Administering FileVault on OS X El Capitan with the Casper Suite

Technical Paper
Casper Suite v9.81 or Later
27 May 2016

JAMF software

JAMF Software
100 Washington Ave S Suite 1100
Minneapolis, MN 55401-2155
(612) 605-6625

JAMF Software would like to acknowledge Rich Trouton for contributing content to this technical paper.

Contents

Introduction

What's in This Guide

This guide provides step-by-step instructions for administering FileVault on OS X v10.11 with the Casper Suite.

Important Concepts

Administrators using this guide should be familiar with the following Casper Suite-related concepts:

- Deployment
- Smart computer groups

Additional Resources

For more information on related topics, see the *Casper Suite Administrator’s Guide*.

Overview

This paper provides a complete workflow for administering FileVault on computers with OS X v10.11.

Activating FileVault disk encryption involves the following steps:

1. Choose a recovery key.
2. Create and export an institutional recovery key (for institutional recovery keys only).
3. Create a disk encryption configuration.
4. Deploy the disk encryption configuration.

After activating FileVault disk encryption on computers, you can create smart computer groups to use as the basis for performing the following additional tasks:

- View FileVault information for a computer.
- Issue a new FileVault recovery key to computers.
- Enable or disable a local account for FileVault.
- Enable or disable the management account for FileVault.
- Access encrypted data.

General Requirements

Administering FileVault on computers requires:

- The JAMF Software Server (JSS) v9.81 or later
- An administrator's computer with OS X v10.8 or later
- Target computers with OS X v10.11 and a "Recovery HD" partition

Note: There are additional requirements for specific procedures covered in this guide.

Choosing a Recovery Key

The first step to administering FileVault disk encryption is to choose the type of recovery key that you want to use to recover encrypted data.

There are two types of recovery keys:

- **Individual (also known as "Personal")—**Uses a unique alphanumeric recovery key for each computer. The individual recovery key is generated on the computer and sent back to the JSS for storage when the encryption takes place.
- **Institutional—**Uses a shared recovery key. This requires you to create the recovery key with Keychain Access and upload to the JSS for storage.

You can also choose to use both recovery keys (individual and institutional) together in the JSS.

If you plan to use an institutional recovery key, you must first create the institutional recovery key using Keychain Access. For instructions, see Creating and Exporting an Institutional Recovery Key.

Creating and Exporting an Institutional Recovery Key

To use an institutional recovery key, you must first create and export a recovery key using Keychain Access.

You can export the recovery key with or without the private key. Exporting with the private key allows you to store it in the JSS. If you export without the private key, you must store it in a secure location so you can access it when needed.

Creating and Exporting an Institutional Recovery Key with the Private Key

1. On an administrator computer, open Terminal and execute the following command:

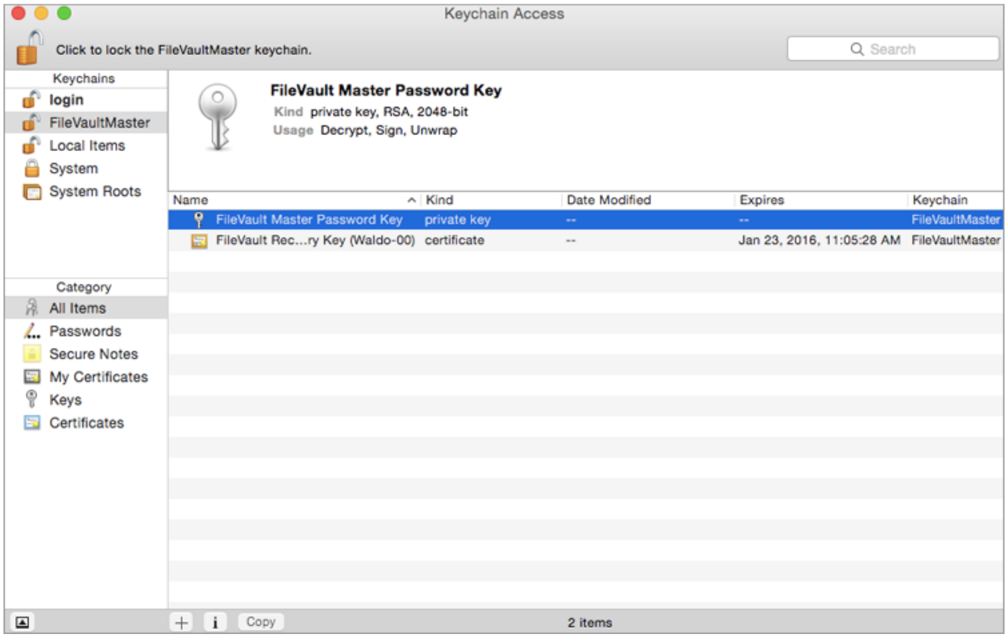
   ```
   sudo security create-filevaultmaster-keychain /Library/Keychains/
   FileVaultMaster.keychain
   ```

2. Enter a password for the new keychain when prompted.
   A keychain (`FileVaultMaster.keychain`) is created in the following location:
   `/Library/Keychains/`
3. Unlock the keychain by opening Terminal and executing:

   ```
   security unlock-keychain /Library/Keychains/FileVaultMaster.keychain
   ```

4. Make a backup of the keychain and save it in a secure location.
5. Open Keychain Access.
6. From the menu bar, choose **File > Add Keychain** and add the `FileVaultMaster.keychain` file located in `/Library/Keychains/`.
7. Select **FileVaultMaster** under the Keychains heading in the sidebar, and then select **All Items** under the Category heading.

8. Verify that a private key is associated with the certificate.



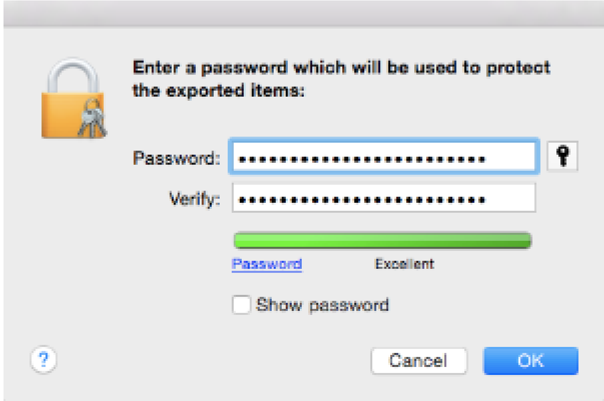
FileVault Master Password Key
Kind private key, RSA, 2048-bit
Usage Decrypt, Sign, Unwrap

Name	Kind	Date Modified	Expires	Keychain
FileVault Master Password Key	private key	--	--	FileVaultMaster
FileVault Rec...ry Key (Waldo-00)	certificate	--	Jan 23, 2016, 11:05:28 AM	FileVaultMaster

9. Select the certificate and the private key.

10. From the menu bar, choose **File > Export Items** and save the items as a .p12 file.
The .p12 file is a bundle that contains both the FileVault Recovery Key and the private key.

11. Create and verify a password to secure the file, and then click **OK**.
You will be prompted enter this password when uploading the recovery key to the JSS.



Enter a password which will be used to protect the exported items:

Password: ••••••••••••••••••••••••

Verify: ••••••••••••••••••••••••

12. Quit Keychain Access.

The FileVault Recovery Key and the private key are saved as a .p12 file in the location you specified.

