SOPHOS
Security made simple.

Sophos SafeGuard File Encryption for Mac

Quick startup guide

Product version: 7
Document date: December 2014

Contents

1 About Sophos SafeGuard File Encryption for Mac....3

2 First use....4

3 Working with SafeGuard File Encryption for Mac....5

3.1 Initial encryption....5

4 Sophos SafeGuard File Encryption system menu....6

5 Preference pane....7

5.1 About tab....7

5.2 Server tab....7

5.3 User tab....8

5.4 Keys tab....8

5.5 Policies tab....9

6 Working with removable devices....11

7 General hints....12

8 Technical support....13

9 Legal notices....14

1 About Sophos SafeGuard File Encryption for Mac

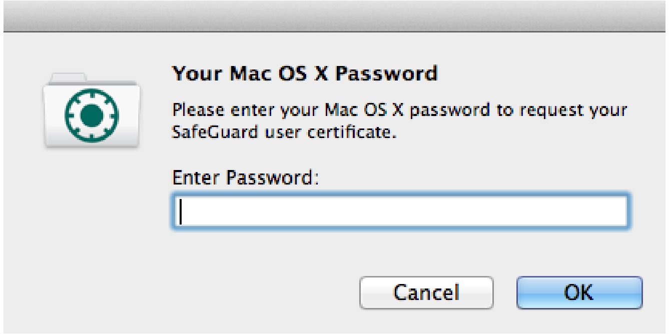
Sophos SafeGuard File Encryption for Mac extends the data protection offered by Sophos SafeGuard Enterprise from Windows to the Mac world. It offers transparent file-based encryption on local drives, network shares, removable drives and in the cloud. With SafeGuard File Encryption for Mac you can safely encrypt and decrypt files and exchange these files with others.

- New files in the relevant locations are encrypted automatically.
- If you have the key for an encrypted file, you can read and modify the content.
- If you do not have the key for an encrypted file, you cannot read its content in plain text but only see the encrypted content.
- If you access an encrypted file from any other computer where File Encryption is not installed, the encrypted content is shown.

2 First use

This manual assumes that the software has been installed as described in the *Sophos SafeGuard File Encryption for Mac Administrator help* and communication with the SafeGuard Enterprise backend has been successfully established.

1. Switch on the Mac.
2. Login to your Mac with your OS X password as usual.
3. When you first login after the product has been installed, you are prompted to enter your password again into the following dialog:



Your Mac OS X Password

Please enter your Mac OS X password to request your SafeGuard user certificate.

Enter Password:

Figure 1: This login dialog appears only after installation and first login per user.

4. Enter the password and confirm by clicking OK.

   Note: In order to use the product properly, you need a personal certificate. This certificate is generated per user when you enter the password in the dialog box. This is only required after product installation, first login or password reset.

5. According to the security settings which have been assigned to you, you see one or more new volumes on your desktop.

   Important: Make sure the option "Connected Servers" in your Finder setting is enabled. Select **Finder - Preferences - Tab "General"**, and then activate option **Connected Servers**.

3 Working with SafeGuard File Encryption for Mac

SafeGuard File Encryption for Mac allows your security administrator to define whether files located in specified directories and/or volumes will be encrypted or not. Spotlight search and permanent version storage ("Browse All Versions...") are not supported. However, if you try to eject a volume which points to a local directory, it will be automatically reconnected immediately.

The encryption itself is transparent. After the initial encryption the system ensures that files located in a volume or directory that is specified for encryption (called "Secured Folder" further on) are encrypted.

3.1 Initial encryption

Before starting to work, perform an initial encryption:

1. Open the **System Preferences**.
2. Click the Sophos Encryption icon.
3. Select the **Policies** tab.
4. Switch to **Locally Translated Path** view and click on **Enforce all policies** to apply all policies.

All plain files will be encrypted after performing this operation.

If you want to enforce a single policy, select the policy with the mouse and click **Enforce Policy**. To deselect a single policy, press the **Cmd** key and click with the mouse.

4 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 in the menu bar automatically shows you the encryption and key status:

🟢	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. (*)
⚫	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.

2. When a file is being processed, the wheel of the icon rotates. This behavior is independent of 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 whether the user owns this key is displayed.

     Note: To make sure the current encryption and key state 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 folder icons, the full path of the folder is shown.

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

     Opens the Sophos Encryption preference pane.

