



Sophos SafeGuard Disk Encryption for Mac

User help

Product version: 5.55

Document date: August 2011



Content

- 1 About Sophos SafeGuard Disk Encryption for Mac 2
- 2 Sophos SafeGuard Disk Encryption system menu 3
- 3 Power-on Authentication 4
- 4 User management 8
- 5 Disk management 12
- 6 Using Sophos SafeGuard Disk Encryption via Terminal 14
- 7 Time Machine backups 20
- 8 Supported Hardware and Configurations 21
- 9 Unsupported hardware, configurations and operations 23
- 10 Technical support..... 26
- 11 Copyright 27

1 About Sophos SafeGuard Disk Encryption for Mac

Sophos SafeGuard Disk Encryption for Mac is a software that provides Power on Authentication for your Mac and encrypts hard disks or partitions of your Mac.

With **Power-on Authentication (POA)** a user is required to authenticate during the pre-boot phase; that is, before the operating system is started. Only when the user has been properly authenticated in the POA, the actual operating system is started and the user is logged on automatically to OS X if the system is configured for auto-logon.

Sophos SafeGuard Disk Encryption encrypts data on a Mac in a partition based manner. A SafeGuard Admin defines the hard disks or partitions that are to be encrypted. A SafeGuard User is not allowed to change these settings.

The files on an encrypted partition are encrypted transparently. You will not see any prompts for encryption or decryption when opening, editing, and saving files. When you open the files, they will be decrypted and you can edit them. On closing or saving the files, they will be encrypted again.

Note: After Sophos SafeGuard Disk Encryption for Mac has been installed the system partition where the product is installed receives a new icon (the disk icon with the SafeGuard shield). This icon indicates only that SafeGuard is installed, this partition is not encrypted! Data partitions receive this icon when they have been encrypted.

2 Sophos SafeGuard Disk Encryption system menu

The Sophos SafeGuard Disk Encryption system menu is represented by an icon on the right end of the menu bar. This menu gives you quick access to the features of Sophos SafeGuard Disk Encryption and shows the status of Sophos SafeGuard Disk Encryption.

The Sophos SafeGuard Disk Encryption system menu contains the following menu options:

- **About SafeGuard:** View information about Sophos SafeGuard Disk Encryption, including version and copyright information.
- **Disk Management:** Open the disk management. Only SafeGuard Admins are allowed to change disk management settings. SafeGuard Users are only allowed to view the settings.
- **User Management:** Open the user management. Only SafeGuard Admins are allowed to change user management settings. SafeGuard Users are only allowed to view the settings.
- **Status information:** In case of running encryption/decryption, status information includes the name of the partition and encryption/decryption progress.

3 Power-on Authentication

With **Power-on Authentication (POA)**, a user is required to authenticate during the pre-boot phase; that is, before the operating system is started. Only when the user has been properly authenticated in the POA, the actual operating system is started and the user is logged on automatically to OS X when auto-logon is configured.

As long as there are no SafeGuard Users present the POA will show the "Secured by SOPHOS" logo and then continue booting the operating system after about one second.

If SafeGuard users are in place, the authentication screen will appear. Power-on Authentication is always enabled, regardless if there are encrypted partitions or not.

3.1 Logging on at POA

Authentication at POA is done using Sophos SafeGuard Disk Encryption user credentials. These credentials have to be provided by a system administrator or the person who installed and/or configured Sophos SafeGuard Disk Encryption on your Mac.

Authentication is done by entering the SafeGuard user name and password in the edit fields.

If the Sophos SafeGuard Disk Encryption user account is accepted, logon to the operating system is done automatically, if configured.

3.2 Troubleshooting at POA

Sophos SafeGuard Disk Encryption offers troubleshooting options at Power-on Authentication:

- Recover
- Permanently decrypt partition
- Show log

These options will help you in case of any issues like: your Sophos SafeGuard Disk Encryption installation is damaged, the operating system does not start, etc.

Choosing **Troubleshooting** in the authentication dialog opens a menu with the troubleshooting options.

3.2.1 Recover

Besides recovering forgotten passwords of user accounts Sophos SafeGuard Disk Encryption provides more recovery options to assure that even damaged systems can be recovered easily.