Creating and Exporting an Institutional Recovery Key without the Private Key

1. On an administrator computer, open Terminal and execute the following command:

```
sudo security create-filevaultmaster-keychain /Library/Keychains/
FileVaultMaster.keychain
```

2. Enter a password for the new keychain when prompted.
   A keychain (`FileVaultMaster.keychain`) is created in the following location:
   `/Library/Keychains/`

3. Unlock the keychain by opening Terminal and executing:

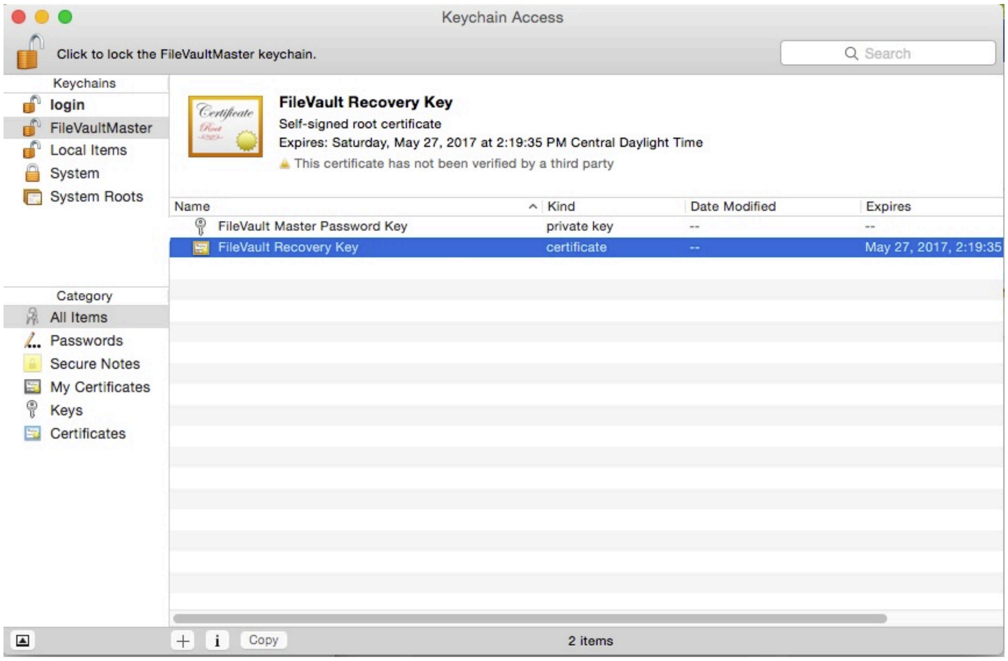
```
security unlock-keychain /Library/Keychains/FileVaultMaster.keychain
```

4. Open Keychain Access.

5. From the menu bar, choose **File > Add Keychain** and add the `FileVaultMaster.keychain` file located in `/Library/Keychains/`.

6. Select **FileVaultMaster** under the Keychains heading in the sidebar, and then select **All Items** under the Category heading.

7. Select the certificate.
   Do not select the private key associated with the certificate.



FileVault Recovery Key
Self-signed root certificate
Expires: Saturday, May 27, 2017 at 2:19:35 PM Central Daylight Time
This certificate has not been verified by a third party

Name	Kind	Date Modified	Expires
FileVault Master Password Key	private key	--	--
FileVault Recovery Key	certificate	--	May 27, 2017, 2:19:35

9. From the menu bar, choose **File > Export Items** and save the recovery key as a .pem file or .cer file.
   You will need to upload this file to the JSS when creating the disk encryption configuration.

10. Quit Keychain Access.
11. Store the keychain (`FileVaultMaster.keychain`) in a secure location so you can use it to access encrypted data at a later time.

    The FileVault Recovery Key is saved as a .cer file or a .pem file in the location you specified.

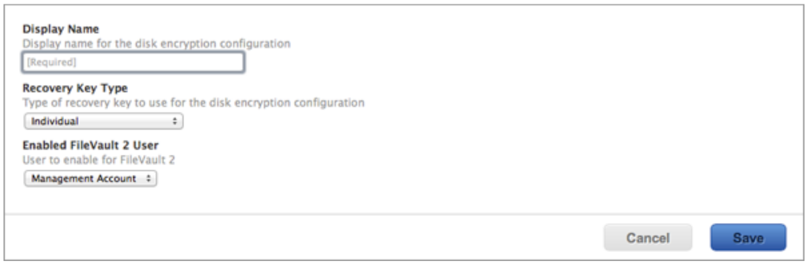
Creating a Disk Encryption Configuration

Creating a disk encryption configuration in the JSS is the first step to activating FileVault on computers.

Disk encryption configurations allow you to configure the following information:

- The type of recovery key to use for recovering encrypted data
- The user for which to enable FileVault

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙ .
3. Click **Computer Management**.
   On a smartphone, this option is in the pop-up menu.
4. In the “Computer Management” section, click **Disk Encryption Configurations** .
5. Click **New** + .
6. Enter a name for the disk encryption configuration in the **Display Name** field.

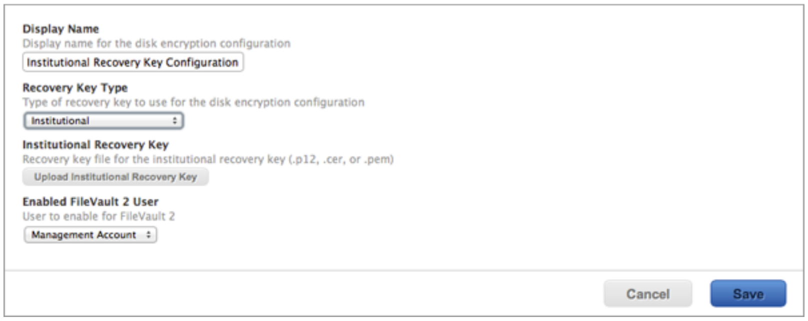


Display Name
Display name for the disk encryption configuration
[Required]

Recovery Key Type
Type of recovery key to use for the disk encryption configuration
Individual

Enabled FileVault 2 User
User to enable for FileVault 2
Management Account

7. Choose a type of recovery key from the **Recovery Key Type** pop-up menu.
8. If you chose an “Institutional” or “Individual and Institutional” recovery key, click **Upload Institutional Recovery Key** and upload the recovery key to the JSS.
   The recovery key must be a .p12, .cer, or .pem file.
   If you upload a .p12 file, you are prompted to enter the password that you created when exporting the key from Keychain Access.



Display Name
Display name for the disk encryption configuration
Institutional Recovery Key Configuration

Recovery Key Type
Type of recovery key to use for the disk encryption configuration
Institutional

Institutional Recovery Key
Recovery key file for the institutional recovery key (.p12, .cer, or .pem)

Enabled FileVault 2 User
User to enable for FileVault 2
Management Account

9. Choose the user for which to enable FileVault:
   - **Management Account—**Makes the management account on the computer the enabled FileVault user.
   - **Current or Next User—**Makes the user that is logged in to the computer when the encryption takes place the enabled FileVault user. If no user is logged in, the next user to log in becomes the enabled FileVault user.

   Note: If you make the management account the enabled FileVault user on computers with OS X v10.11, you will be able to issue a new recovery key to those computers later if necessary. (For more information, see Issuing a New FileVault Recovery Key.)

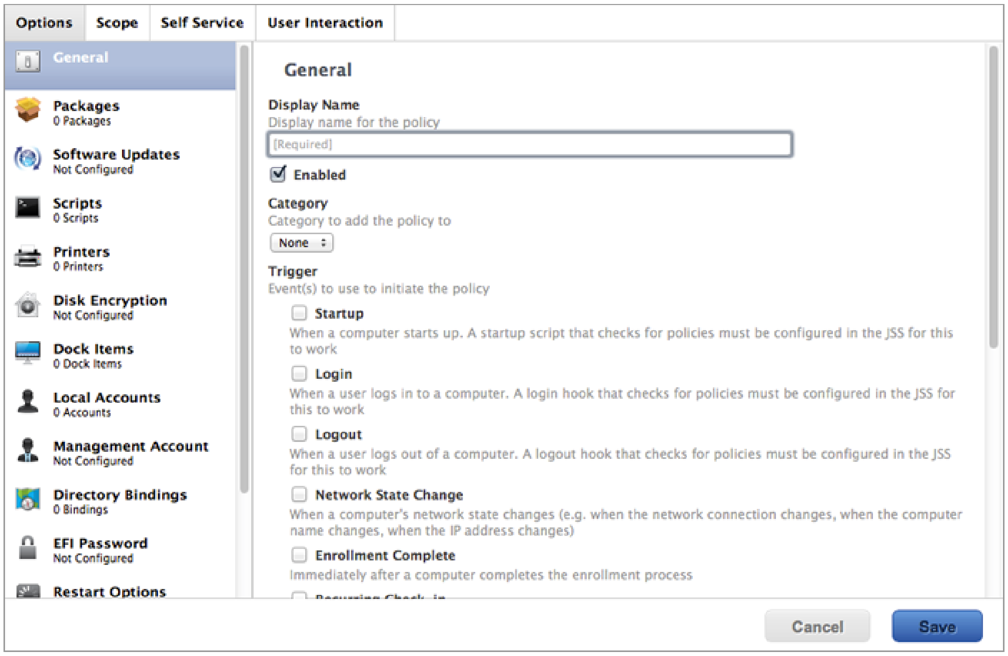
10. Click **Save**.

