open the **Active Directory Users and Computers** management window and go to **Advanced Features**.
2. Right-click the domain and then click **Properties**.
3. Add a user (or a group) and select the **Allow** checkbox to assign **Read** permission.
4. Click **Advanced**, select the user (or group) and click **Edit**.
5. In the **Permission Entry for <domain>** dialog, select **This object and all child objects** from the **Apply onto:** drop-down list.

   The result should look like this:



3.2.2 Users displayed with "#" in the Management Center

Users that registered in SafeGuard Enterprise when no domain controller was available are marked with "#" in the Management Center.

3.3 Policies

3.3.1 Folders to be excluded from encryption

Make sure to exclude the following paths from encryption when you use **Synchronized Encryption**:

Windows

- **`<Local Application Data\Temp>`**

  Reason: Some applications create many small temporary files. If not excluded, all temporary files will be encrypted according to the policy. Exclude the folder to avoid performance issues.

- **`<Local Application Data>\Microsoft and subdirs`**

  Reason: Some applications call other applications (for example embedded video in Microsoft PowerPoint). If the calling application is an application that encrypts files, the temporary file (for example video) will be encrypted. If the called application (for example browser) is an application that does not encrypt files (it is not on the Application list) it cannot run the encrypted file.

- **<Program Files>**

  Reason: Access to this folder needs administrator rights. SafeGuard Initial Encryption cannot encrypt these files because of the missing access rights. Excluding this folder prevents the SafeGuard database from being cluttered with event messages caused by failed file encryption.

All systems

- **<!cloud storage providers!>**

  In general we recommend to encrypt cloud storage, but you can exclude certain cloud storage providers which are used to share data with external parties. This prevents files in known local cloud storage synchronization folders from being encrypted. Thus, problems when exchanging files with external parties via Cloud synchronization can be avoided. It is not necessary to exclude these folders if you do not use Cloud folders for exchanging files with external parties.

- **<Music>**, **<Pictures>**

  Reason: Usually, you do not need to encrypt these files. If you do not want these folders to be excluded from encryption, applications to open these files need to be part of the **Application List**.

  Note: On Mac OS X you cannot use the Photos application and pictures library when you encrypt files in **<Pictures>**.

- **<User Profile>\AppData\Roaming\AppleComputer**

  Reason: This is the local synchronization folder for Apple iCloud on Windows endpoints. It should be excluded for the same reasons that apply to **<!cloud storage providers!>**.

3.3.2 Recommendations for policy settings

Define an "Unencrypted" folder

This folder can be used for sharing plain files, for example with Linux endpoints in the company or in a partial rollout scenario, see Create policies for application-based file encryption.

- **Windows**

  To exclude the "Unencrypted" folder from encryption on all endpoints, you have to add the **Unencrypted** folder (relative path) as exemption in a policy with **Encryption scope** set to **Everywhere**. If you do so, all files in folders with this name, regardless of where the folder is located, will not be encrypted.

- **Mac OS X**

  Relative paths are not supported on Mac OS X. We recommend that you define **<Documents>\Unencrypted** as exemption in a policy with **Encryption scope** set to **Everywhere**.

Outlook add-in

We recommend setting the **Encryption method for white-listed domains** option in a policy of type **General Settings** to **Unchanged**.

Remove keys on compromised machines

SafeGuard Enterprise **Synchronized Encryption** endpoints are informed by Sophos Central Endpoint Protection about compromised machine status.

We recommend that the **Remove keys on compromised machines** option is set to **No**. You should check the feedback about affected endpoints under **Reports** in the SafeGuard Management Center for Red health state detections. Next you should check and clean up the endpoints, if necessary. Finally you should set the **Remove keys on compromised machines** option to **Yes**.

3.3.3 Guest user

On endpoints that have only SafeGuard Enterprise BitLocker management installed, companies may still have the **Allow registration of new SGN users for** option set to **Owner**.

For endpoints without SafeGuard Enterprise POA that have BitLocker management or file encryption modules installed, the **Allow registration of new SGN users for** option must be set to **Everybody**. If you do not set this option to **Everybody**, further users will only have **SGN guest** status. They will not get certificates and cannot encrypt files after a file encryption module like **Synchronized Encryption** has been installed.