A prerequisite for every recovery action is that kernel and authentication data are exported immediately after the software has been installed and users have been created.

Note: In case of the users authentication data you have to export these data each time you add users or modify their credentials in order to keep your back-ups up to date. In case you updated the Sophos SafeGuard Disk Encryption software on your Mac it is also necessary to export the kernel again.

3.2.1.1 Creating recovery media

To export the recovery data:

1. Choose the Sophos SafeGuard Disk Encryption icon and click **User Management**.
2. Enter your SafeGuard credentials (Admin, User, Recovery) and click **OK**.
3. The **Action** menu (looks like a gear) contains three options:

Create machine independent recovery media

Choose **Create machine independent recovery media** if you want to create universal recovery media for your Macs. This media lets you recover every machine as long as their authentication data is OK.

To create the media click **Create machine independent recovery media**. In the dialog displayed, choose the desired location, leave the **Save to Disk Image** option checked and click **Create machine independent recovery media**.

Note: Regardless of which storage location you have chosen (already on USB stick or temporarily on the hard disk of your Mac), you have to "restore" the disk image to the USB stick's root using your Mac's Disk Utility afterwards. This ensures that the recovery media is working properly.

Export Authentication Data

Choose **Export Authentication Data** to back up all of your user credentials. You should store them in a secure location where you can access them in case of emergency.

Create machine specific recovery media

Choose **Create machine specific recovery media** if you are a single user, who wants to create a recovery package that contains every data needed in an emergency case. The procedure is the same as creating a machine-independent recovery media.

These recovery actions can all be initiated at the Power-on Authentication.

3.2.1.2 How to recover

In general, recovery can be necessary for two reasons:

- Corrupted authentication data. This will be indicated by a message displayed at Power-on Authentication or from the operating system.
- Kernel problems which for example can result from bad sectors on your hard disk.

Corrupted authentication data

1. Attach an USB stick that contains the exported authentication data and start your Mac.
2. At Power-on Authentication choose **Troubleshooting** and select **Recover** from the **Troubleshooting** menu.
3. Sophos SafeGuard Disk Encryption searches all attached removable media devices for authentication and key data, which have to reside in the root directory.
4. If found, you have to confirm that you want to recover the authentication data. After that, the local authentication data is replaced with those from the USB stick.
5. After you have confirmed successful recovery go back to Power-on Authentication and log on as usual.

Kernel recovery

In this case, you have to launch Power-on Authentication from your recovery media.

1. Attach your recovery media and boot your Mac from this media.
2. When the hard disk symbol with a white cross on a green background appears, click it.
3. The Power-on Authentication launched from the recovery media appears.
4. Choose **Troubleshooting** and select the **Recover** option from the **Troubleshooting** menu.
5. Select the **Kernel partition** option from the **Recovery** menu. Selecting **Authentication data** would do the same as described under **Corrupted authentication data**.
6. After you have confirmed successful recovery go back to Power-on Authentication and log on as usual.

3.2.2 Permanently decrypt partition

Permanently decrypting a partition can be necessary for example, if the operating system cannot be started anymore, but you need to have access to encrypted data. This way it is possible to decrypt partitions without the need of running the operating system.

Choosing this option displays a list of all available partitions on your Mac.

You can select a partition by pressing the SPACE key. You have to authorize decryption by entering SafeGuard Admin credentials in the edit fields.

Selecting **Decrypt** starts decryption of the selected partition.

3.2.3 Show log

Choosing this option displays the log file which can help you to analyze problems.

It is possible to export the content of the log to a file on a USB stick.

To do so, attach a USB stick to your Mac and select **Export**. The log file will automatically be stored in the root directory of the USB stick.

Note: The USB stick needs to have a FAT partition.

4 User management

The Sophos SafeGuard Disk Encryption user management is based on three types of different users:

- Type: **Admin**
- Type: **User**
- Type: **Recovery**

These roles are unrelated to the system accounts and reflect a kind of "cryptographic SafeGuard User".

4.1 Admin user

The Admin user is the only role that can be used to:

- **Add** users of any type
- **Delete** users of any type
- **Change** the encryption state of partitions

There must always be one Admin user. When the first user is created, this user must always be an Admin user. This is enforced by the SafeGuard user management and is the prerequisite for all administration tasks. When users are deleted, it is not possible to delete the last Admin user, if more than one have been created.

