SOPHOS

Security made simple.

Sophos SafeGuard File Encryption for Mac

Administrator help

Product version: 7

Document date: December 2014

Contents

1 About Sophos SafeGuard File Encryption for Mac

Sophos SafeGuard File Encryption for Mac extends the data protection offered by Sophos SafeGuard Enterprise from Windows to the Mac world. It offers file-based encryption on local drives, network shares, removable drives and in the cloud.

With SafeGuard File Encryption for Mac, you can safely encrypt and decrypt files and exchange these files with other users on Macs or Windows PCs.

To read files encrypted by SafeGuard Enterprise on mobile devices, use Sophos Mobile Encryption for iOS or Android.

In the SafeGuard Management Center, you define rules for file-based encryption in File Encryption policies. In these File Encryption policies, you specify the folders that are to be handled by File Encryption, the encryption mode and the key to be used for encryption. This central management guarantees that identical folders and encryption keys are processed on different platforms.

1.1 About this document

This document describes how to install, configure and manage Sophos SafeGuard File Encryption for Mac.

For detailed information on SafeGuard Management Center operation and policy settings, refer to the *SafeGuard Enterprise Administrator help*.

For user-relevant information refer to the *Quick Startup Guide for Sophos SafeGuard File Encryption for Mac*.

1.2 Terms and acronyms

The following terms and acronyms are used in this document:

Term or acronym	Meaning or explanation
FUSE	Filesystem in user space (see http://osxfuse.github.io/)
GUID	Globally Unique Identifier: a unique reference number used as an identifier in computer software.
Secured Folder	A Secured Folder is a folder for which a rule was created in the SafeGuard Management Center. The

Term or acronym	Meaning or explanation
	rule specifies that the contents of the folder will be encrypted.
SSL	Secure Sockets Layer: a cryptographic protocol that provides communication security over the internet.

2 Installation

The following chapter describes the installation of Sophos SafeGuard File Encryption on Mac OS X clients. For a description of how to install the administration environment (backend), refer to the *SafeGuard Enterprise Installation Guide*.

Two Mac OS X client installation types are possible:

- manual (attended) installation
- automated (unattended) installation.

Note: If you have installed SafeGuard Disk Encryption 6.01 or earlier you have to uninstall it before you can install SafeGuard File Encryption for Mac version 7.

If you want to use SafeGuard File Encryption and SafeGuard Native Device Encryption (called SafeGuard Disk Encryption up to version 6.10) both need to be version 7. Using different versions of these products on one Mac is not supported.

The installer package is signed, and OS X will try to validate this signature. If there is a slow internet connection or a misconfiguration you may have a delay of up to 20 minutes during the installation procedure.

2.1 Installation prerequisites

Before starting the installation, make sure the SafeGuard Enterprise-SSL server certificate has been imported into the system keychain and is set to **Always Trust** for SSL.

Note: It must not be stored in the login keychain.

1. Ask your SafeGuard Server Administrator to provide you with the certificate for SSL (file *<certificate name>.cer*).
2. Import the *<certificate name>.cer* file into your keychain. To do so, go to **Applications** - **Utilities** and double-click the **Keychain Access.app**.
3. In the left pane select **System**.
4. Open a Finder window and select the *<certificate name>.cer* file from above.
5. Drag the certificate file and drop it into the System Keychain Access window.
6. You will be prompted to enter your Mac OS X password.
7. After entering the password click **Modify Keychain** to confirm your action.
8. Then double-click the *<certificate name>.cer* file. Click on the arrow next to **Trust** to display the trust settings.
9. For **Secure Sockets Layer (SSL)** select the option **Always Trust**.
10. Close the dialog. You will be prompted again to enter your Mac OS X password.
11. Enter the password and confirm by clicking **Update Settings**. A blue plus symbol in the lower right corner of the certificate icon indicates that this certificate is marked as trusted for all users.

12. Open a web browser and check that your SafeGuard Enterprise Server is available using **`https://<servername>/SGNSRV`**.

Now you can start the installation.

