Sophos SafeGuard Disk Encryption for Mac and the Casper Suite

Deploying, Activating, and Reporting on Sophos SafeGuard Disk Encryption for Mac with the Casper Suite

Technical Paper
March 2011

JAMF Software, LLC
© 2011 JAMF Software, LLC. All rights reserved.

JAMF Software has made all efforts to ensure that this guide is accurate.

JAMF Software
1011 Washington Ave. South
Suite 350
Minneapolis, MN 55415
(612) 605-6625

Casper Admin, Casper Remote, the Casper Suite, JAMF Software, the JAMF Software logo, the JAMF Software Server (JSS), and the JSS Setup Utility are trademarks of JAMF Software, LLC, registered in the U.S. and other countries.

Sophos and SafeGuard are registered trademarks of Sophos PLC, Sophos Group and Utimaco Safeware AG, as applicable.

All other product and service names mentioned are the trademarks of their respective companies.

Contents

Introduction

Target Audience

This guide is designed for Casper Suite administrators who plan to use Sophos SafeGuard® Disk Encryption for Mac.

What's in This Guide

This guide provides step-by-step instructions for deploying, activating, and reporting on SafeGuard with the Casper Suite. Be sure to review the information in the "Requirements" section before you begin.

Important Concepts

Before using this guide, make sure you are familiar with the following Casper Suite-related concepts:

- Package and script management
- Deployment
- Extension attributes
- Advanced computer searches
- Smart computer groups

Additional Resources

For more information on applications, concepts, and processes related to the Casper Suite, see the *Casper Suite Administrator's Guide*, available for download at:

http://jamfsoftware.com/resources/documentation

For more information on Sophos SafeGuard Disk Encryption for Mac, go to:

http://www.sophos.com/products/enterprise/encryption/disk-encryption-for-mac

Overview

The Casper Suite is the complete solution for Mac administrators who rely on Sophos SafeGuard® Disk Encryption for Mac to protect the data in their environments. In addition to deploying and updating SafeGuard, the Casper Suite offers script-based activation and disk encryption reporting to ensure that each disk is fully encrypted and compliant with security standards.

Requirements

To administer SafeGuard using the instructions in this guide, you need:

- The Casper Suite v8.1 or later running in your environment
- Sophos SafeGuard installer media, v05.50.00 or later
- Access to the JAMF Software Server (JSS)
- Casper Admin
- Casper Remote
- Casper Suite Resource Kit, available for download at:

    http://www.jamfsoftware.com/downloads/ResourceKit.dmg

Deploying SafeGuard

Deploying SafeGuard involves two simple steps:

1. Uploading the SafeGuard Installer to the JSS.

2. Deploying the installer.

Uploading the SafeGuard Installer

First, upload the SafeGuard Installer to the JSS using the Casper Admin application.

To upload the SafeGuard Installer:

1. Mount the SafeGuard Installer disk image.

2. Open Casper Admin.

3. Log in using credentials for a JSS administrator account.

4. Drag the SafeGuard Installer into Casper Admin.

5. Double-click the installer package in the list of items, and then click the **Info** tab.

6. Enter a new display name for the package if desired.

7. Use the **Category** pop-up menu to assign the package to a category.

8. Click the **Options** tab.

9. Assign the package a priority by choosing from the **Priority** pop-up menu.

    The recommended priority for installers is "10". For more information on priorities, see the "Changing Package Attributes" section in the *Casper Suite Administrator's Guide*.

10. Select the **Requires Reboot** option.
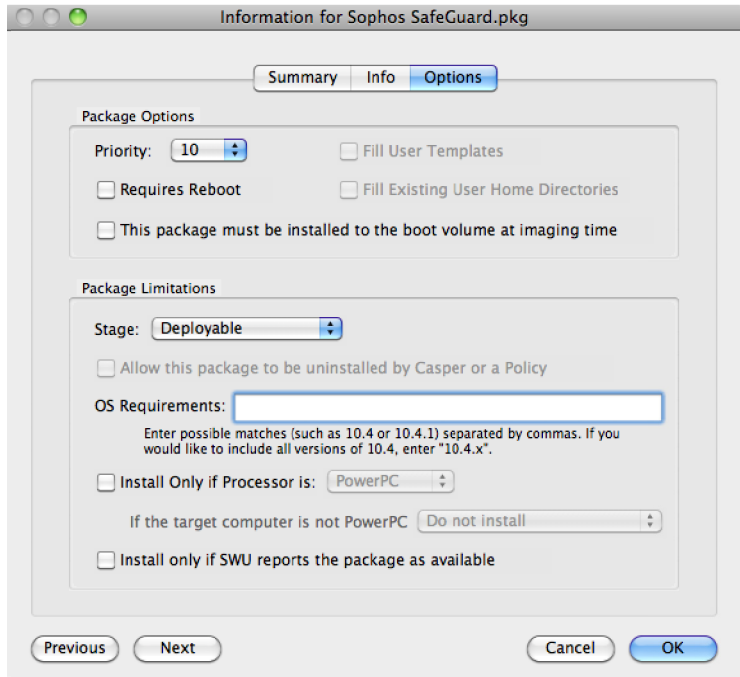
11. If you plan to deploy the package during imaging, select the **This package must be installed to the boot volume at imaging time** checkbox.