4.1.1 Creating the first Sophos SafeGuard Disk Encryption Admin user

1. Choose the Sophos SafeGuard Disk Encryption icon and click **User Management**.
2. Enter a name for the Admin user.
3. Enter the password in the **Password** and **Confirm Password** fields. Sophos SafeGuard Disk Encryption accepts only passwords with eight or more characters (up to 127). Checking the **Show Password** option makes the entered password visible.
4. Click **OK**.

4.2 User

The **User** type reflects a normal user. Users of this type are not allowed to create/delete any other users or to manage disks, but they are allowed to view the current settings on their Macs. They are allowed to authenticate at the POA.

4.2.1 Creating a SafeGuard User

For creating a SafeGuard User you have to know SafeGuard Admin credentials.

1. Choose Sophos SafeGuard Disk Encryption icon and click **User Management**.
2. Enter your SafeGuard credentials (Admin, User, Recovery) and click **OK**.
3. Choose **Users** in the management pane.
4. Click the **Add (+)** button below the list of user accounts.
5. Choose **User** from the **Add User** pop-up menu.
6. Enter a name for the SafeGuard User.
7. Enter the User password in the **Password** and **Confirm Password** fields. Sophos SafeGuard Disk Encryption accepts only password with eight or more characters (up to 127). Checking the **Show Password** option makes the entered password visible.
8. Enter your Admin credentials in the **Admin Name** and **Admin Password** fields.
9. Click **OK**.

The new SafeGuard User is now displayed in the list of accounts and these credentials can now be used to authenticate at POA.

4.3 Recovery user

A Recovery user is used to recover a forgotten password of an existing SafeGuard user. A Recovery user cannot be used to recover an Admin user or different Recovery users.

A Recovery user can be understood as a one time user. Each Recovery user is bound to a specific SafeGuard user. This means that a Recovery user can only recover a specific SafeGuard user. If the SafeGuard user is deleted, his Recovery users are also removed.

Recovery Users are allowed to authenticate at the POA but will be removed after they have been used to recover the password of a SafeGuard User.

Note: We recommend to create several Recovery Users for each SafeGuard User to assure that there is always a Recovery User left in case the user has forgotten his or her password.

4.3.1 Creating a Recovery user

For creating a SafeGuard Recovery user you have to know SafeGuard Admin credentials.

1. Choose Sophos SafeGuard Disk Encryption icon and click **User Management**.
2. Enter your SafeGuard credentials (Admin, User, Recovery) and click **OK**.
3. Choose **Users** in the management pane.
4. Click the **Add (+)** button below the list of user accounts.
5. Choose **Recovery** from the **Add User** pop-up menu.
6. Select an existing SafeGuard user from the pop-up menu. The Recovery user can only be used to recover the password of this specific user.
7. Enter a name for the Recovery user.
8. Enter the password for the Recovery user in the **Password** and **Confirm Password** fields. Sophos SafeGuard Disk Encryption accepts only passwords with eight or more characters. Checking the **Show Password** option makes the entered password visible.
9. Enter your Admin credentials in the **Admin Name** and **Admin Password** fields.
10. Click **OK**.

The new Recovery user is now displayed in the list of accounts. This Recovery user can now be used to authenticate at POA and recover a user's forgotten password.

4.3.2 Recovering a forgotten SafeGuard user's password

1. Log on at POA using your SafeGuard Admin credentials or use the credentials of the corresponding Recovery user.
2. Choose Sophos SafeGuard Disk Encryption icon and click **User Management**.
3. Enter your SafeGuard credentials (Admin, User, Recovery) and click **OK**.
4. Choose **Users** in the management pane.
5. Choose **Recover User** on the right-hand side of the SafeGuard user account for which you want to recover the password.

6. Enter a new password in the **New Password** and **Confirm Password** fields.
7. Enter name and password of the Recovery user in the **Recovery name** and **Recovery Password** edit fields.
8. Click **OK**.

The password of the SafeGuard User is reset. It can now be used to authenticate at POA.

