SOPHOS

Security made simple.

Sophos SafeGuard Native Device Encryption for Mac

Administrator help

Product version: 7

Document date: December 2014

Contents

1 About SafeGuard Native Device Encryption for Mac

Sophos SafeGuard Native Device Encryption for Mac offers Mac OS X users the same data protection that the disk encryption feature of SafeGuard Enterprise already offers to Windows users.

SafeGuard Native Device Encryption for Mac builds on Mac OS X's integrated FileVault 2 encryption technology. It uses FileVault 2 to encrypt the entire hard disk, so that your data is safe even if the computer is lost or stolen. However, it also enables you to provide and manage disk encryption for entire networks.

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

In SafeGuard Enterprise´s Management Center, you can select which computers (Windows as well as Macs) to encrypt, monitor their encryption status, and provide recovery for users who forget their passwords.

1.1 About this document

This document describes how to install, configure and administer Sophos SafeGuard Native Device 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 Native Device Encryption for Mac*.

1.2 Terms and acronyms

The following terms and acronyms are used in this document:

Term or acronym	Meaning or explanation
GUID	Globally Unique Identifier: a unique reference number used as an identifier in computer software.
POA	Power-On Authentication (synonym: "pre-boot authentication")
SGN	SafeGuard Enterprise

Term or acronym	Meaning or explanation
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 Native Device 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

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.

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.

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:

1. Ask your SafeGuard Server Administrator to provide you with the SafeGuard Enterprise server 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 with 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 **`sgdeadmin --disable-server-verify`** with sudo rights as described here: Command line options (page 15). 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 the server has been properly set up as described in Installation prerequisites (page 5).

1. Open *Sophos SafeGuard DE.dmg*.
2. After reading through the readme file offered, double-click *Sophos SafeGuard DE.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 DE/*.
3. Click **Close** to complete the installation.
4. After a restart, logon with your Mac password.
5. Open the **System Preferences** and click the Sophos Encryption icon to show the product settings.
6. Click the **Server** tab.
7. 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.
8. Select the configuration zip file (For a description of how to create a configuration package for Macs see *SafeGuard Enterprise Administrator Help* version 7.0, *Working with configuration packages > Create configuration package for Macs*).
9. Drag the zip file to the **Server** dialog and drop it into the drop zone.
10. You will be prompted to enter a Mac administrator password. Enter the password and click **OK** to confirm.

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 12) 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 Native Device Encryption for Mac. Use the management software installed on your system. Depending on the management solution you are using, the actual steps may vary.

Note:

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

1. Download the installer file *Sophos SafeGuard DE.dmg*.
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 (For a description of how to create a configuration package for Macs see *SafeGuard Enterprise Administrator Help* version 7.0, *Working with configuration packages* > *Create configuration package for Macs*) and copy it to the target machines.
5. Run the following command on the target machines:

    ```
    /usr/bin/sgdeadmin --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.

3 Configuration

Sophos SafeGuard Native Device 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*.

Note:

SafeGuard Native Device Encryption for Mac only makes use of policies of the type **Device Protection** and **General Settings** and ignores all policy settings except **Target**, **Media encryption mode** and **Connection interval to server (min)**.

3.1 Centrally administered configuration options

The following options are configured centrally in the Management Center:

Policies

Policies are configured centrally in the SafeGuard Management Center. In order to initiate full disk encryption the settings must be chosen as follows:

1. Create a new policy of type **Device Protection**. For **Device protection target** choose **Local Storage Devices**, **Internal Storage** or **Boot Volumes**. Type a name for the policy and click **OK**.
2. For **Media encryption mode** select **Volume based**.

A new policy for device protection has been created and configured for full disk encryption for Macs.

Note: Make sure that the policy is assigned to the clients that will be encrypted. If all of the endpoints are to be encrypted you might assign the policy to the top level of your domain or workgroup. If IT staff take care of the installation, do not assign the policy before the clients are given to the end users. There is the risk that the endpoint is encrypted too early and IT staff are registered for FileVault 2 instead of the end users.

Connection interval to server

You can find more information on policies and the connection interval to the server in the *SafeGuard Enterprise Administrator help*.

3.2 Locally administered configuration options

The following options are configured locally on the Mac client:

- **Synchronize database information**

  Use the command `sgdeadmin --synchronize` to start synchronizing database information from the SafeGuard Enterprise backend such as policies and keys.

- **Enable or disable the system menu**

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

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

Note: Default setting after installing SafeGuard Native Device Encryption is "disabled".

For more information on the system menu, see Sophos SafeGuard Native Device Encryption system menu (page 14).

Refer to Command line options (page 15) for a complete overview of all command line options.

4 Working with SafeGuard Native Device Encryption for Mac

A separate Quick Startup Guide for SafeGuard Native Device 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 SafeGuard Native Device Encryption for Mac from an administrator's perspective.