Note:

Certificate import can also be done by running the command **`sudo /usr/bin/security add-trusted-cert -d -k /Library/Keychains/System.keychain -r trustAsRoot -p ssl "/<folder>/<certificate name>.cer"`**. This can also be used for automated deployment via script. Change folder and certificate names according to your settings.

Note:

If you want to bypass the process described above, you can run the command **`sudo sgfsadmin --disable-server-verify`**, see also Command line options (page 19). We do not recommend this option as it may create a security vulnerability.

2.2 Manual (attended) installation

A manual (or attended) installation allows you to control and test the installation while proceeding step by step. It is performed on a single Mac.

Note:

Make sure FUSE for OS X (OSXFUSE) version 2.7.0 or later is installed. For more information about FUSE for OS X and download options go to http://osxfuse.github.io/.

Make sure the server connection has been properly set up as described in Installation prerequisites (page 5).

1. Open *Sophos SafeGuard FE.dmg*.
2. After reading through the readme file offered, double-click *Sophos SafeGuard FE.pkg* and follow the installation wizard. You will be prompted for your password to allow the installation of new software. The product will be installed to the folder */Library/Sophos SafeGuard FS/*.
3. Click **Close** to complete the installation.
4. Open the **System Preferences** and click the Sophos Encryption icon to show the product settings.

5. Click the **Server** tab.
6. If server and certificate details are shown, skip the next steps and go to Step 11 and click **Synchronize**. If no information is shown, continue with the next step.
7. Select the configuration zip file (For a description of how to create a configuration package for Mac endpoints see *SafeGuard Enterprise Administrator Help*, *Working with configuration packages* > *Create configuration package for Macs*).
8. Drag the zip file to the **Server** dialog and drop it into the drop zone.
9. You will be prompted to enter a Mac administrator password. Enter the password and click **OK** to confirm.
10. Enter your Mac password to request your SafeGuard user certificate.

11. Check the connection to the SafeGuard Enterprise server: Company certificate details are shown in the lower part of the **Server** dialog. Then click **Synchronize**. A successful connection will result in an updated "Last Contacted" time stamp (Tab **Server**, **Server Info** area, **Last Contacted:**). An unsuccessful connection will display the following icon:

    

    Refer to the system log file for further information.

    Refer to Server tab (page 15) for more information on synchronization and server connection.

2.3 Automated (unattended) installation via remote management software

An automated (unattended) installation does not require any user interaction during the installation process.

This section describes the basic steps for an automated (unattended) installation of SafeGuard File Encryption for Mac. Depending on the management solution you are using, the actual steps may vary. Use your installed management software.

Note:

Install the packages in the correct order.

To install SafeGuard File Encryption for Mac on client computers, perform the following steps:

1. Download the installer file *Sophos SafeGuardFS.pkg*.
2. Copy the file to the target machines.
3. Install the file on the target machines. If you use Apple Remote Desktop, steps 2 and 3 are one single step.
4. Select the configuration zip file (see *SafeGuard Enterprise Administrator Help*, *Working with configuration packages* > *Create configuration package for Macs* for a description of how to create a configuration package for Macs) and copy it to the target machines.
5. Run the following command on the target machines:

    `/usr/bin/sgfsadmin --import-config /full/path/to/file.zip`

    Change */full/path/to/file* according to your settings. This command needs to be run with administrator privileges. If you are using Apple Remote Desktop, then enter **`root`** in the field **user name** to specify which user issues the above stated command.

6. You can add additional steps to your workflow, based on your specific settings, e.g. shutting down the target machines.

3 Recommendations and limitations

3.1 Recommendations

Reduce administration effort

- Keep the number of mount points (or Secured Folders) as low as possible.
- **Deactivate the option "Require confirmation before creating a mobile account"**

  If you create or use mobile accounts for Mac endpoints, make sure the option **Require confirmation before creating a mobile account** is deactivated. With the option activated, the user could select “Don’t Create”. This would result in the creation of an incomplete OS X user, for example a user that does not have a local home directory.