Deploying the Disk Encryption Configuration

After creating a disk encryption configuration, use a policy to deploy it to activate FileVault.

The event that activates FileVault depends on the enabled FileVault user specified in the disk encryption configuration. If the enabled user is “Management Account”, FileVault is activated on a computer the next time the computer restarts. If the enabled user is “Current or Next User”, FileVault is activated on a computer the next time the current user logs out or the computer restarts. In addition, if you are deploying a disk encryption configuration using a policy, you can configure the policy to defer FileVault enablement until after multiple user logins have occurred.

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Policies**.
   On a smartphone, this option is in the pop-up menu.
4. Click **New** + .
5. In the General payload, enter a display name for the policy. For example, “FileVault Disk Encryption“.



General

Display Name
Display name for the policy
[Required]

☑ Enabled

Category
Category to add the policy to
None

Trigger
Event(s) to use to initiate the policy

□ Startup
When a computer starts up. A startup script that checks for policies must be configured in the JSS for this to work

□ Login
When a user logs in to a computer. A login hook that checks for policies must be configured in the JSS for this to work

□ Logout
When a user logs out of a computer. A logout hook that checks for policies must be configured in the JSS for this to work

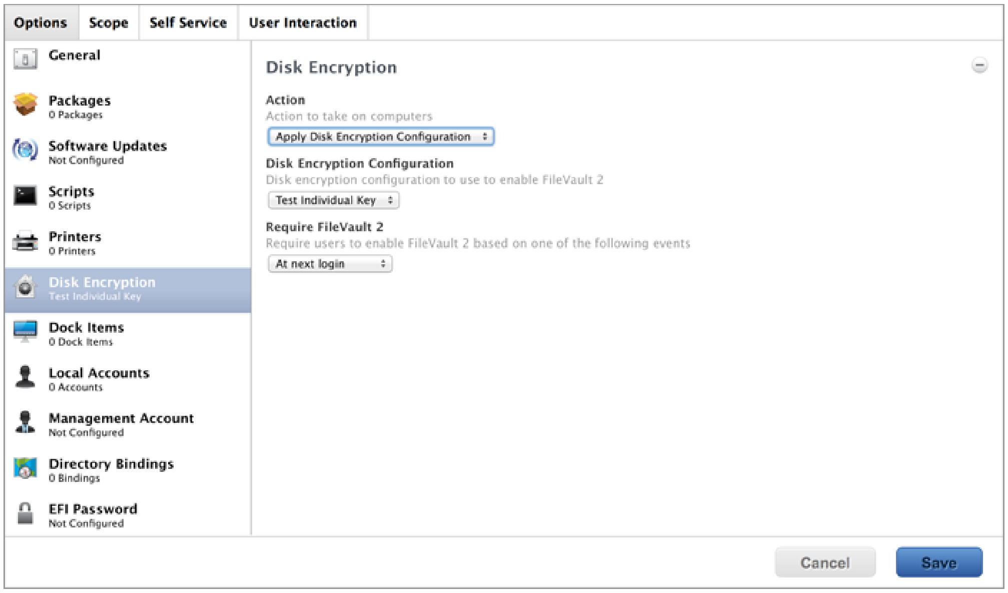
□ Network State Change
When a computer's network state changes (e.g. when the network connection changes, when the computer name changes, when the IP address changes)

□ Enrollment Complete
Immediately after a computer completes the enrollment process

6. Select a trigger.
7. Choose “Once per computer” from the **Execution Frequency** pop-up menu.
8. Select the Disk Encryption payload and click **Configure**.
9. Choose “Apply Disk Encryption Configuration” from the **Action** pop-up menu.

10. Choose the disk encryption configuration from the **Disk Encryption Configuration** pop-up menu.

11. Choose an event from the **Require FileVault 2** pop-up menu to specify when users must enable disk encryption.



Disk Encryption

Action
Action to take on computers
Apply Disk Encryption Configuration

Disk Encryption Configuration
Disk encryption configuration to use to enable FileVault 2
Test Individual Key

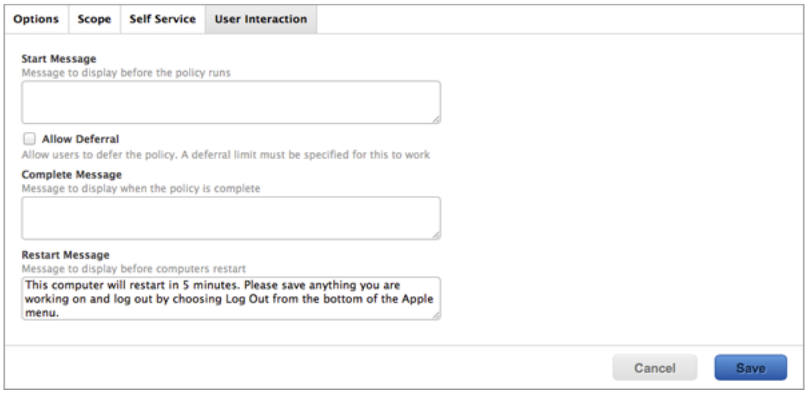
Require FileVault 2
Require users to enable FileVault 2 based on one of the following events
At next login

12. If “Management Account” is selected as the enabled FileVault user in the disk encryption configuration, do the following:

    a. Select the Restart Options payload and configure restart settings for the computer.

    b. (Optional) If you are using the Casper Suite v9.63 or later, select **Perform authenticated restart on computers with FileVault 2 enabled** to allow computers with OS X v10.8.2 or later that are FileVault enabled to be restarted without requiring an unlock the next time the computer starts up.
    For this to work on computers with FileVault activated, the enabled FileVault user must log in after the policy runs for the first time and the computer has restarted.

    c. (Optional) Click the **User Interaction** tab and customize the restart message displayed to users.



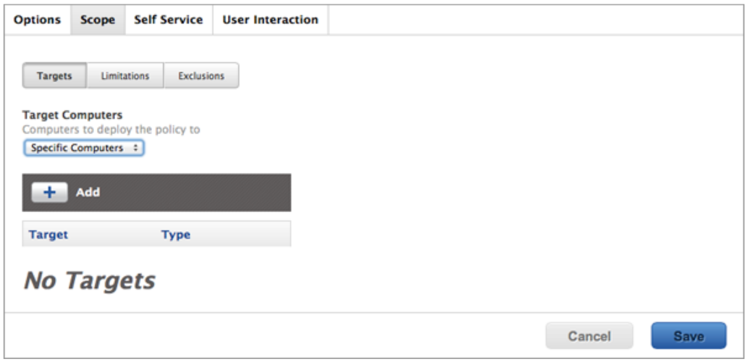
Start Message
Message to display before the policy runs

□ Allow Deferral
Allow users to defer the policy. A deferral limit must be specified for this to work

Complete Message
Message to display when the policy is complete

Restart Message
Message to display before computers restart
This computer will restart in 5 minutes. Please save anything you are working on and log out by choosing Log Out from the bottom of the Apple menu.

13. Click the **Scope** tab and configure the scope of the policy.



Target Computers
Computers to deploy the policy to
Specific Computers

No Targets

Note: It is recommended that the scope of this policy includes a smart group with computers that are FileVault eligible, but are not yet encrypted. For information on how to create this smart group, see Creating Smart Computer Groups for FileVault.