Note: The Recovery user is deleted from the list of accounts. Make sure that there is always a Recovery user left for each account. If necessary, create a new one. Without a recovery user there is no way to recover a forgotten password.

5 Disk management

Sophos SafeGuard Disk Encryption lets you encrypt the hard disk or partitions of your Mac. Every disk management task (encrypt/decrypt/pause/resume) requires authentication as a SafeGuard Admin.

The Sophos SafeGuard Disk Encryption system menu on the right end of the menu bar displays the status of running encryption/decryption tasks.

5.1 Encrypting a partition

Before you begin to encrypt a data partition ensure that all files on this partition are closed.

1. Choose Sophos SafeGuard Disk Encryption icon and click **Disk Management**.
2. Enter your SafeGuard Admin credentials and click **OK**.
3. Choose **Partitions** in the management pane. All available partitions are displayed.
4. Click **Encrypt** right beside the partition you want to encrypt.
5. Encryption of the selected partitions starts immediately. To enhance encryption speed, check the **Fast Mode** option in the lower left corner of the **Disk management** pane.

You can continue working on the data partition during the encryption process.

Note: We recommend not to install updates and initially encrypt/finally decrypt a machine simultaneously as installations can be very slow in this case.

Encryption/decryption can be paused by clicking the **Pause** button on the right end of the progress bar. To resume encryption, click the **Resume** button which is displayed when encryption has been paused. For both actions, you must authenticate as a SafeGuard Admin.

Paused encryption/decryption tasks are resumed automatically after you restart your Mac.

Note: Do not start encryption for unmounted partitions and do not unmount a partition during encryption. Both can result in data loss.

5.2 Decrypting a partition

Make sure that all files on the data partition to be decrypted are closed while decryption is performed.

1. Choose Sophos SafeGuard Disk Encryption icon and click **Disk Management**.

2. Enter your SafeGuard Admin credentials and click **OK**.
3. Choose **Partitions** in the management pane. All available partitions are displayed.
4. Click **Decrypt** right beside the partition you want to decrypt.
5. Decryption of the selected partition starts immediately.

Decrypting partitions is also possible at Power-on Authentication. This can be helpful for example, when the operating system cannot be started.

Choosing **Troubleshooting > Permanently decrypt partition** lets you decrypt the partitions of your Mac.

Note: Do not start decryption of unmounted partitions and do not unmount a partition during decryption. Both can result in data loss.

6 Using Sophos SafeGuard Disk Encryption via Terminal

You can use Sophos SafeGuard Disk Encryption via Terminal, the Mac OS X command-line interface.

6.1 Commands

The following commands are available via "sgadmin" command line:

```
sgadmin --help | -h

sgadmin --status

sgadmin --add-user
    --type "user | admin"
    [--user "username"]
    [--password "password"]
    [--confirm-password "confirm password"]
    [--authenticate-user "admin username"]
    [--authenticate-password "admin password"]

sgadmin --add-recovery-user
    --user-to-recover "username"
    [--user "username"]
    [--password "password"]
    [--confirm-password "confirm password"]
    [--authenticate-user "admin username"]
    [--authenticate-password "admin password"]

sgadmin --add-recovery-users
    --user-to-recover "username"
    [--count "number of users"]
    [--authenticate-user "admin username"]
    [--authenticate-password "admin password"]

sgadmin --remove-user
    [--user "username"]
    [--authenticate-user "admin username"]
    [--authenticate-password "admin password"]

sgadmin --list-users
    [--authenticate-user "username"]
    [--authenticate-password "password"]

sgadmin --change-password
    [--user "username"]
    [--old-password "old password"]
    [--new-password "new password"]
    [--confirm-password "confirm password"]
```

```

sgadmin --recover-password
    [--user "username"]
    [--new-password "new password"]
    [--confirm-password "confirm password"]
    [--recovery-user "recovery username"]
    [--recovery-password "recovery password"]

sgadmin --backup-authentication
    --target "/path/to/target/folder"

sgadmin --backup-kernel
    --target "/path/to/target/folder"
    [--include-authentication]
    [--create-dmg]

sgadmin --encrypt "uuid | index | system | all"
    [--authenticate-user "admin username"]
    [--authenticate-password "admin password"]

sgadmin --decrypt "uuid | index | system | all"
    [--authenticate-user "admin username"]
    [--authenticate-password "admin password"]

sgadmin --pause "uuid | index | all"
    [--authenticate-user "admin username"]
    [--authenticate-password "admin password"]

sgadmin --resume "uuid | index | all"
    [--authenticate-user "admin username"]
    [--authenticate-password "admin password"]

sgadmin --enable-fast

sgadmin --disable-fast

sudo sgadmin --set-boot