  To deactivate the option, perform the following steps:

  1. Open the **System Preferences** and click on **Users & Groups**.
  2. Click the lock icon, then enter your password.
  3. Select the User.
  4. Click **Login Options**.
  5. Go to **Network Account Server** and click **Edit...**
  6. Select the Active Directory Domain.
  7. Click **Open Directory Utility...**
  8. Click the lock icon, then enter your password and click **Modify Configuration**.
  9. Select Active Directory and click the edit icon.
  10. Click the arrow left beside **Show Advanced Options**.
  11. Select **Create mobile account at login** and deselect the option **Require confirmation before creating a mobile account**.
  12. Confirm with **Ok**.

3.2 Limitations

- **Maximum number of Secured Folders (mount points) on a client**

  On each Mac OS X client you can have a maximum of 24 Secured Folders (mount points). If more than one user is logged in on a single machine, you need to add up the mount points from all logged-in users. If you use other products on your Mac which are also using FUSE for OS X, you must consider these mount points too within the overall maximum number of 24.

- **Permanent version storage is not available in Secured Folders**

  When opening a file (which has been modified before) from a Secured Folder, the standard functionality **Browse All Versions...** is not available.

- **Excluded folders**

The following folders are excluded from encryption:

- **Folders are excluded, but not their subfolders:**
  - <Root>/
  - <Root>/Volumes/
  - <User Profile>/
- **Folders as well as their subfolders are excluded:**
  - <Desktop>/
  - <Root>/bin/
  - <Root>/sbin/
  - <Root>/usr/
  - <Root>/private/
  - <Root>/dev/
  - <Root>/Applications/
  - <Root>/System/
  - <Root>/Library/
  - <User Profile>/Library/
  - /<Removables>/SGPortable/
  - /<Removables>/System Volume Information/

This means that for example an encryption rule for the root of an additional partition (<Root>/Volumes/) has no effect, although it will be shown as received policy.

An encryption rule on <Root>/abc will have an effect, while an encryption rule on <Root>/private/abc will not.

- **Searching for files**
  - **Spotlight search**

    The Spotlight search does not work in encrypted files, therefore it will not return any matches when searching in Secured Folders.

  - **Labelled files**

    Searching for labelled files does not work in Secured Folders.

- **Burning CDs**

  It is not possible to burn an encrypted CD.

- **Sharing Secured Folders**

  A secured folder cannot be shared over the network. For example, if there is a rule on <Documents> this folder can no longer be shared.

- **Deleting files**

  When deleting files from a Secured Folder (mount point), a message prompts you to confirm the delete process. Deleted files are not moved to the Trash folder and thus cannot be restored.

- **SafeGuard Portable**

  SafeGuard Portable is not available for Mac OS X.

- **Use of Time Machine**

  If you use Time Machine with an encrypted folder, no old versions are displayed. However - provided that you have enabled Time Machine - the backups are there, they are just hidden. Proceed as follows:

  - Open Time Machine (for example by typing "Time Machine" in the Spotlight search). The contents of your root folder will be displayed.
  - Press **Shift - Command - G** (for "Go to the folder:") and enter the hidden path of the encrypted folder you want to restore. Example: If the encrypted folder you usually work with is named /Users/admin/Documents, then enter /Users/admin/.sophos_safeguard_Documents/.
  - Browse to the file you want to restore, click the wheel icon from the Time Machine menu bar and select **Restore <file name> to...**. After returning from Time Machine to your desktop, your file will be restored and can be decrypted.

    Note: You are not able to read the contents of the files located in the hidden path. So the backup contains only encrypted data and your contents are kept secure.

- **Use of AirDrop**

  Encrypted files can be transferred with AirDrop. Ensure that the target device can handle encrypted files. If it cannot, applications may behave unpredictably.

- **Handoff**

  Using Handoff for encrypted files is not supported.

- **Mounting network file shares with `autofs`**

  Network file shares which have a policy applied and are automatically mounted at startup will not be detected by Sophos SafeGuard File Encryption. It is not possible to handle such mount points because the original mount point cannot be replaced.

4 Configuration

Sophos SafeGuard File Encryption for Mac OS X is administered in the SafeGuard Management Center. The following chapter focuses on the Mac-specific configuration. Any standard Management Center functionality is described in the *SafeGuard Enterprise Administrator help*. For specific information on File Encryption policies, refer to the chapter "Policy settings" and the following chapters in the *SafeGuard Enterprise Administrator help*.