14. Click **Save**.

    The policy runs on computers in the scope the next time they check in with the JSS and meet the criteria in the General payload.

Creating Smart Computer Groups for FileVault

You can use the JSS to create smart computer groups that can be used as the scope of FileVault tasks. FileVault smart computer groups can be based on the following criteria:

- Computers that are eligible to be FileVault encrypted but are not yet encrypted
- Computers that are FileVault encrypted
- Computers that are in a specific FileVault partition encryption state
- Computers that are not eligible to be FileVault encrypted
- Computers with an invalid individual recovery key
- Computers on which a specified user is enabled for FileVault

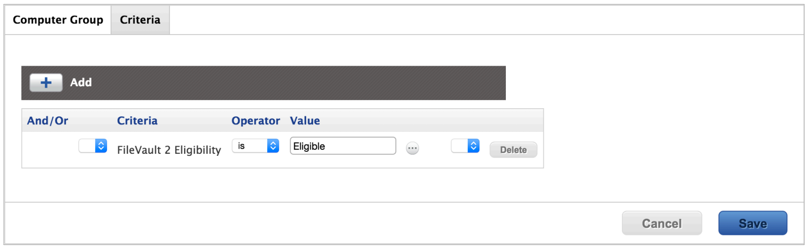
After creating a smart computer group, you can view its memberships.

Note: You can create smart computer groups based on additional FileVault criteria that are not covered in this guide. For information on all FileVault smart group criteria, see the following Knowledge Base article:
Smart Group and Advanced Search Criteria for FileVault 2 and Legacy FileVault

Creating a Smart Group of Computers that are Eligible to be FileVault Encrypted but are Not Yet Encrypted

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Smart Computer Groups**.
   On a smartphone, this option is in the pop-up menu.
4. Click **New** + .
5. On the Computer Group pane, enter a display name for the group.
6. To enable email notifications, select the **Send email notification on membership change** checkbox.
7. Click the **Criteria** tab.
8. Click **Add** + .
9. Click **Choose** for “All Criteria”, and then click **Choose** for “FileVault 2 Eligibility”.
   When the criteria is displayed, make sure the operator is set to “is”.

10. Click **Browse** , and then click **Choose** for “Eligible”.

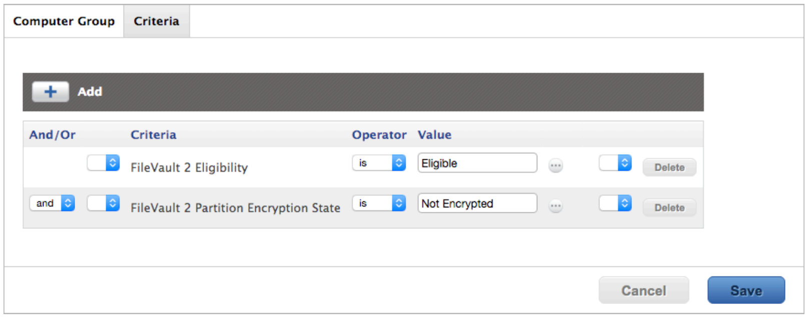


And/Or	Criteria	Operator	Value
	FileVault 2 Eligibility	is	Eligible

11. Click **Add** .

12. Click **Choose** for “All Criteria”, and then click **Choose** for “FileVault 2 Partition Encryption State”.
When the criteria is displayed, make sure the operator is set to “is”.

13. Click **Browse** , and then click **Choose** for “Not Encrypted”.



And/Or	Criteria	Operator	Value
	FileVault 2 Eligibility	is	Eligible
and	FileVault 2 Partition Encryption State	is	Not Encrypted

14. Choose “and” from the **And/Or** pop-up menu to specify the relationship between the criteria.

15. Click **Save**.

Group memberships are updated each time computers check in with the JSS and meet or fail to meet the specified criteria.

To view the group’s membership, click **View**.

Creating a Smart Group of Computers that are FileVault Encrypted

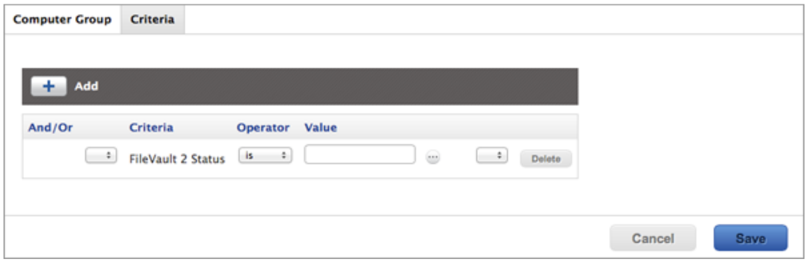
1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Smart Computer Groups**.
   On a smartphone, this option is in the pop-up menu.
4. Click **New** .
5. On the Computer Group pane, enter a display name for the group.
6. To enable email notifications, select the **Send email notification on membership change** checkbox.

7. Click the **Criteria** tab.

8. Click **Add** + .

9. Click **Choose** for “All Criteria“, and then click **Choose** for “FileVault 2 Status”.
   When the criteria is displayed, make sure the operator is set to “is”.

10. Click **Browse** ⋯ , and then click **Choose** for “Boot Partitions Encrypted”.



11. Click **Save**.

Group memberships are updated each time computers check in with the JSS and meet or fail to meet the specified criteria.

To view the group’s membership, click **View**.

Creating Smart Groups of Computers with a Partition in a Specific Encryption State

You can create a smart group of computers with a partition that is in any of the following encryption states:

- Decrypted
- Decrypting
- Encrypted
- Encrypting
- Ineligible
- Not Encrypted
- Unknown

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

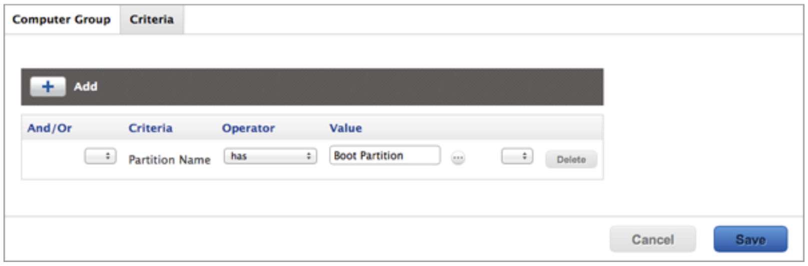
2. Click **Computers** at the top of the page.

3. Click **Smart Computer Groups**.
   On a smartphone, this option is in the pop-up menu.

4. Click **New** + .

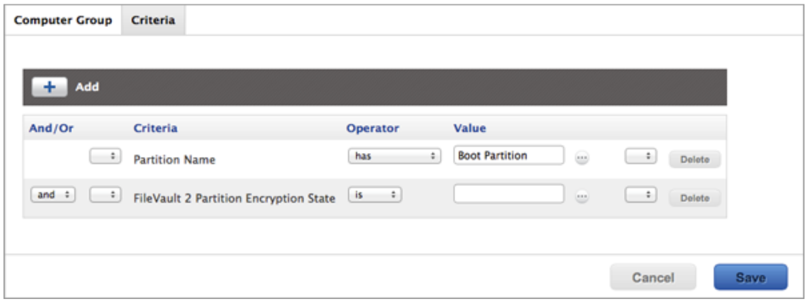
5. On the Computer Group pane, enter a display name for the group.

6. To enable email notifications, select the **Send email notification on membership change** checkbox.
7. Click the **Criteria** tab.
8. Click **Add** + .
9. Click **Choose** for “All Criteria“, and then click **Choose** for “Partition Name”.
10. Choose “has” from the **Operator** pop-up menu.
11. Type a partition name in the **Value** field, or click **Browse** ⋯ , and then click **Choose** for “Boot Partition”.



And/Or	Criteria	Operator	Value
	Partition Name	has	Boot Partition

12. Click **Add** + .
13. Click **Choose** for “All Criteria“, and then click **Choose** for “FileVault 2 Partition Encryption State”. When the criteria is displayed, make sure the operator is set to “is”.
14. Click **Browse** ⋯ , and then click **Choose** for the encryption state you want to base the group on.