```

6.2 Command descriptions

The following table describes all commands and options. Everything in square brackets "[...]" is optional. User names and passwords are queried interactively, if not provided by the options. User names are entered "visibly" and passwords "invisibly".

Command	Description
--help -h	Displays the help text.
--status	Displays status information. The index information displayed by <code>sgadmin --status</code> is dynamic. This means that depending on the number of mounted partitions, index information may vary.

Command	Description
--add-user	<p>The "add-user" command is used to add a user to the machine. The only required parameter is "type". The user name and password as well as authenticate user and authenticate password can be passed on by options or will be queried interactively. The first user added must be an Admin. When the first user is added, it is not necessary to specify auth-user and auth-password.</p> <p>Options:</p> <ul style="list-style-type: none"> ■ --type: User type (Admin, User) ■ --user: Name of the user to add ■ --password: Password of the user to add ■ --authenticate-user: "Admin" user required to authenticate (if not the first user) ■ --authenticate-password: "Admin" password required to authenticate (if not the first user)
--add-recovery-user	<p>Adds a Recovery user for a specific user. Options:</p> <ul style="list-style-type: none"> ■ --user-to-recover: Name of the user to recover ■ --recovery-user: Name of the recovery user to add ■ --recovery-password: Password of the user to add ■ --confirm-password: Confirm the password ■ --authenticate-user: "Admin" user required to authenticate ■ --authenticate-password: "Admin" password required to authenticate
--add-recovery-users	<p>The "count" parameter gives the numbers of Recovery users to be created (random user name as well as random password) and reported back via "stdout". Options:</p> <ul style="list-style-type: none"> ■ --user-to-recover: Name of the user to recover ■ --count: Number of users ■ --authenticate-user: "Admin" user required to authenticate ■ --authenticate-password: "Admin" password required to authenticate

Command	Description
--remove-user	Removes a user. Options: <ul style="list-style-type: none"> ■ --user: Name of the user to remove ■ --authenticate-user: "Admin" user required to authenticate ■ --authenticate-password: "Admin" password required to authenticate
--list-users	Lists all "SafeGuard" users on the machine. Options: <ul style="list-style-type: none"> ■ --authenticate-user: Any user which has access to the machine ■ --authenticate-password: Password of the user
--change-password	Changes the password of a user. Options: <ul style="list-style-type: none"> ■ --recover-password ■ --old-password: Old password of the user ■ --new-password: New password of the user ■ --confirm-password: Confirmation of the new password
--recover-password	Recovers the password of a user. Options: <ul style="list-style-type: none"> ■ --user: Name of the user to recover ■ --new-password: New password of the user ■ --confirm-password: Confirmation of the new password ■ --recovery-user: Name of the Recovery User used for recovery (will be deleted after successful recovery) ■ --recovery-password: Password of the recovery user
--backup-authentication	Backs up authentication and key data used to unlock the machine. Options: <ul style="list-style-type: none"> ■ --target: Full path to the target folder (must be a folder)

Command	Description
--backup-kernel	<p>Backs up pre-boot Kernel (POA and boot loader). Options:</p> <ul style="list-style-type: none"> ■ --target: Full path to the target folder (must be a folder) ■ --include-authentication: Also include authentication and key data ■ --create-dmg: Create a disk image (.dmg). This is called "sgRecoveryMedia.dmg"
--encrypt	<p>Encrypts a partition. You can either specify a partition uuid or an index. Both can be retrieved with the --status command. It is also possible to use the keywords "system" and "all". In these cases, either the system or all partitions will be encrypted. Options:</p> <ul style="list-style-type: none"> ■ --authenticate-user: "Admin" user required to authenticate ■ --authenticate-password: "Admin" password required to authenticate
--decrypt	<p>Decrypts a partition. You can either specify a partition uuid or an index. Both can be retrieved with the --status command. It is also possible to use the keywords "system" and "all". In these cases, either the system or all partitions will be decrypted. Options:</p> <ul style="list-style-type: none"> ■ --authenticate-user: "Admin" user required to authenticate ■ --authenticate-password: "Admin" password required to authenticate
--pause	<p>Pauses an encrypt/decrypt operation. You can either specify a partition uuid or an index. Both can be retrieved with the --status command. It is also possible to use the keyword "all". In these cases, either operations on the system or all partitions will be paused. Options:</p> <ul style="list-style-type: none"> ■ --authenticate-user: "Admin" user required to authenticate ■ --authenticate-password: "Admin" password required to authenticate