Note:

SafeGuard File Encryption for Mac only uses policies of the type **File Encryption** and **General Settings**. This means that you only need to use a **File Encryption** policy for managing encryption of data on the local file system, removable media, network shares and cloud storage. **Device Protection** policies (including **Cloud Storage** and **Removable Media Encryption** policies) will be ignored for SafeGuard File Encryption for Mac OS X. Always assign **File Encryption** policies to the user objects. **File Encryption** policies assigned to endpoints will not have any effect on OS X endpoints.

Note:

In the SafeGuard Management Center, paths have to be entered using backslashes. They are automatically converted to forward slashes on the Mac client side.

4.1 Centrally administered configuration options

The following options are configured centrally in the Management Center:

- **Policies**
- **Keys**
- **Certificates**

  The SafeGuard Enterprise backend provides the X.509 certificate for the user. When logging in for the first time, a certificate is generated. The certificate secures the users keyring. For details about how to request a certificate after login, see the *Quick startup guide*.

- **Connection interval to server**

Note: You can find more information on the options mentioned above in the *SafeGuard Enterprise Administrator help*.

4.2 Locally administered configuration options

The following options are configured locally on the Mac client:

- **Synchronize database information**

  Use the command **`sgfsadmin --synchronize`** to start synchronizing database information from Management Center such as policies, keys and certificates.

- **Enable or disable the system menu**

  Use the command **`sgfsadmin --enable-systemmenu`** to activate the system menu in the upper right corner.

  Use the command **`sgfsadmin --disable-systemmenu`** to deactivate the system menu.

  For both options refer also to Sophos SafeGuard File Encryption system menu (page 18).

Refer to Command line options (page 19) for a complete overview of all command line options.

5 Working with File Encryption for Mac

A separate Quick Startup Guide for File Encryption explains the user-relevant aspects of the application. You can find the latest version of the product documentation on our Documentation page at http://www.sophos.com/en-us/support/documentation.aspx.

In the following sections you will find information on how to work with File Encryption for Mac from an administrator's perspective.

5.1 How does encryption work?

Each encrypted file is encrypted with a randomly generated key called Data Encryption Key (DEK) using algorithm AES-256. This randomly generated and unique DEK is encrypted and stored as a file header together with the encrypted file, increasing the original file size by 4 KB.

The DEK is encrypted with a Key Encryption Key (KEK). This KEK is stored in the central SafeGuard Enterprise database. It will be assigned by the security officer to a single user, to groups or to organizational units.

To decrypt an encrypted file, the user must have the KEK specific to this file in their keyring.

5.2 Initial encryption

On the client side, perform the following tasks:

1. Open the **System Preferences**.
2. Click the Sophos Encryption icon:

   

3. Select **Policies** tab.
4. Switch to **Locally Translated Path** view if not already opened. You can now
   a) enforce all policies. To do so, click the button **Enforce all policies** in the lower part of the window.

      or

   b) select a single policy and click the button **Enforce policy**.

   Note: Do not disconnect devices while the initial encryption is running on them.

   Note: If you want to see details and contents of the locally translated path, select the path from the table and click **Show in Finder**. The Finder window is opened displaying the path selected and its contents where available.

5.3 Password handling

The Sophos SafeGuard key ring is secured with a user certificate. The corresponding private key is protected by the OS X password.

The password is required to allow the certificate to be generated if the user has not been created in SafeGuard Enterprise.

Changing password locally

Users can change their passwords locally in **System Preferences > Users & Groups**, and no further steps are required.

Password has been changed on a different endpoint

Note: Passwords can be changed on Windows as well as Mac endpoints.

Since the password is no longer known on this endpoint the following steps need to be completed:

1. Log in to OS X with your new password.
2. **The system was unable to unlock your keychain** is displayed.
3. Select **Update Keychain Password**.
4. Enter the old password.

For details of how to reset a forgotten password see Forgotten Mac OS X login password (page 23).

