SOPHOS

Security made simple.

Sophos SafeGuard Native Device Encryption for Mac

quick startup guide

Product version: 7

Document date: December 2014

Contents

1 About SafeGuard Native Device Encryption for Mac

Sophos SafeGuard Native Device Encryption for Mac extends the data protection offered by Sophos SafeGuard Enterprise from Windows to the Mac world.

Encrypting the entire hard disk ensures that all information is protected without the potential for accidental exposure, even when a computer is lost or stolen.

2 Working with SafeGuard Native Device Encryption for Mac

The disk encryption works transparently. You will not see any prompts for encryption or decryption when opening, editing, and saving files.

The security officer specifies which clients will be encrypted using the Sophos SafeGuard Management Center (a core component of SafeGuard Enterprise). It provides information about the encryption status of each client and helps with recovery if a user has forgotten the logon password.

2.1 Perform initial encryption

If a volume-based encryption of the system disk is defined in the policy, then disk encryption will be activated for the user currently logged on. Before encryption starts, a dialog is shown to ask the user for the logon password.

1. Enter your Mac OS X password when asked for it.

   If the dialog is shaking, the password is incorrect. Try again.

   Note: If your password is empty, please change it. It is not possible to enable disk encryption without a password set.

2. Wait for the Mac to restart.

   Note: If activation of the encryption fails, an error message will be displayed. Please contact your system administrator.

Disk encryption operates in the background, so you can continue with your work.

2.2 Decryption

Usually, it is not necessary to decrypt. If the security officer sets a policy that specifies no encryption for your Mac client that is already encrypted, it will remain encrypted. However, in this case you have the choice to decrypt. You will find the corresponding button in the preference pane.

3 Recovery of Mac OS X logon password

If you forget your Mac OS X logon password, proceed as follows:

1. Switch on your Mac.
2. In the logon dialog click on **?**. (Alternatively, enter a wrong logon password three times.)

   Your password hint is displayed and you are asked if you want to reset your password using your recovery key.

3. If you still do not remember your password, click the icon next to the text:

   

4. Call the helpdesk and enter the recovery key you are given.

   The Mac starts and you are asked to enter a new password and a password hint.

4 Sophos SafeGuard Native Device Encryption system menu

The system menu provides the following information:

- The icon (on the left) shows the encryption status:

Figure 1: System menu

	Green icon: The system disk is encrypted.
	Red icon: The system disk is not encrypted.

- The following menu item is available when you click on the icon:
  - **Open Sophos Encryption Preferences...**

    Opens the Sophos Encryption preference pane.

Note: To enable or disable the system menu see User tab (page 8).

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 File 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 Sophos SafeGuard Enterprise server is enabled or disabled. It should be enabled.

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.

If the synchronization fails, the following icon will appear:

Open the log file to retrieve 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

5.3 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 logon.

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

- **Show System Menu for Native Device Encryption**: when activated, the Sophos SafeGuard Native Device Encryption icon appears in the menu bar. See also Sophos SafeGuard Native Device Encryption system menu (page 6).

The third window section displays information about the **User Certificate** (it is not necessary for disk encryption):

- **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 Disk Encryption tab

Click on **Disk Encryption** to display information about the current policies and the status of the Mac client.

The first window section tells you whether the system disk should be encrypted according to the policy set by the security officer.

The second window section displays the status of the Mac client. This can be one of the following:

- The system disk is encrypted and a centrally stored recovery key is available.
- The system disk is encrypted but there is no centrally stored recovery key available.
- The system disk is not encrypted.

At the bottom a button **Decrypt System Disk** is displayed. It will be enabled if the security officer has set a policy defining that no encryption is necessary for the client.

Note: If there is no centrally stored recovery key available, the helpdesk cannot assist you with password recovery. To make the recovery key centrally available, import it using the command

line tool: **`sgdeadmin --import-recoverykey`**. Then, the security officer can provide you with the recovery key when you need it. If you do not know the recovery key, contact your security officer. Decryption and subsequent encryption of the disk will be necessary in order to create a new recovery key. This is important because if you forget your logon password and there is no recovery key available, all data stored on the encrypted disk will be lost.

6 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.

7 Legal notices