Command	Description
--resume	<p>Resumes an encrypt/decrypt operation. You can either specify a partition uuid or an index. Both can be retrieved with the --status command. It is also possible to use the keyword "all". In these cases, either operations on the system or all partitions will be resumed. Options:</p> <ul style="list-style-type: none">■ --authenticate-user: "Admin" user required to authenticate■ --authenticate-password: "Admin" password required to authenticate
--enable-fast	<p>Tunes all encrypt/decrypt operations to run as fast as possible. By default, the actual speed of those operations is throttled. If this command is executed, operations will not be throttled. This should increase overall speed by 20%-30%.</p>
--disable-fast	<p>Enables default behavior (throttling) for encrypt/decrypt operations.</p>
--set-boot	<p>Sets the default operating system back to OS X.</p>

7 Time Machine backups

The following components of Sophos SafeGuard Disk Encryption should be excluded from Time Machine Backups:

- /.com.sophos
- /System/Library/Extensions/sgbiodrv.kext
- /usr/sbin/sgd
- /usr/bin/sgadmin
- /Library/Sophos SafeGuard
- /Library/LaunchDaemons/com.sophos.sgd.plist
- /Library/LaunchAgents/com.sophos.sguimenu.plist
- /Library/LaunchAgents/com.sophos.sgsynclang.plist
- /Applications/sgui.app

8 Supported Hardware and Configurations

- **Hardware** (Intel-based 64bit CPU only)

- MacBook
- MacBook Pro
- MacBook Air
- iMac
- Mac mini
- Mac Pro

- **EFI**

- EFI32 (firmware)
- EFI64 (firmware)

With the following terminal command, the EFI firmware can be verified:

```
"ioreg -l -p IODeviceTree | grep firmware-abi"
```

The return value should be "firmware-abi" = <"EFI64" > or "firmware-abi" = <"EFI32" >.

- **Operating system**

- 10.7 (Lion) recent patch level, 32 or 64 bit kernel

- **Update of Sophos SafeGuard Disk Encryption for Mac**

- As Sophos SafeGuard Disk Encryption for Mac 5.55 is the first version for Mac OS X 10.7 (Lion), an update from previous versions is not possible.

- **Update of Mac OS X to version 10.7 (Lion)**

- To upgrade from Mac OS X 10.6 (Snow Leopard) to 10.7 (Lion), you need to uninstall Sophos SafeGuard Disk Encryption for Mac 5.50.x first. This step includes a final decryption of the encrypted partitions.

After the successful update to Lion, you need to install Sophos SafeGuard Disk Encryption 5.55.x and encrypt the partitions again.

It is not necessary to change your exclude rules for your time machine configuration for this.

8.1 Bootcamp Support

It is required to set up a machine with a Bootcamp partition prior to installing Sophos SafeGuard Disk Encryption. It is not supported to set up or remove Bootcamp after installing Sophos SafeGuard Disk Encryption. Note that it is not supported to change/resize the partition layout after installing SafeGuard.

If the default operating system is changed from OS X to Windows it cannot be set back to OS X neither with Windows Bootcamp Control Panel nor with OS X Startup Disk Utility. This has to be done using the functionality provided by Sophos SafeGuard Disk Encryption.

You can set the default boot system to OS X in the following ways:

1. via user interface:

- Open **SafeGuard Disk Management**.
- Open the **Edit** menu and select **Boot this operating system by default**. It is required to authenticate as an OS X Administrator.