5.4 Fast user switching

SafeGuard File Encryption for Mac also works with fast user switching. It allows you to switch between user accounts on a single endpoint without quitting applications or logging out from the machine.

Note: OS X FUSE can handle a maximum number of 24 mount points (Secured Folders). See also Recommendations and limitations (page 8).

5.5 Preference pane

The preference pane allows you to set preferences for a specific application or the system. After installing Sophos SafeGuard File Encryption (or Sophos SafeGuard Native Device Encryption) on a Mac client, the following preference pane icon appears in the **System Preferences**:

Click on the icon to open the Sophos Encryption preference pane. The **About** content is shown.

The menu bar allows you to open the following menu information windows:

5.5.1 About tab

The **About** tab informs you about the product version installed on your Mac OS X client and about the copyright and registered trademark(s). If Sophos SafeGuard Disk Encryption or Native Device Encryption is installed, it will also be listed.

Click on the Sophos link in the lower part of the window to open the Sophos website.

5.5.2 Server tab

Click on **Server** to display a window containing the following information and functionality:

Server Info

- **Contact interval:** shows the interval at which synchronization with the server is started. Refer to the *SafeGuard Enterprise Administrator help* > *Policy settings* > *General settings* for information on how to set this interval.
- **Last Contacted:** shows the date when a client last communicated with the server.
- **Primary Server URL:** URL of the main server connection.
- **Secondary Server URL:** URL of the secondary server connection.
- **Server Verification:** shows whether SSL server verification for communication with the SafeGuard Enterprise server is enabled or disabled. Refer to Command line options (page 19) for a description of how to modify this option.

Drag configuration zip file here

Drag the configuration zip file to this drop zone in order to apply configuration information from the SafeGuard Management Center to the Mac client. See also Manual (attended) installation (page 6).

Synchronize

Click this button to start manually synchronizing database information such as policies and/or keys. This might be required after having performed modifications in the SafeGuard Management Center.

If the synchronization fails, the following icon will appear:

If the problem persists, check the connection to the server using the primary and secondary server URL. See Installation (page 5) for general prerequisites. If synchronization has worked previously, the issue might be caused by an expired SSL certificate. See also the system log for more information about possible causes.

Company Certificate

- **Valid from:** the date the certificate has become valid
- **Valid to:** the date the certificate validity expires
- **Issuer:** the instance which has issued the certificate
- **Serial:** the serial number of the company certificate

5.5.3 User tab

Click on **User** to display information about:

- The **Username** of the user currently logged on.
- The **Domain**, listing the domain directory the client belongs to. For local users the local computer name is displayed.
- The **SafeGuard User GUID**, displaying the GUID which has been generated for the user following their first login.

In the second window section you can check/uncheck the following option:

- **Show System Menu for File Encryption**: when activated, the Sophos SafeGuard File Encryption icon appears in the menu bar. See also Sophos SafeGuard File Encryption system menu (page 18).

The third window section displays information about the **User Certificate**:

- **Valid from:** the date the certificate has become valid
- **Valid to:** the date the certificate validity expires
- **Issuer:** the instance which has issued the certificate
- **Serial:** the serial number of the certificate

5.5.4 Keys tab

Click on **Keys** to display all existing key names in a list view.

Click on the list icon in the lower right corner next to **Number of Keys** to hide or show the GUID information of the respective key(s).

You can list and sort the keys using one of the header elements **Key Name** or **Key GUID**.

If a key is displayed in blue, it is the personal key of the user.

5.5.5 Policies tab

Click on **Policies**, to open the policies view. Click on one of the icons in the right lower corner to switch between **Locally Translated Path** view and **Received Policies** view:

- The **Locally Translated Path** displays only those policies which apply at this point in time to the logged in user on a specific Mac. The columns in the table contain the following information:
  - **@-symbol**: during initial encryption or when encrypting larger files you can see a turning wheel in the first column headed with an @, until the encryption is completed.
  - **Mode**: either **encrypt** or **exclude** is displayed.

    Note:

    Refer to the *SafeGuard Enterprise Administrator help* for detailed information on these modes.

  - **Scope**: specifies whether subfolders are to be encrypted.