4.1 How does encryption work?

FileVault 2 keeps all data on the hard drive secure with XTS-AES-128 data encryption at the disk level. The algorithm has been optimized for 512-byte blocks. The conversion from plaintext to ciphertext and back is performed on the fly with low impact on the user experience since it is given a lower priority.

One traditional obstacle to usability with full disk encryption is that it was necessary for the end user to authenticate twice: once to unlock the encrypted boot volume (POA), and the second time to log on to the user desktop.

However, this is no longer necessary. Users enter their password at the pre-boot logon and the system initiates password-forwarding when the operating system is up and requiring logon credentials. Password-forwarding eliminates the need for users to log on twice after a cold boot.

Users are able to reset their passwords at any time without the need to re-encrypt the volume. The reason is that a multi-level key system is employed. The keys shown to the users (e.g. logon keys and recovery keys) are derived encryption keys and therefore can be replaced. The true volume encryption key will never be given to a user.

For further information on FileVault 2 see *Apple Technical White Paper - Best Practices for Deploying FileVault 2 (Aug. 2012)*, which can be downloaded from the Apple website.

4.2 Initial encryption

If a volume-based encryption of the system disk is specified in the policy, then disk encryption will be activated for the user currently logged on. On the client side, perform the following tasks:

1. Before encryption starts, a dialog is shown to ask for the logon password. Enter the Mac OS X password.

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

   Note: If the 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. More information can be found in the log files. The default location is `/var/log/system.log`

3. Disk encryption starts and is done in the background. The user can continue working.

The user is added as the first FileVault 2 user of the endpoint.

4.3 Decryption

Usually it is not necessary to decrypt. If you set a policy that specifies **No encryption** for Mac clients that are already encrypted, they will remain encrypted. But in this case the users have the choice to decrypt. They will find the corresponding button in the preference pane, see Disk Encryption tab (page 14).

Users with local administrator rights cannot be prevented from attempting to manually decrypt their hard disk using built-in FileVault 2 functionality. However, they will be prompted for a restart to complete the decryption. As soon as the Mac has completed the restart, SafeGuard Native Device Encryption for Mac will enforce encryption if a corresponding policy has been set.

4.4 Add FileVault 2 user

Only users that are already registered for FileVault 2 at the endpoint will be able to log on to the system after a restart. In order to add a user to FileVault 2 proceed as follows:

1. While the Mac is still running, log on with the user you want to register for FileVault 2.
2. Provide the credentials of that user in the dialog **Enable Your Account**. If you are using Mac OS X version 10.8, the user's own credentials as well as those of a user already active in FileVault 2 will be requested. With Mac OS X version 10.9 this is no longer necessary.

Therefore, with the exception of Mac OS X version 10.8, users will be able to log on as easily as if there was no disk encryption enforced.

4.5 Remove FileVault 2 user

A user can be removed from the list of users assigned to a Mac in the SafeGuard Management Center. After the next synchronization, the user will be removed from the list of FileVault 2 users of the endpoint as well. But this does not mean that the user will not be able to log on to that Mac anymore. Like any new user, the user just needs to log on to a running Mac in order to become authorized again.

If you really want to prevent a user from booting a Mac, mark the user as blocked in the Management Center. The user will then be removed from the list of FileVault 2 users of the client and no new authorization will be possible.

It is possible to remove all FileVault 2 users but the last one. If the owner is removed, then the next user in the list will be marked as owner. In SafeGuard Native Device Encryption for Mac it does not make a difference if a user is owner or not.

4.6 Synchronization with backend

In the process of synchronization, the states of the clients are reported to the SafeGuard Enterprise backend, policies are updated and the user-machine assignment is checked.

Therefore, the following information is sent from the clients and appears in the SafeGuard Management Center:

- As soon as an endpoint is encrypted, "POA" is checked. Other information that is displayed includes drive name, label, type, state, algorithm and operating system.
- New FileVault 2 users are added also in the Management Center.

Note: If the SafeGuard Enterprise client software is removed from an endpoint, the endpoint and its users are still visible in the SafeGuard Management Center. But the timestamp of the last server contact does not change any more.

On the client side the following things are changed:

- Policies that were changed in the Management Center are changed on the client.
- Users that have been deleted or blocked in the Management Center are also removed from the list of FileVault 2 users on the client.

4.7 Preference pane

A preference pane allows you to set preferences for a specific application or the system. After installing Sophos SafeGuard Native Device Encryption (or Sophos SafeGuard File 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:

4.7.1 About tab

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

4.7.2 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 15) (command **`sgdeadmin --enable-server-verify`** or **`sgdeadmin --disable-server-verify`**) 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. This might be required after having performed modifications in the SafeGuard Management Center.

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

4.7.3 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 14).

The third window section displays information about the **User Certificate** (if a user certificate was assigned in the SafeGuard Management Center):

- **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

4.7.4 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 FileVault 2 is enabled, the current user is active in FileVault 2 and 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 with password recovery. Therefore, the recovery key should be imported using the command line tool: **`sgdeadmin --import-recoverykey`**. If the recovery key is unknown by the user as well as the security officer, decryption and subsequent encryption of the disk will be necessary in order to create a new recovery key.