And/Or	Criteria	Operator	Value
	Partition Name	has	Boot Partition
and	FileVault 2 Partition Encryption State	is	

15. Choose “and” from the **And/Or** pop-up menu to specify the relationship between the criteria.
16. Click **Save**.

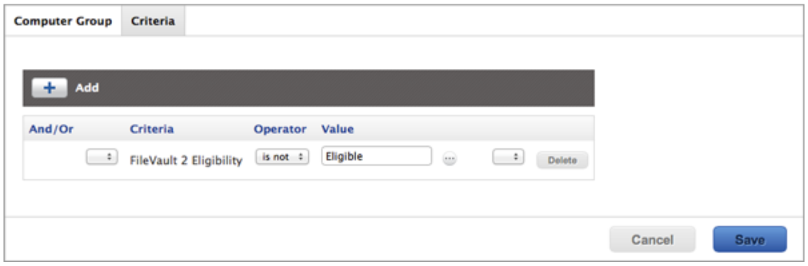
Group memberships are updated each time computers check in with the JSS and meet or fail to meet the specified criteria.

To view the group’s membership, click **View**.

Creating a Smart Group of Computers that are Not Eligible for FileVault Encryption

You can create a smart group of computers that do not have an institutional recovery key.

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Smart Computer Groups**.
   On a smartphone, this option is in the pop-up menu.
4. Click **New** + .
5. On the Computer Group pane, enter a display name for the group.
6. To enable email notifications, select the **Send email notification on membership change** checkbox.
7. Click the **Criteria** tab.
8. Click **Add** + .
9. Click **Choose** for “All Criteria“, and then click **Choose** for “FileVault 2 Eligibility”.
10. Choose “is not” from the **Operator** pop-up menu.
11. Click **Browse** ⋯ , and then click **Choose** for “Eligible”.



And/Or	Criteria	Operator	Value
	FileVault 2 Eligibility	is not	Eligible

12. Click **Save**.

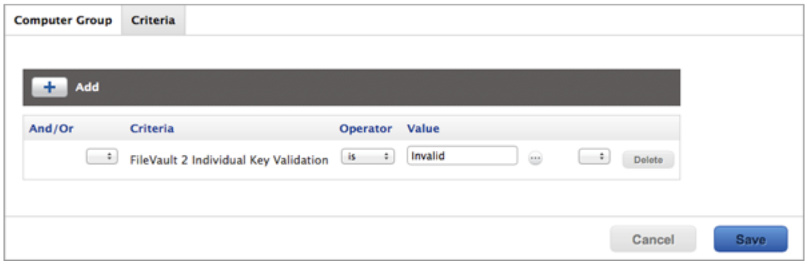
Group memberships are updated each time computers check in with the JSS and meet or fail to meet the specified criteria.

To view the group’s membership, click **View**.

Creating a Smart Group of Computers with an Invalid Individual Recovery Key

You can create a smart computer group to validate that the individual recovery key on computers matches the key stored in the JSS.

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Smart Computer Groups**.
   On a smartphone, this option is in the pop-up menu.
4. Click **New** + .
5. On the Computer Group pane, enter a display name for the group.
6. To enable email notifications, select the **Send email notification on membership change** checkbox.
7. Click the **Criteria** tab.
8. Click **Add** + .
9. Click **Choose** for "All Criteria", and then click **Choose** for "FileVault 2 Individual Key Validation".
   When the criteria is displayed, make sure the operator is set to "is".
10. Click **Browse** ⋯ , and then click **Choose** for "Invalid".



And/Or	Criteria	Operator	Value
	FileVault 2 Individual Key Validation	is	Invalid

11. Click **Save**.

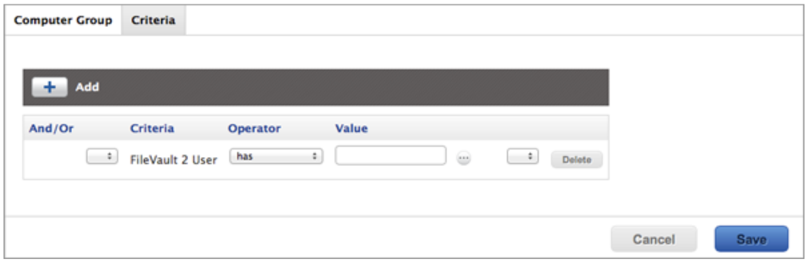
Group memberships are updated each time computers check in with the JSS and meet or fail to meet the specified criteria.

To view the group's membership, click **View**.

Creating a Smart Group of Computers for Which a Specified User is Enabled for FileVault

You can create a smart computer group to identify the computers for which a specified user is enabled for FileVault.

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Smart Computer Groups**.
   On a smartphone, this option is in the pop-up menu.
4. Click **New** + .
5. On the Computer Group pane, enter a display name for the group.
6. To enable email notifications, select the **Send email notification on membership change** checkbox.
7. Click the **Criteria** tab.
8. Click **Add** + .
9. Click **Choose** for “All Criteria“, and then click **Choose** for “FileVault 2 User”.
   When the criteria is displayed, make sure the operator is set to “has”.
10. Enter a username, or click **Browse** ··· **,** and then click **Choose** for a FileVault 2-enabled user.



And/Or	Criteria	Operator	Value
	FileVault 2 User	has	

11. Click **Save**.

Group memberships are updated each time computers check in with the JSS and meet or fail to meet the specified criteria.

To view the group’s membership, click **View**.

Viewing FileVault Information for a Computer

You can view the FileVault disk encryption information for a computer. You can also view its FileVault recovery key.

Viewing FileVault Disk Encryption Information for a Computer

You can use the smart computer group you created in “Creating a Smart Group of Computers that are FileVault Encrypted” to view the following information for the boot partition on a FileVault-encrypted computer:

- Last inventory update
- FileVault partition encryption state
- Individual recovery key validation
- Institutional recovery key
- Disk encryption configuration
- FileVault-enabled users

You can also view the last inventory update date and partition encryption state for any non-boot partitions on the computer.

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Smart Computer Groups**.
   On a smartphone, this option is in the pop-up menu.
4. Click the smart computer group you created in “Creating a Smart Group of Computers that are FileVault Encrypted”, and then click **View**.
5. Click the computer you want to view disk encryption information for.
6. Select **Disk Encryption** in the list of categories.

The computer’s FileVault disk encryption information is displayed for the boot partition. For any additional partitions, the last inventory update date and partition encryption state is displayed.

Viewing the FileVault Recovery Key for a Computer

You can use the smart computer group you created in “Creating a Smart Group of Computers that are FileVault Encrypted” to view the recovery key for a FileVault-encrypted computer.

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Smart Computer Groups**.
   On a smartphone, this option is in the pop-up menu.
4. Click the smart computer group you created in the “Creating a Smart Group of Computers that are FileVault Encrypted” section, and then click **View**.
5. Click the computer you want to view the recovery key for, and then click the **Management** tab.
6. Select FileVault 2 in the list of categories, and then click **Get Recovery Key**.
   - If the recovery key is an “Individual” recovery key, it is displayed in the JSS.
   - If the recovery key is an “Institutional” recovery key, click **Download** to download it.
   - If the recovery key is an “Individual and Institutional” recovery key, the individual recovery key is displayed in the JSS. To download the institutional recovery key, click **Download**.

Issuing a New FileVault Recovery Key

You can use a policy to issue a new FileVault recovery key to computers with OS X v10.11 that have FileVault activated. This allows you to do the following:

- Replace an individual recovery key that has been reported as invalid and does not match the recovery key stored in the JSS.
- Update the recovery key on computers on a regular schedule, without needing to decrypt and then re-encrypt the computers.