5 Preference pane

A preference pane allows you to set preferences for a specific application or the system. After installing Sophos 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:

5.1 About tab

The **About** tab informs you about the product version installed on your Mac 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.

5.2 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. It is centrally defined by the security officer.
- **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.

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.

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, contact your security administrator to solve it.

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

5.3 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 6).

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

5.4 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's your personal key.

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.

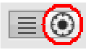
    - **Scope**: specifies whether subfolders are to be encrypted.

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

      If a key is displayed in blue, it's your personal key.

      A key that is displayed in orange means it has been configured in a policy that was assigned to you. But, you do not own the key, as it was not assigned to your keyring. This can cause trouble when accessing data. In this case contact your security officer.

  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.

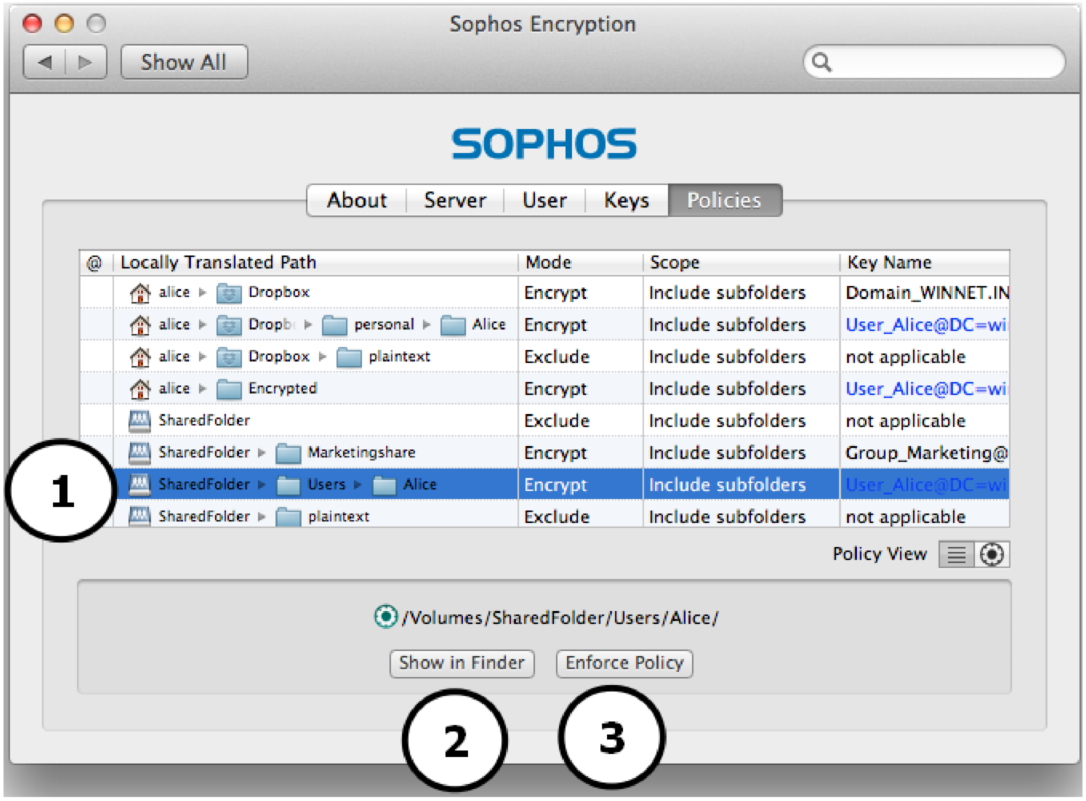
- Click **Enforce Policy** (3) to apply the selected policy on all files permitted. A progress bar is displayed. Wait for the system to complete the policy application process or cancel the process by clicking the cross next to the bar.

  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.