- **Key Name**: name of the key assigned to the specified location.

  If a key is displayed in blue, it is the personal key of the user.

  A key that is displayed in orange is configured in a policy that was assigned to the user. But the user does not own the key, because it was not assigned to their keyring. This can cause trouble when accessing data, see also Problems when trying to access data (page 23).

To switch to the Received Policies View, click in the right lower corner for **Policy View** on the right icon:

- The **Received Policies view** displays all policies which are received from the server. This view is identical to the view in the SafeGuard Management Center. The table lists the following information:
  - **Received Policies**: specifies which files or folders to encrypt.
  - All other columns contain the information described above for the **Locally Translated Path** view.

Display Secured Folders and apply policies in Locally Translated Path view

If a policy is selected (1) in the **Locally Translated Path** table, you can

- Click the button **Show in Finder** (2) to open the selected Secured Folder (mount point) in a Finder window and to display its contents.
- Click **Enforce Policy** (3) to apply the selected policy on all files in the specified location. A progress bar is displayed. Wait for the system to complete the policy application process or cancel the process by clicking the cross next to the bar.

  Note:

  To deselect a single policy, press the **Cmd** key and click with the mouse.

  Note:

  Files which are write-protected or not accessible because of missing permissions will be excluded from encryption.

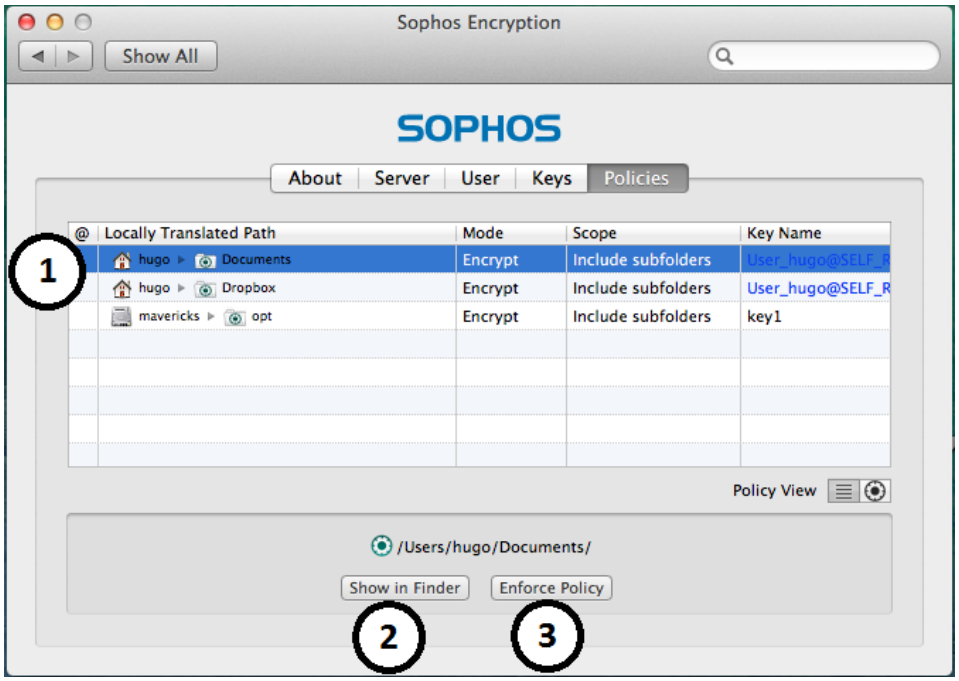

Figure 1: Policies tab screen - Locally Translated Path view

Possible results from enforcing policies

If you have policies enforced:

- Plain files will be encrypted with the encryption key assigned by a policy.
- Files already encrypted with the encryption key specified in the policy will remain encrypted.
- Files already encrypted with another encryption key will
  - remain unchanged if the user does not have the corresponding encryption key in their keyring.
  - be re-encrypted with the encryption key assigned via policy if the user has this encryption key in their keyring.
- Files which were encrypted multiple times will be encrypted once with the encryption key assigned by the policy. If one of the required encryption keys is not available, these files will be decrypted as far as possible.