Requirements

To issue a new individual recovery key to a computer, the computer must have:

- OS X v10.11
- A "Recovery HD" partition
- FileVault activated
- One of the following conditions met:
  - The management account configured as the FileVault-enabled user
  - An existing, valid individual recovery key that matches the key stored in the JSS

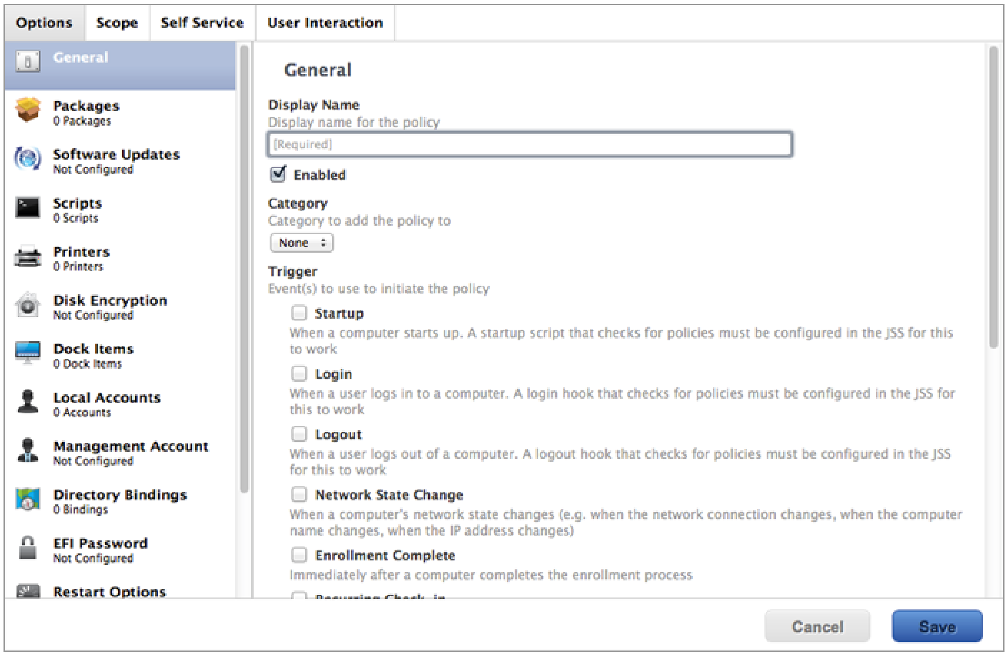
To issue a new institutional recovery key to a computer, the computer must have:

- OS X v10.11
- A "Recovery HD" partition
- FileVault activated
- The management account configured as the FileVault-enabled user

Issuing a New FileVault Recovery Key to Computers

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Policies**.
   On a smartphone, this option is in the pop-up menu.
4. Click **New** + .

5. In the General payload, enter a display name for the policy. For example, “FileVault New Individual Recovery Key“.



General

Packages
0 Packages

Software Updates
Not Configured

Scripts
0 Scripts

Printers
0 Printers

Disk Encryption
Not Configured

Dock Items
0 Dock Items

Local Accounts
0 Accounts

Management Account
Not Configured

Directory Bindings
0 Bindings

EFI Password
Not Configured

Restart Options

General

Display Name
Display name for the policy
[Required]

☑ Enabled

Category
Category to add the policy to
None

Trigger
Event(s) to use to initiate the policy

□ Startup
When a computer starts up. A startup script that checks for policies must be configured in the JSS for this to work

□ Login
When a user logs in to a computer. A login hook that checks for policies must be configured in the JSS for this to work

□ Logout
When a user logs out of a computer. A logout hook that checks for policies must be configured in the JSS for this to work

□ Network State Change
When a computer's network state changes (e.g. when the network connection changes, when the computer name changes, when the IP address changes)

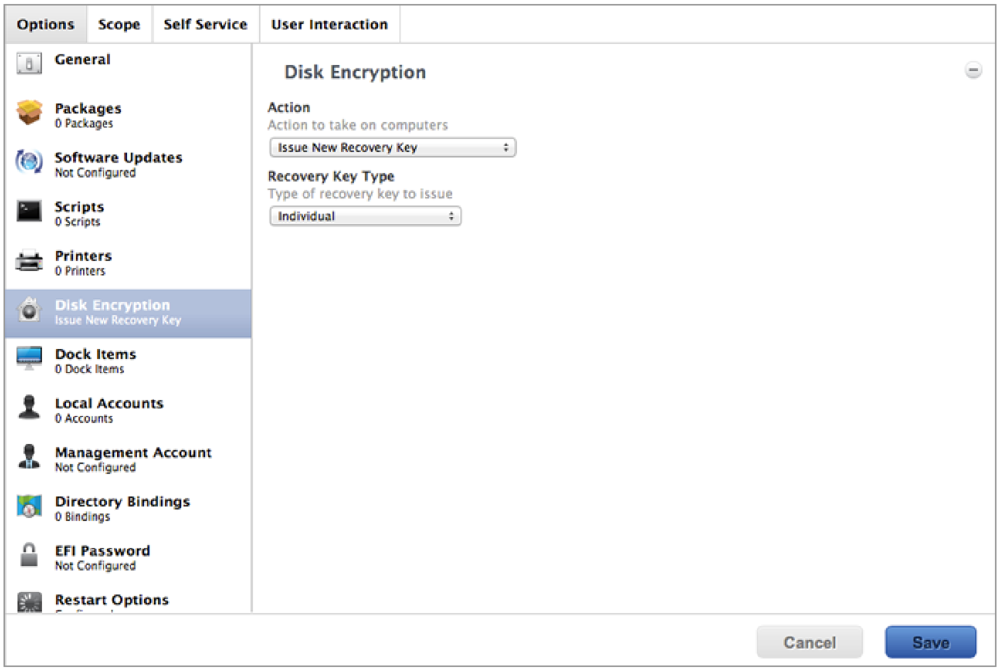
□ Enrollment Complete
Immediately after a computer completes the enrollment process

□ Recurring Check-in

6. Select a trigger and execution frequency.

7. Select the Disk Encryption payload and click **Configure**.

8. Choose “Issue New Recovery Key” from the **Action** pop-up menu.



General

Packages
0 Packages

Software Updates
Not Configured

Scripts
0 Scripts

Printers
0 Printers

Disk Encryption
Issue New Recovery Key

Dock Items
0 Dock Items

Local Accounts
0 Accounts

Management Account
Not Configured

Directory Bindings
0 Bindings

EFI Password
Not Configured

Restart Options

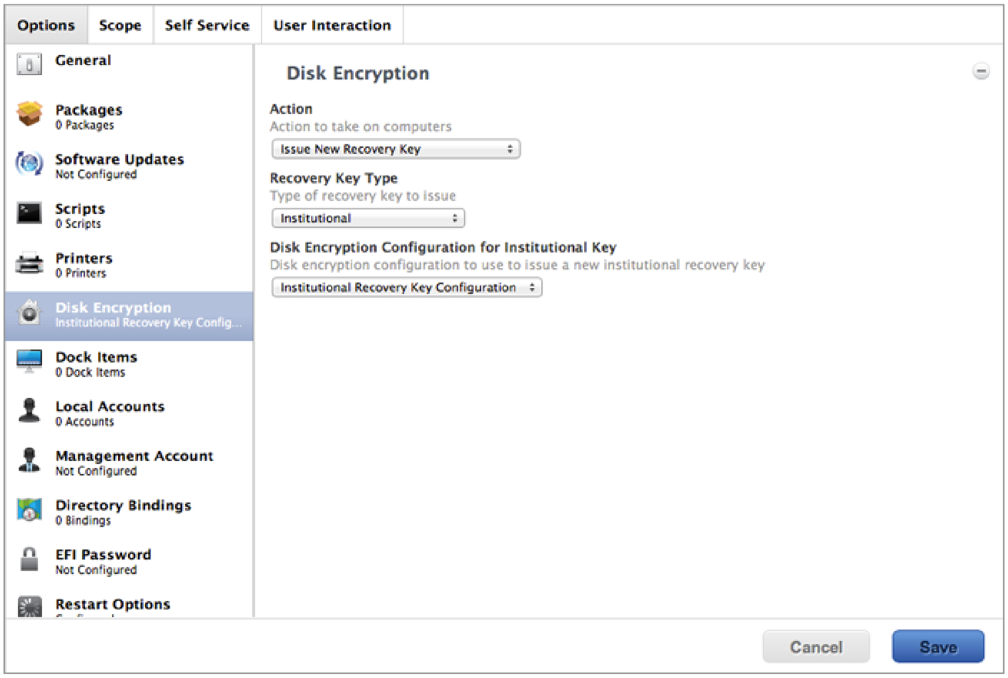
Disk Encryption

Action
Action to take on computers
Issue New Recovery Key

Recovery Key Type
Type of recovery key to issue
Individual

9. Choose the type of recovery key you want to issue from the **Recovery Key Type** pop-up menu:
   - **Individual—**A new individual recovery key is generated on each computer and then submitted to the JSS for storage.
   - **Institutional—**A new institutional recovery key is deployed to computers and stored in the JSS.
   - **Individual and Institutional—**Issues both types of recovery keys to computers.