4.8 Sophos SafeGuard Native Device Encryption system menu

The system menu provides the following information:

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

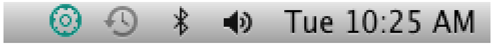
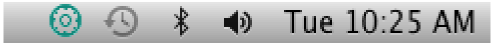
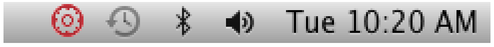


Figure 1: System menu

	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 13).

4.9 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)
`sgdeadmin`	Lists available commands including short help hints.	**`--help`**
`sgdeadmin --version`	Displays version and copyright information of the installed product.	
`sgdeadmin --status`	Returns system status information such as version, server and certificate information.	
`sgdeadmin --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.
`sgdeadmin --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
`sgdeadmin --synchronize`	Forces immediate contact with the server (needs working server connection).	
`sgdeadmin --import-recoverykey` ["recoverykey"]	Imports the FileVault 2 recovery key, overwrites existing recovery key.	**`--force`** existing recovery key will be overwritten without any additional confirmation **`"recoverykey"`** if it is not entered, the user will be asked for it
`sgdeadmin --import-config "/path/to/target/file"`	Imports the specified configuration zip file. See also Manual (attended) installation (page 6). The	

Command name	Definition	Additional parameters (optional)
	command needs administrative rights (sudo). **Note:** Use the drag and drop functionality to drag a complete path from, for example, the Finder into the Terminal application.	
`sgdeadmin --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).	
`sgdeadmin --disable-server-verify`	Turns off SSL 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 computer 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 8):

- **`sgdeadmin --enable-systemmenu`**

- **`sgdeadmin --disable-systemmenu`**
- **`sgdeadmin --synchronize`**

5 Recovery

Recovery provides a way of accessing an encrypted volume by means of a centrally stored recovery key. This is necessary because a user might forget the Mac OS X logon password and there might be no other credentials available.

5.1 Recovery key handling

If all FileVault-enabled users on a particular system forget their passwords, other credentials are not available and there is no recovery key available, then the encrypted volume cannot be unlocked and the data is inaccessible. Data may be lost permanently, so proper recovery planning is essential.

A new recovery key is generated during each activation of disk encryption. Without Sophos SafeGuard Native Device Encryption being installed at the time of the encryption, it is displayed to the user who consequently is responsible for its protection against loss. With Sophos SafeGuard Native Device Encryption, it is securely sent to the SafeGuard Enterprise backend and stored centrally. The security officer can retrieve it whenever needed. See Forgotten Mac OS X logon password (page 18) for more information about the recovery process.

But even if SafeGuard Native Device Encryption was not installed when the disk was encrypted, the recovery key can be managed centrally. Therefore it is necessary to import it. The relevant command line option is **`sgdeadmin --import-recoverykey`**, see also Command line options (page 15). The recovery key will be sent in upper case.

Note:

- Mac OS X 10.8: the recovery key will not be checked, it is the responsibility of the user to enter it correctly. An error will be displayed only if the format is invalid.
- Mac OS X 10.9: the recovery key will be checked if valid or not.

In order to check whether a recovery key is present for a client, see Disk Encryption tab (page 14).

If there is an institutional recovery key present, it can be used for recovery as well. For more information see *OS X: How to create and deploy a recovery key for FileVault 2* at support.apple.com/kb/HT5077

5.2 Forgotten Mac OS X logon password

If a user forgets the Mac OS X logon password and there are no other credentials available, proceed as follows:

1. The user switches on the Mac.
2. The user clicks on **?** in the logon dialog. Alternatively, the user can enter a wrong logon password three times.

   The password hint is displayed and the user is asked if he or she wants to reset the password using the recovery key.

3. The user clicks on the triangle next to the message in order to get to the next step (to enter the recovery key):

4. In the SafeGuard Management Center, open the recovery wizard by selecting **Tools** > **Recovery** and display the recovery key for the specific machine.
5. Tell the user the recovery key to be entered at the Mac.

   The Mac starts and the user can enter a new password and a password hint.

Mac OS X 10.9 only: The recovery key is replaced as soon as it has been used once to start the system. The new recovery key is generated automatically and sent to the SafeGuard Enterprise backend where it is stored to be available for the next recovery.

Note: Be careful to whom you give a recovery key of an endpoint. As a recovery key is always machine specific and not user specific, it might also be necessary to check that the recovery key is not used to get unauthorized access to another user's sensitive data on the same machine.

6 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. Select the folder */Sophos SafeGuard DE*.
3. Select and double-click the file *Sophos SafeGuard DE Uninstaller.pkg*
4. A wizard guides you through uninstallation.

Note: It is not necessary to decrypt the disk before uninstalling the software.

Note: A user with administrative rights cannot be prevented from uninstalling the software. (A policy that prevents this on Windows clients has no effect on Mac clients.)

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.

7 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.

8 Legal notices

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