3.3.4 Policies for Mac OSX and RSOP

On Mac OSX only policies assigned to users are evaluated. If you assign them to machines, Mac OS X endpoints will not get any policies.

However, the RSOP in the Management Center displays the policy currently assigned to the Mac although it will not become active.

3.3.5 File tracking

Note that the file tracking functionality of SafeGuard Enterprise is subject to national laws. You should check what you are legally permitted to track.

3.3.6 Reminder to change password

If you use the SafeGuard Enterprise Credential Provider the Windows pop-up dialog that informs users when their password will expire is no longer displayed.

To remind users to change their passwords, you need to create and assign a SafeGuard Enterprise policy of type **Password** with the required settings, see Syntax rules for passwords.

3.4 Endpoints - all platforms

3.4.1 Endpoint does not return to healthy state - cleanup fails

Next-Generation Data Protection ensures that Sophos SafeGuard communicates with Sophos Endpoint Protection, if available. This is an extension of the Synchronized Security message. SafeGuard and Endpoint will share the health status of a system using the heartbeat between them.

If a system becomes highly infected with malware it will be locked down to protect sensitive files.

In the event this occurs, users will be advised by Sophos Endpoint Protection that they now have an unhealthy system with a Red health state. Additionally, they will be advised by Sophos SafeGuard that they will no longer be able to access any encrypted files. They will remain in this state, unable to access encrypted files, until the health of the system is returned to a healthy (Green) state. When the system returns to a healthy state, Sophos SafeGuard will synchronize with the backend and allow users to once again access encrypted files.

If users receive these notifications and their system does not return to a healthy state in a short period of time, they should contact IT for help.

If an endpoint is unable to return to a healthy state, it means Sophos Anti-Virus cleanup has failed (cleanup is set to automatic in Sophos Central). If cleanup fails, then additional actions are required by IT to clean up the malware, see https://www.sophos.com/en-us/support/knowledgebase/112129.aspx.

3.5 Windows endpoints

3.5.1 Encrypt/Decrypt files manually

Synchronized 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**: Encrypts your file with the Synchronized Encryption key provided that the file type is included in the application list and the location of the file has not been excluded from encryption.
- **Decrypt selected file** (only for encrypted files): 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 unencrypted files): Allows you to manually encrypt your file with the Synchronized Encryption key.
- **Create password protected file**: Here you can define a password to encrypt your file manually. This is useful if you want to securely share your file with someone who does not have the Synchronized Encryption key of your organization. Your file is encrypted and saved as an HTML file. Your recipients can open the file with their web browser as soon as you communicate the password to them.

Note: This option is only available for files that are either plaintext or encrypted with a key available in your keyring. If files are encrypted, they are first decrypted automatically before they are password protected.

Note: Password protection uses base64 encoding, therefore, files are bigger than the original file. The maximum supported file size is 50 MB.

Note: You can only password-protect single files, not folders or directories. However, you can select more than one file to show their encryption state and to encrypt/decrypt them.

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**: The system automatically detects all unencrypted files and encrypts them with the default Synchronized Encryption key provided that the file type is included in the application list and the location of the file has not been excluded from encryption. Depending on your policy, files encrypted with other keys may be re-encrypted with the Synchronized Encryption key, too.

3.5.2 Emails sent via auto-forward rule

When you define an auto-forward or redirect rule **on client side**, emails sent automatically are not logged.

3.6 Mac OS X endpoints

3.6.1 Position of icons on the desktop

When using SafeGuard Enterprise for Mac, the positions of the icons on your desktop may not be saved correctly. When you change the position of an icon, it will move back to its original position after every restart or logon.

To save your icons' positions, do the following:

1. Start the Terminal application on your Mac.
2. Enter the following command:

   ```
   defaults write com.sophos.encryption MountDesktopAsNetworkVolume 1
   ```

3. Log off and log back on to you Mac.

The system is now able to save the positions of your desktop icons.

Important: When you run this command, the functionality of the Trash changes. Deleting files will delete them permanently instead of moving them to the Trash. To remove the setting, enter the following command in the Terminal application:

`defaults remove com.sophos.encryption MountDesktopAsNetworkVolume`.

4 Technical support

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 knowledgebase 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.

5 Legal notices