   If you chose "Institutional" or "Individual and Institutional", choose the disk encryption configuration to use to issue the new recovery key from the **Disk Encryption Configuration for Institutional Key** pop-up menu.



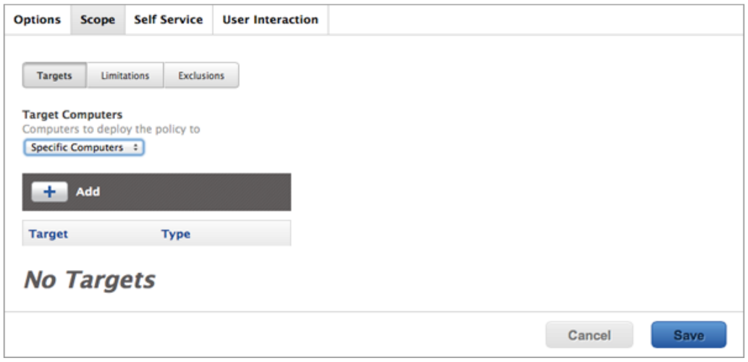
Disk Encryption

Action
Action to take on computers
Issue New Recovery Key

Recovery Key Type
Type of recovery key to issue
Institutional

Disk Encryption Configuration for Institutional Key
Disk encryption configuration to use to issue a new institutional recovery key
Institutional Recovery Key Configuration

10. Click the **Scope** tab and configure the scope of the policy.
    Note: If applicable, you can use the smart computer group you created in "Creating a Smart Group of Computers with an Invalid Individual Recovery Key" as the scope for the policy.



Target Computers
Computers to deploy the policy to
Specific Computers

Target	Type

No Targets

11. Click **Save**.

The policy runs on computers in the scope the next time they check in with the JSS and meet the criteria in the General payload.

Enabling or Disabling a Local Account for FileVault

When you create a new account, you can enable the account for FileVault. You can also disable an existing account for FileVault.

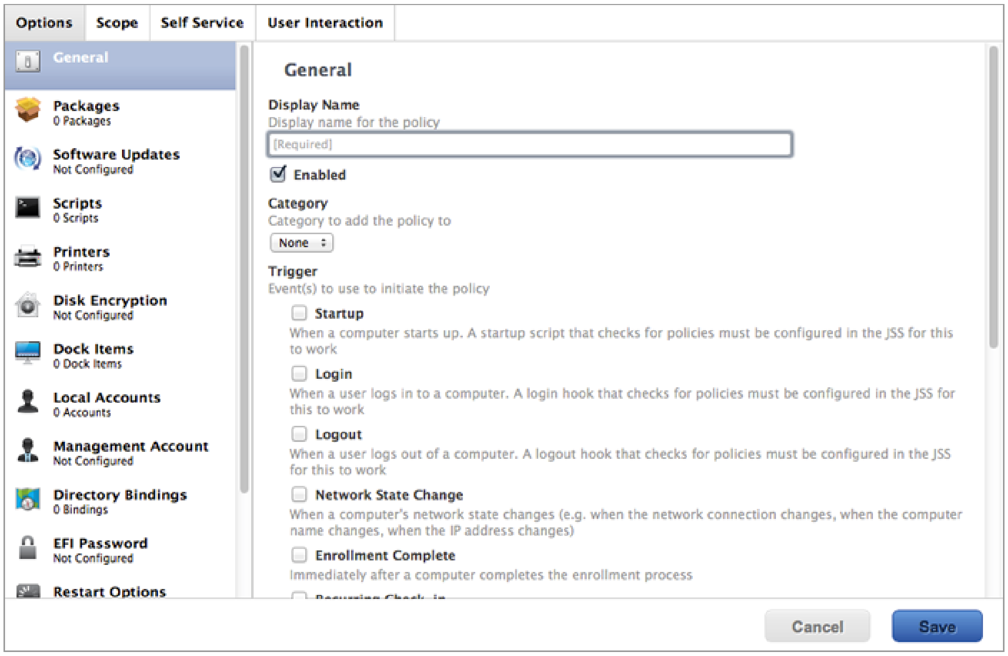
Requirements

To enable a new account for FileVault, the computer must have OS X v10.11 and have an existing, valid individual recovery key that matches the key stored in the JSS.

To disable an existing account for FileVault, the computer must have OS X v10.11.

Enabling a New Local Account for FileVault

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Policies**.
   On a smartphone, this option is in the pop-up menu.
4. Click **New** + .
5. In the General payload, enter a display name for the policy. For example, “Add Local Account for FileVault“.



General

Display Name
Display name for the policy
[Required]

☑ Enabled

Category
Category to add the policy to
None

Trigger
Event(s) to use to initiate the policy

☐ Startup
When a computer starts up. A startup script that checks for policies must be configured in the JSS for this to work

☐ Login
When a user logs in to a computer. A login hook that checks for policies must be configured in the JSS for this to work

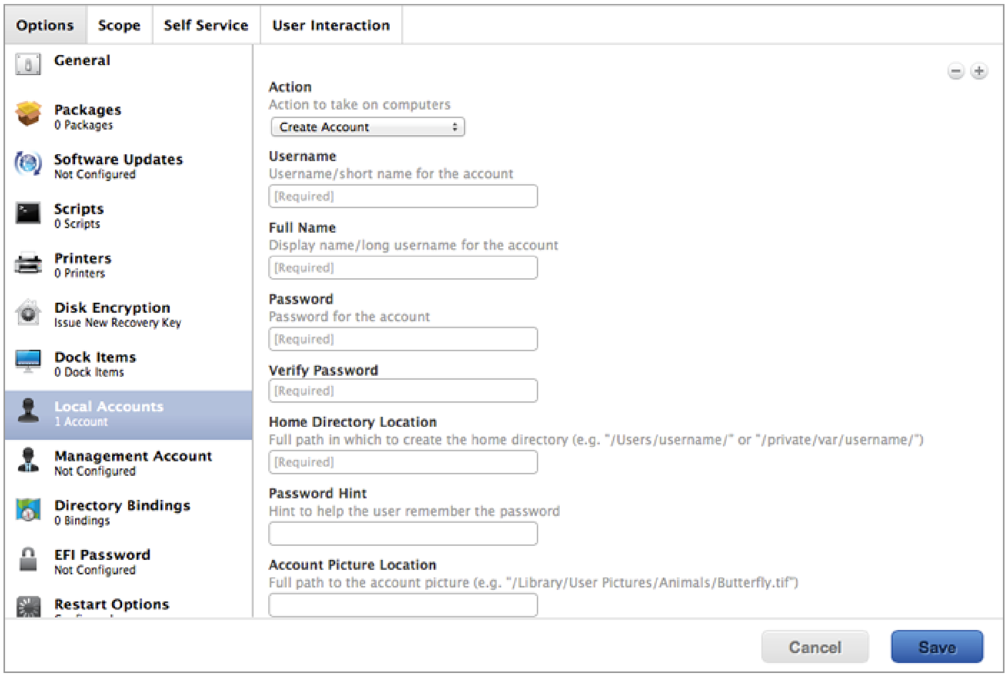
☐ Logout
When a user logs out of a computer. A logout hook that checks for policies must be configured in the JSS for this to work

☐ Network State Change
When a computer's network state changes (e.g. when the network connection changes, when the computer name changes, when the IP address changes)

☐ Enrollment Complete
Immediately after a computer completes the enrollment process

☐ Recurring Check-in

6. Select a trigger and execution frequency.
7. Select the Local Accounts payload and click **Configure**.
8. Choose “Create Account” from the **Action** pop-up menu.