2. via Terminal

- Open a **Terminal** and enter “`sudo sgadmin --set-boot`”. Note that OS X Administrator authentication is required.

9 Unsupported hardware, configurations and operations

- **Hardware**
 - PowerPC based hardware
- **Operating system**
 - 10.6 and prior
- **Bootcamp + SafeGuard Enterprise/SafeGuard Easy for Windows**
 - SafeGuard Enterprise for Windows does not support Apple hardware and cannot be installed in a Bootcamp/Windows environment. This restriction is valid until explicitly stated otherwise in the SafeGuard Enterprise for Windows documentation.
- **The following LIMITATIONS apply to the product:**
 - Sophos SafeGuard Disk Encryption for Mac does not support multi-boot systems, this means multiple installations of OS X on the same Mac.

 - **Sophos SafeGuard Disk Encryption for Mac and Mac OS X 10.7 (Lion)**
FileVault cannot be installed at the same point in time. If FileVault shall be used, no local partition must be encrypted by FileVault. If FileVault shall be used, Sophos SafeGuard Disk Encryption for Mac must not be installed.

 - Do not install the software on systems with more than 50 partitions.

 - We recommend not to encrypt more than five partitions simultaneously.

 - **Keyboard:** The keyboard translation code only deals with normal keys and keys with a shift modifier. Non-numeric keypad keys cannot be guaranteed to give the same character sequence when the keyboard is changed from one layout to another. So only use "0-9" from that block. It is due to EFI only returning a US ANSI character equivalent and no modifier keys. During translation, the normal keyboard key takes precedence over the numeric keypad key. This affects the non-numeric keys on the numeric keypad, this means the '=', '/', ', -', '+ ' keys. These keys may translate into a different character due to the keyboard layout. For example, on a German keyboard the numeric keypad " key will translate into the keyboard '(' character. The code has been developed and tested with the following keyboards: US, French, German. There is no guarantee that other keyboards work.

- **Partitioning:** After Sophos SafeGuard Disk Encryption for Mac has been installed it is not possible/supported to change the partitioning layout. This means it is not allowed to change anything with "gpt" or "diskutil". If someone repartitions the machine, this machine will be lost and will need to be reinstalled.
- **Formatting:** Formatting of encrypted partitions is not supported. If you want to remove all data, we recommend that you delete the files or decrypt the partition, format it and encrypt it again. Note that only HFS+ partitions are supported for encryption.
- **Target Disk Mode:** The usage of Target Disk Mode is not supported, if both the local machine and the target disk are encrypted. It is supported, if the local machine is not encrypted and the target disk is, or if the local machine is encrypted and the target disk is not.
- **diskutil from a system started via network boot:** Do not use diskutil from a system started via network boot while local partitions are encrypted. In this case diskutil does not recognize the encrypted partitions and wants to initialize them. Doing so results in data loss.
- **Erasing partitions:** Erasing a partition while an initial encryption or a final decryption operation is performed is not supported. Also, erasing encrypted partitions is not supported. Partitions have to be decrypted first and can then be encrypted again.
- **Unmounted partitions and encryption/decryption:** Starting initial encryption or final decryption for partitions that are not mounted is not supported. Unmounting a partition while it is encrypting or decrypting is also not supported. Doing so may result in data loss.
- **OS upgrades (like from 10.6 to 10.7) are not supported:** It is necessary to decrypt the partitions of your Mac first and then to uninstall Sophos SafeGuard Disk Encryption for Mac. Afterwards, you can upgrade the operating system, install Sophos SafeGuard Disk Encryption for Mac released for 10.7 and encrypt the partitions again.
- **Deep Sleep:** When Sophos SafeGuard Disk Encryption for Mac is installed the hibernation feature "Deep Sleep" is not supported and is disabled. Some applications do not auto-save their data when the sleep mode is activated. In case the sleep mode is used for an extended period while not being connected to power and such an application is open with unsaved data, data might be lost.
- **Bad sectors:** We recommend not to install the product if there are bad sectors on your hard disk. Initial encryption does not stop when bad sectors are encountered, but a log entry is created in the kernel log.

- **Initial encryption/final decryption on data partitions:** Before you begin to encrypt a data partition ensure that all files on this partition are closed. Make sure that all files on the data partition to be decrypted are closed while decryption is performed.