5.6 Sophos SafeGuard File Encryption system menu

The system menu provides you with the following information and functionality:

1. When a file is selected, the icon automatically shows you the encryption status and key name:

	Green icon: The file is encrypted and you own the corresponding key.

	Red icon: The file is encrypted but you do not own the corresponding key.
	Gray icon: The file should be encrypted but is not yet encrypted. (*)
	Black icon: The file is ignored or excluded from encryption.

(*) Possible scenario: If you have selected an unencrypted file which is located in a directory where an encryption policy is applied, the icon will become gray. Open the **Policies** tab, select the corresponding policy for this directory and select **Enforce Policy** to initially encrypt this file. See also Policies tab (page 16).

2. When a file is being processed, the wheel of the icon rotates. This behavior is independent from the current encryption state.
3. Depending on files or volumes selected, the following menu items are available:
   - Current encryption and key state:

     If a file, directory or volume is selected, a related message about the current encryption status, the name of the necessary key and information about whether the user owns this key is displayed.

     Note:

     To make sure the current encryption state and key name for files and directories is displayed, it might be necessary to switch the focus from the selected file or directory to somewhere on the desktop and back to the selected file/directory.

   - List of available SafeGuard Secured Folders (mount points):

     Note:

     If you hover with the mouse over one of the Secured Folder icons, the full path to the folder is shown.

   - **Open Sophos Encryption Preferences...**

     Opens the Sophos Encryption preference pane. See also Preference pane (page 14)

5.7 Command line options

The Terminal application allows you to enter commands and command line options. The following command line options are available:

Command name	Definition	Additional parameters (optional)
`sgfsadmin`	Lists available commands including short help hints.	**`--help`**

Command name	Definition	Additional parameters (optional)
sgfsadmin --version	Displays version and copyright information of the installed product.	
sgfsadmin --status	Returns system status information such as version, server and certificate information.	
sgfsadmin --list-user-details	Returns information on the user currently logged on.	**--all** displays information for all users (sudo required) **--xml** returns output in xml format.
sgfsadmin --list-keys	Lists existing GUIDS and names of all keys in the keystore.	**--all** displays information for all users (sudo required) **--xml** returns output in xml format
sgfsadmin --list-policies	Displays policy-specific information. Key GUIDs are resolved to key names if possible. Bold print indicates a personal key.	**--all** displays information for all users (sudo required) **--xml** returns output in xml format **--raw** displays raw policies, i.e. policies as set on the SafeGuard Management Center server side
sgfsadmin --enforce-policies	Applies the encryption policy.	**--all** applies the policy to all directories where policies apply **"directoryname"** applies the policy to the directory specified.
sgfsadmin --file-status "filename1" ["filename2"..."filenameN"]	Returns encryption information for a file or a list of files. Wildcards are accepted.	**--xml** returns output in xml format
sgfsadmin --import-config "/path/to/target/file"	Imports the specified configuration zip file. See also Manual (attended) installation (page 6). The command needs administrative rights (sudo). **Note:** Use the drag and drop functionality to drag a complete path from, for	

Command name	Definition	Additional parameters (optional)
	example, the Finder into the Terminal application.	
sgfsadmin --enable-server-verify	Turns on SSL server verification for communication with the SafeGuard Enterprise server. After installation, the SSL server verification is activated. The command needs administrative rights (sudo).	
sgfsadmin --disable-server-verify	Turns off server verification for communication with the SafeGuard Enterprise server. The command needs administrative rights (sudo). **Note:** We do not recommend this option as it may create a security vulnerability.	
sgdeadmin --update-machine-info [--domain "domain"]	Updates the currently stored machine information which is used to register this client on the SafeGuard Enterprise server. The command needs administrative rights (sudo). **Note:** Use this command only after changing the domain or workgroup the computer belongs to. If the computer is a member of multiple domains or workgroups and you execute this command, this might result in a change of the domain registration and removal of personal keys and/or FileVault 2 users.	**--domain "domain"** The domain the client should use to register on the SafeGuard Enterprise server. This parameter is only required if the machine is a member of multiple domains. The computer must be joined to this domain, otherwise the command will fail.