@	Locally Translated Path	Mode	Scope	Key Name
	alice ▸ Dropbox	Encrypt	Include subfolders	Domain_WINNET.IN
	alice ▸ Dropb ▸ personal ▸ Alice	Encrypt	Include subfolders	User_Alice@DC=wi
	alice ▸ Dropbox ▸ plaintext	Exclude	Include subfolders	not applicable
	alice ▸ Encrypted	Encrypt	Include subfolders	User_Alice@DC=wi
	SharedFolder	Exclude	Include subfolders	not applicable
	SharedFolder ▸ Marketingshare	Encrypt	Include subfolders	Group_Marketing@
	SharedFolder ▸ Users ▸ Alice	Encrypt	Include subfolders	User_Alice@DC=wi
	SharedFolder ▸ plaintext	Exclude	Include subfolders	not applicable

/Volumes/SharedFolder/Users/Alice/

Figure 2: Policies tab screen - Locally Translated Path view

Possible results from enforcing policies

If you have policies enforced:

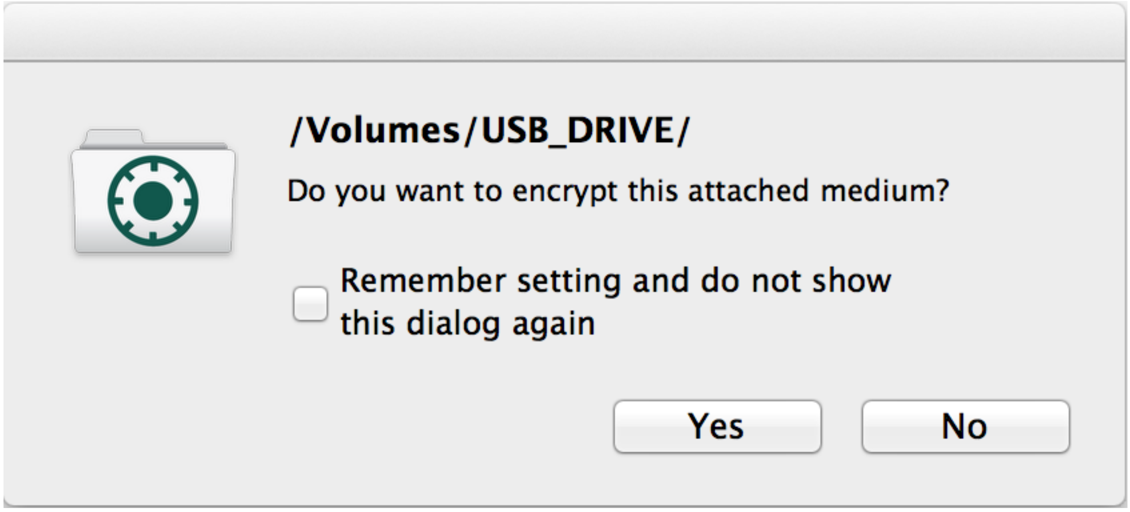
- Plain files will be encrypted with the encryption key assigned by a policy.
- Files already encrypted with the encryption key specified in the policy will remain encrypted.
- Files already encrypted with another encryption key will
  - remain unchanged if the user does not have the corresponding encryption 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.

6 Working with removable devices

Important: Make sure you have been assigned a policy and key that allow you to encrypt and modify files on removable media.

If you want to encrypt files on a removable device, proceed as follows:

1. Insert the device into the Mac.
2. A dialog prompts you to confirm that you want to encrypt the files.



/Volumes/USB_DRIVE/

Do you want to encrypt this attached medium?

□ Remember setting and do not show this dialog again

3. Click **Yes** to confirm.
4. The files on your device will be encrypted. The wheel of the icon will rotate.
5. When all files on your device are encrypted, the wheel of the icon will stop rotating.
6. Eject the removable device. The corresponding volume icon disappears automatically.

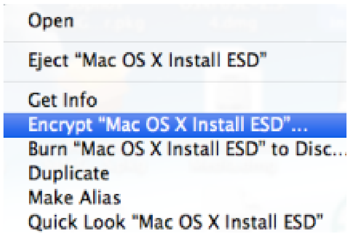
To be able to exchange and modify data on removable devices between two parties, both parties must have the corresponding policy and key assigned.

Important: If you exchange larger files on removable devices, make sure you have more free space available than twice the largest file size to be exchanged.

7 General hints

If you encounter Mac OS X FileVault 2 disk encryption functionality...

If you select a volume (on your desktop or in the Finder) and right-click with the mouse, a menu item "Encrypt <volume name> ..." may appear:


Open
Eject "Mac OS X Install ESD"
Get Info
Encrypt "Mac OS X Install ESD"...
Burn "Mac OS X Install ESD" to Disc...
Duplicate
Make Alias
Quick Look "Mac OS X Install ESD"

This is the Apple OS X internal disk encryption application FileVault 2, which is not linked to our SafeGuard File Encryption application.

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

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