10 Technical support

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

- Visit the SophosTalk forum at <http://community.sophos.com/> and search for other users who are experiencing the same problem.
- Visit the Sophos support knowledgebase at <http://www.sophos.com/support/>
- Download the product documentation at <http://www.sophos.com/support/docs/>
- Send an email to support@sophos.com, including your Sophos software version number(s), operating system(s) and patch level(s), and the text of any error messages.

11 Copyright

Copyright © 2010 - 2011 Sophos Group. All rights reserved. SafeGuard is a registered trademark of Sophos Group.

All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the documentation can be reproduced in accordance with the licence terms or you otherwise have the prior permission in writing of the copyright owner.

11.1 Disclaimer and Copyright for 3rd Party Software

Portions of this software are copyright © 2010 The FreeType Project (www.freetype.org). All rights reserved.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)

Gladman AES

Copyright (c) 1998-2007, Brian Gladman, Worcester, UK. All rights reserved.

LICENSE TERMS

The free distribution and use of this software is allowed (with or without changes) provided that:

1. source code distributions include the above copyright notice, this list of conditions and the following disclaimer;
2. binary distributions include the above copyright notice, this list of conditions and the following disclaimer in their documentation;
3. the name of the copyright holder is not used to endorse products built using this software without specific written permission.

DISCLAIMER

This software is provided 'as is' with no explicit or implied warranties in respect of its properties, including, but not limited to, correctness and/or fitness for purpose.

EDK

Copyright (c) 2008

Intel Corporation.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by Intel Corporation and its contributors.
4. Neither the name of Intel Corporation or its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY INTEL CORPORATION AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL INTEL CORPORATION OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (c) 1988, 1993

The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by the University of California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Freetype

Copyright 2000 Computing Research Labs, New Mexico State University

Copyright 2001, 2002, 2003, 2004 Francesco Zappa Nardelli

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE COMPUTING RESEARCH LAB OR NEW MEXICO STATE UNIVERSITY BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING

FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

FreeType font driver for bdf files

Copyright (C) 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008 by Francesco Zappa Nardelli

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

FreeType font driver for pcf fonts

Copyright (C) 2000, 2001, 2002 by Francesco Zappa Nardelli

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN

CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Copyright (c) 2000

Intel Corporation.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by Intel Corporation and its contributors.
4. Neither the name of Intel Corporation or its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY INTEL CORPORATION AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL INTEL CORPORATION OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (c) 1992, 1993

The Regents of the University of California. All rights reserved.

Portions copyright (c) 1999, 2000

Intel Corporation.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by the University of California, Berkeley, Intel Corporation, and its contributors.
4. Neither the name of University, Intel Corporation, or their respective contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS, INTEL CORPORATION AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS, INTEL CORPORATION OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (c) 1990, 1993

The Regents of the University of California. All rights reserved.

This code is derived from software contributed to Berkeley by Chris Torek.

Portions copyright (c) 1999, 2000

Intel Corporation.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by the University of California, Berkeley, Intel Corporation, and its contributors.
4. Neither the name of University, Intel Corporation, or their respective contributors may be used to endorse or promote products derived from this software without specific prior written permission.
5. THIS SOFTWARE IS PROVIDED BY THE REGENTS, INTEL CORPORATION AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS, INTEL CORPORATION OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Zlib, Part of FreeType

zlib.h -- interface of the 'zlib' general purpose compression library version 1.1.4, March 11th, 2002

Copyright (C) 1995-2002 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly

jloup@gzip.org

Mark Adler

madler@alumni.caltech.edu

The data format used by the zlib library is described by RFCs (Request for Comments) 1950 to 1952 in the files <ftp://ds.internic.net/rfc/rfc1950.txt> (zlib format), [rfc1951.txt](ftp://ds.internic.net/rfc/rfc1951.txt) (deflate format) and [rfc1952.txt](ftp://ds.internic.net/rfc/rfc1952.txt) (gzip format).

PCF, Part of FreeType

Copyright (C) 2000 by Francesco Zappa Nardelli

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

GptLib

Copyright (c) 2002 Marcel Moolenaar

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.