The following commands are explained in detail in section Locally administered configuration options (page 11):

- **sgfsadmin --enable-systemmenu**
- **sgfsadmin --disable-systemmenu**
- **sgfsadmin --synchronize**

5.8 Working with removable devices

Note:

Before working with removable devices, make sure you have been assigned a policy and key that allow you to encrypt files on removable media.

1. Connect the removable device.
2. A dialog, asking if you want to encrypt plain files on the device, appears. Click **Yes** to start encryption. If you click **NO** these files stay plain but you have access to files on the device that are already encrypted. Regardless of your selection, new files on the device will always be encrypted according to the policy.
3. The files on your device will be encrypted automatically. This is indicated by the system menu icon wheel rotating.
4. As soon as all files on your device are encrypted, the wheel rotation stops.
5. Eject the removable device. The corresponding Secured Folder icon disappears automatically.

   Note:

   To be able to exchange and modify data on removable devices between two parties, both parties must have the corresponding policy and key assigned. For the exchange between Windows and Mac OS X clients the device must be formatted using FAT32, and no personal keys can be used. For the Windows client a data exchange policy is necessary. The media passphrase functionality is only available for Windows. From a Mac OS X client the data can be accessed only if corresponding policies of type **File Encryption** are defined.

6 Troubleshooting

6.1 Forgotten Mac OS X login password

If a user forgets the Mac OS X login password, proceed as follows:

1. The user will ask you to create a new user password.
2. To do so, reset the existing password in your user administration environment and generate a new password. Select the corresponding option to make sure you force the user to modify the password after the first login.
3. Switch to the SafeGuard Management Center application and remove the certificate for the user.
4. Contact the user and hand over the new password.
5. Tell the user to login with this new password.
6. After logging in, the **Reset Password** dialog appears.
7. Tell the user to define a new password, to enter and to verify this new password and to specify a password hint. Finally the user has to click **Reset Password** to confirm the changes.
8. After resetting the password, the following message appears on the user side:

   The system was unable to unlock your login keychain
9. Tell the user to select the option **Create New Keychain**.
10. A new keychain for this user is created.
11. Now the user is requested to enter the new OS X password from step 7 to create the SafeGuard user certificate.

The user's keys will be loaded into the new keychain automatically, so all documents will be accessible as before.

6.2 Problems when trying to access data

If a user experiences problems when trying to access data, the reason might be that the user does not have the corresponding key in their keyring:

- Check the Management Center environment and correct if required. See Sophos SafeGuard File Encryption system menu (page 18) for information on how to check whether the currently logged on user has already got the corresponding key.

  Files encrypted with a key that is not in the user's keychain cannot be decrypted. Should the user try to copy files into a Secured Folder (which triggers the initial encryption of these files), and the corresponding key is not available, then Mac OS X displays a dialog asking the user for an administrator's name and password. In this case, the user should click on **Cancel** (the password would not help to access the encrypted files anyway).

6.3 SafeGuard recovered files

Under certain circumstances a folder named **Sophos SafeGuard Recovered Files** can be found in a folder. This happens if SafeGuard File Encryption tries to create a new Secured Folder (mount point), but the hidden folder that needs to be created for storing the encrypted contents (for example /Users/admin/.sophos_safeguard_Documents/) exists already and is not empty. Then the content of the original folder (for example /Users/admin/Documents) will be moved to **Sophos SafeGuard Recovered Files** and only the content of the hidden folder will be displayed as usual.

7 Uninstallation from client

If you need to uninstall the software from a client computer, proceed as follows:

1. On the Mac client go to */Library*.
2. Open the folder *Sophos SafeGuard FS*.
3. Select and double-click the file *Sophos SafeGuard FS Uninstaller.pkg*
4. A wizard guides you through uninstallation.
5. Restart the system before continuing to work with your Mac.

   Note: The uninstaller package is signed, and OS X will try to validate this signature. If there is a slow internet connection or a misconfiguration you may have a delay of up to 20 minutes during the uninstallation procedure.

8 Technical support

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

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

9 Legal notices