12. Click the **OK** button.

13. Type **Command + S** to save your changes, and then quit the application.

Deploying the SafeGuard Installer

There are several ways to deploy the SafeGuard Installer:

*   Using a policy
*   Using Casper Remote
*   During imaging
*   Using the Self Service application

Deploying the SafeGuard Installer using a policy, Casper Remote, or during imaging automatically updates inventory in the JSS when the software is installed.

For instructions on making the SafeGuard Installer available through Self Service, see the "Making Policies Available Through Self Service" section in the *Casper Suite Administrator's Guide*.

To deploy SafeGuard using a policy:

1. Log in to the JSS with a web browser.

2. Click the **Management** tab.

3. Click the **Policies** link.

4. Click the **Create Policy** button in the toolbar.

5. Verify that the **Install or uninstall a package** option is selected and click **Continue**.

6. Follow the onscreen instructions to configure the rest of the policy.

7. On the **Conclusion** pane, click the **Edit Manually** button.

8. Click the **Reboot** tab.

9. In the **If Nobody is Logged In** pane, select the **Reboot immediately** option.

10. In the **If Anybody is Logged In** pane, select the **Reboot** option.

11. Choose "Currently Selected Startup Disk (No Bless)" from the **Reboot To** pop-up menu.

12. Click **Save**.
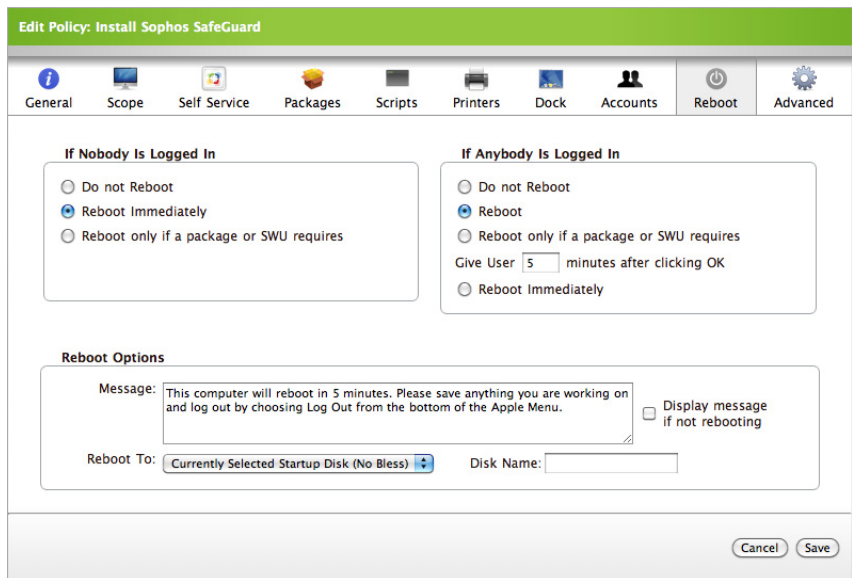

The installer is deployed to computers in the scope the next time they check in with the JSS.

To deploy SafeGuard using Casper Remote:

1. Open Casper Remote.

2. Log in using credentials for a JSS administrator account.

3. On the **Computers** tab, locate the computers you want to deploy the package to and select the checkbox next to each one.

4. Click the **Packages** tab.

5. In the **Packages** list, locate the SafeGuard Installer and select the checkbox next to it.

6. Click the **Reboot** tab.

7. In the **If nobody is logged In** pane, select the **Reboot immediately** option.

8. In the **If anybody is logged In** pane, select the **Reboot** option.

9. Choose "Currently Selected Startup Disk (No Bless)" from the **Reboot To** pop-up menu.
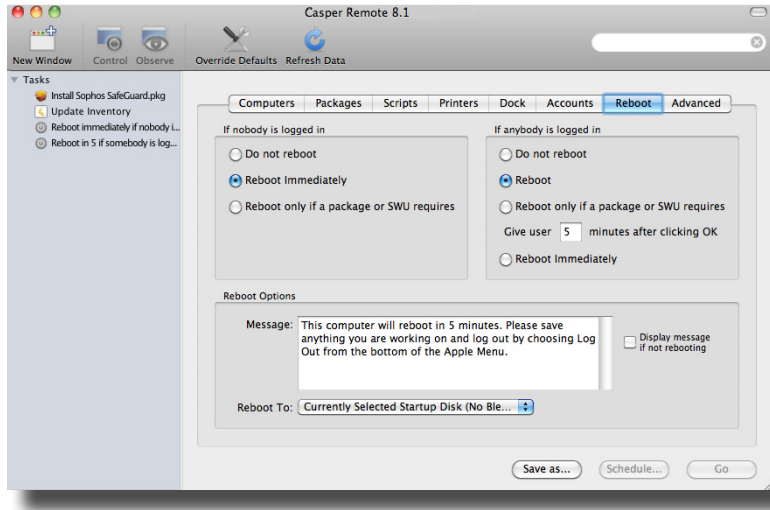
10. Click **Go** to initiate the deployment.

To deploy SafeGuard during imaging:

> *Note:* To deploy a package during imaging, you must have the **This package must be installed to the boot volume at imaging time** option selected for the package in Casper Admin. For more information on selecting this option, see the instructions in "Uploading the SafeGuard Installer" section in this document.

1. Open Casper Admin.

2. Log in using credentials for a JSS administrator account.

3. Drag the SafeGuard Installer from the list of packages to the configuration you plan to use for imaging in the sidebar.

4. Type **Command + S** to save your changes, and then quit the application.

   The installer is deployed the next time the configuration is used to image computers. Casper Imaging automatically detects that the package requires a reboot and reboots the computers after SafeGuard is installed.

Activating SafeGuard

There is a script in the Casper Suite Resource Kit that allows you to configure settings for and activate SafeGuard on remote computers.

This section explains how to activate SafeGuard using the following steps:

1. Customize the SafeGuard activation script.

2. Upload the script to the JSS.

3. Run the script using a policy.

Customizing the SafeGuard Activation Script

There are several parameters that you can customize in the SafeGuard activation script. Customizing these parameters allows you to:

• Create a SafeGuard administrator account used strictly for managing SafeGuard disk encryption settings.

• Specify credentials for a local administrator account.

• Specify the drive you want to encrypt.

To customize the SafeGuard activation script:

1. Open the Casper Suite Resource Kit.

   If you do not have the Resource Kit, you can download it from:

   http://www.jamfsoftware.com/downloads/ResourceKit.dmg

2. Go to Remote Management > Disk Encryption > Sophos.

3. Open the `activateSophosSafeGuard.sh` script with a text editor.

4. Specify the following parameters:

   • `sgUsername` - User name for the SafeGuard administrator account

   • `sgPassword` - Password for the SafeGuard administrator account

   • `localAdmin` - User name for a local administrator account or an existing SafeGuard account

   • `localPassword` - Password for a local administrator account or an existing SafeGuard account

- `driveToEncrypt` - UUID or index of the partition you want to encrypt
  To encrypt the system drive, type `system` as the parameter.

  To encrypt all partitions, type `all` as the parameter.

5. Save your changes, and then quit the application.

Running the SafeGuard Activation Script

Upload the SafeGuard activation script to the JSS and then create a policy to run it.

To upload the SafeGuard activation script:

1. Open Casper Admin.

2. Log in using credentials for a JSS administrator account.

3. Drag the SafeGuard activation script into Casper Admin.

4. Double-click the script in the list of items, and then click the **Info** tab.

5. Use the **Category** pop-up menu to assign the script to a category.

6. Click **OK**.

7. Type **Command+S** to save your changes, and then quit the application.

To run the SafeGuard activation script using a policy:

1. Log in to the JSS with a web browser.

2. Click the **Management** tab.

3. Click the **Policies** link.

4. Click the **Create Policy** button.

5. Select the **Run a script** option and click **Continue**.

6. Follow the onscreen instructions to configure the rest of the policy.

The script runs on computers in the scope the next time they check in with the JSS.

Reporting on SafeGuard

After deploying SafeGuard, you can generate reports to track the following information:

- Computers that have SafeGuard installed
- Computers that have SafeGuard activated
- Disk encryption progress

This section explains how to report on SafeGuard using the following steps:

1. Create extension attributes to collect disk encryption status information.

2. Update inventory in the JSS.

3. View disk encryption status information.

4. Create a smart computer group to track disk encryption status.

Creating Extension Attributes

First, create extensions attributes to collect disk encryption status information from computers that have SafeGuard installed.

There are two extension attribute templates for disk encryption status built right into the JSS, allowing you to create extension attributes quickly and easily:

- SafeGuard Encryption Status - Reports on whether or not a disk is encrypted
- SafeGuard Encryption Percentage - Reports on what percentage of a disk is encrypted

To create extension attributes for SafeGuard:

1. Log in to the JSS with a web browser.

2. Click the **Settings** tab.

3. Click the **Inventory Options** link.

4. Click the **Inventory Collection Preferences** link.

5. Click the **Extension Attributes** tab.

6. Click the **Add Extension Attribute From Template** link.

7. Click the disclosure triangle next to the **Disk Encryption** template and click the **Add** link across from one of the following templates:

   - SafeGuard - Encryption Status
   - SafeGuard - Encryption Percentage

8. Enter the credentials for a SafeGuard administrator account, and then click **OK**.

9. Click the **Save** button.

Updating Inventory

The JSS must have up-to-date inventory information to generate accurate reports. Computers automatically update inventory according to the inventory frequency you configured when you set up the JSS. You can also use Casper Remote to update inventory on the fly.

To update inventory using Casper Remote:

1. Open Casper Remote.

2. Log in using credentials for a JSS administrator account.

3. On the **Computers** tab, select the checkbox next to the computers that have SafeGuard installed.

4. Click the **Advanced** tab.

5. Select the checkbox labeled **Update Inventory**.

6. Click **Go** to initiate the inventory update.

7. When the update is complete, quit the application.

Viewing Disk Encryption Status Information

To view disk encryption status information for multiple computers, perform an advanced computer search for computers that have SafeGuard installed. You can save this search so that you can perform it again in the future.

> **Note:** To view disk encryption status information for a single computer, perform a simple computer search. Then, click the **Details** link across from the computer in the search results to view the information.

To view disk encryption status information:

1. Log in to the JSS with a web browser.

2. Click the **Inventory** tab.

3. Click the **Advanced Search** link.

4. Enter a name for the report, such as "SafeGuard Disk Encryption Status".

5. Select the **Save this Report** checkbox.

6. Click the **Display Fields** tab.

7. Select the checkbox next to the SafeGuard extension attribute(s) that you created.

8. Click **Search** to view the search results.

Creating a Smart Computer Group

Smart computer groups allow you to automatically track and group clients as they move from one stage of the disk encryption process to the next. For example, if you create a smart computer group for computers that have SafeGuard installed and a smart computer group for computers that have SafeGuard activated, the computers that have SafeGuard installed automatically move to the activated group when SafeGuard is activated.

You can also choose to alert administrators by email whenever the membership of a smart computer group changes.

> **Note:** To generate email notifications, you must first configure an SMTP server in the JSS and make sure that the JSS user you want to receive the notifications has email notification privileges configured on their account. For more information on enabling email notifications, see the "Enabling Email Notifications" section in the *Casper Suite Administrator's Guide*.

To create a smart computer group:

1. Log in to the JSS with a web browser.

2. Click the **Management** tab.

3. Click the **Smart Computer Groups** link.

4. Click the **Create Smart Group** button in the toolbar.

5. Enter a name for the smart computer group in the **Computer Group Name** field.

6. In the list of categories, click the **Add (+)** button next to **Extension Attributes Information**.

7. Click the link for the SafeGuard extension attribute that you want to base the group on.

8. Use the **Search Type** pop-up menu and the **Criteria** text field to set values for the criteria, such as "has" and "SafeGuard Installed".

9. To send an email notification when membership changes occur, select the **Send Email Notification on Change** checkbox.

10. Click **Save**.