Action
Action to take on computers
Create Account

Username
Username/short name for the account
[Required]

Full Name
Display name/long username for the account
[Required]

Password
Password for the account
[Required]

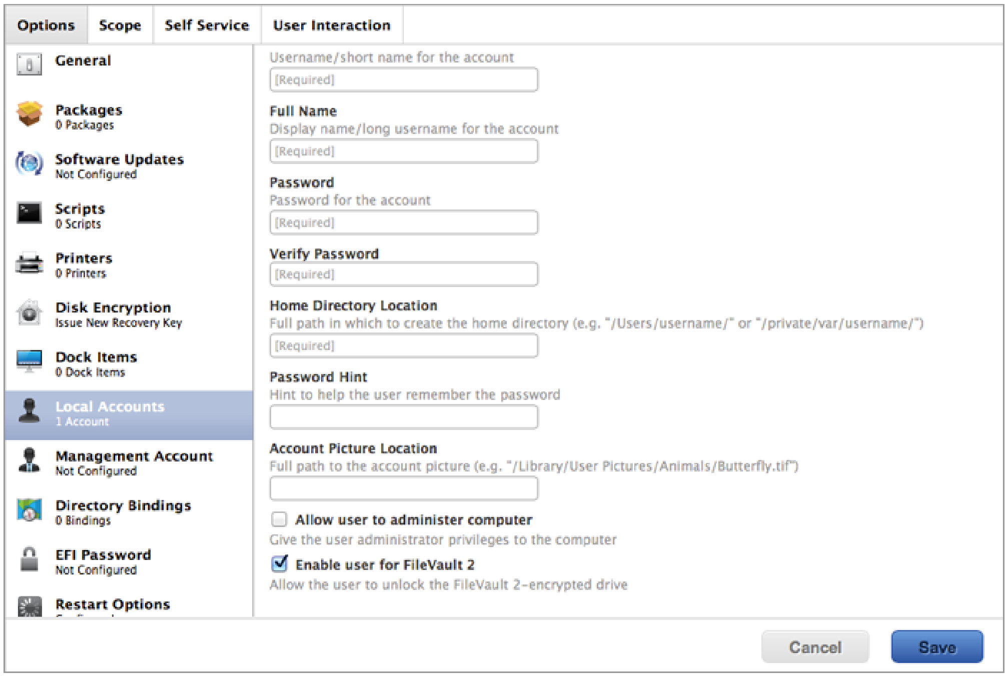
Verify Password
[Required]

Home Directory Location
Full path in which to create the home directory (e.g. "/Users/username/" or "/private/var/username/")
[Required]

Password Hint
Hint to help the user remember the password

Account Picture Location
Full path to the account picture (e.g. "/Library/User Pictures/Animals/Butterfly.tif")

9. Specify the required information for the local account, including the username, full name, password, and home directory location.
10. Select the **Enable user for FileVault 2** checkbox.



Username/short name for the account
[Required]

Full Name
Display name/long username for the account
[Required]

Password
Password for the account
[Required]

Verify Password
[Required]

Home Directory Location
Full path in which to create the home directory (e.g. "/Users/username/" or "/private/var/username/")
[Required]

Password Hint
Hint to help the user remember the password

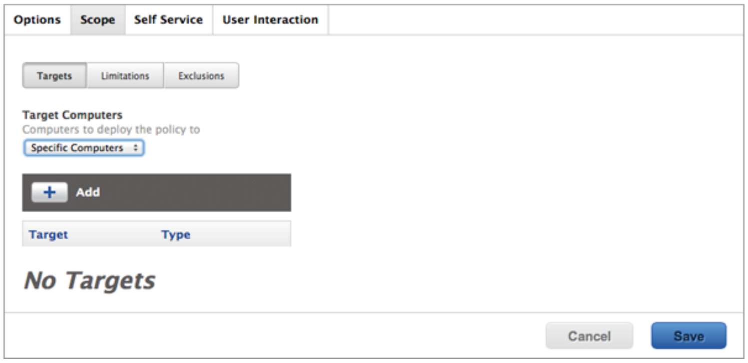
Account Picture Location
Full path to the account picture (e.g. "/Library/User Pictures/Animals/Butterfly.tif")

☐ Allow user to administer computer
Give the user administrator privileges to the computer

☑ Enable user for FileVault 2
Allow the user to unlock the FileVault 2-encrypted drive

11. (Optional) Select the Maintenance payload and then select the **Update Inventory** checkbox so that the FileVault-enabled status for the user is updated in inventory immediately when the policy runs.

12. Click the **Scope** tab and configure the scope of the policy.
    Note: If applicable, you can use the smart computer group you created in "Creating a Smart Group of Computers that are FileVault Encrypted" as the scope for the policy.



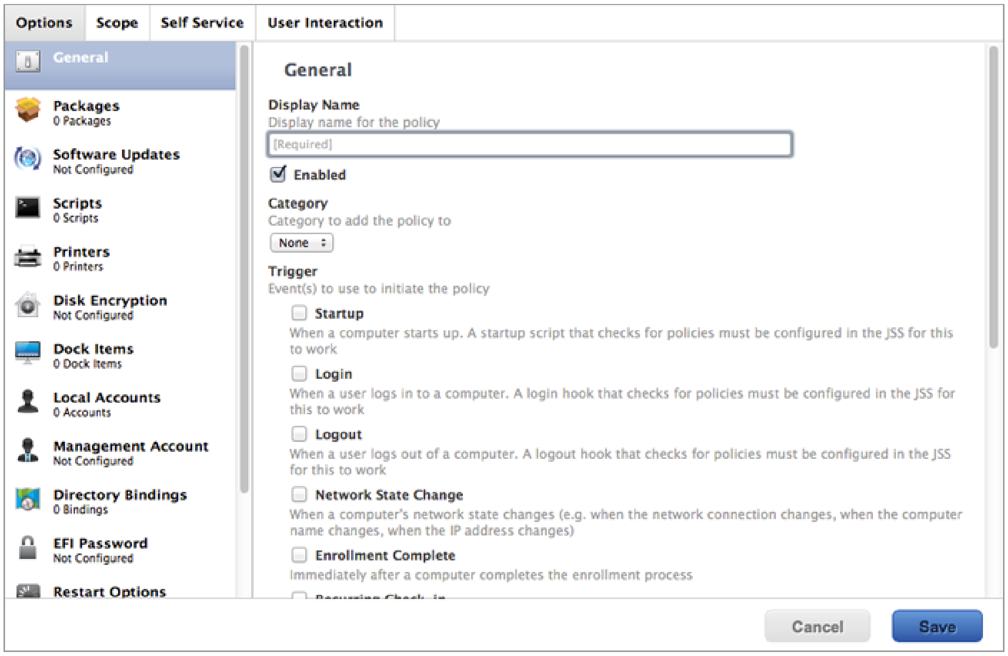
13. Click **Save**.

    The policy runs on computers in the scope the next time they check in with the JSS and meet the criteria in the General payload.

Disabling an Existing Local Account for FileVault

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Policies**.
   On a smartphone, this option is in the pop-up menu.
4. Click **New** + .

5. In the General payload, enter a display name for the policy. For example, “Disable Local Account for FileVault“.



General

Display Name
Display name for the policy
[Required]

☑ Enabled

Category
Category to add the policy to
None

Trigger
Event(s) to use to initiate the policy

□ Startup
When a computer starts up. A startup script that checks for policies must be configured in the JSS for this to work

□ Login
When a user logs in to a computer. A login hook that checks for policies must be configured in the JSS for this to work

□ Logout
When a user logs out of a computer. A logout hook that checks for policies must be configured in the JSS for this to work

□ Network State Change
When a computer's network state changes (e.g. when the network connection changes, when the computer name changes, when the IP address changes)

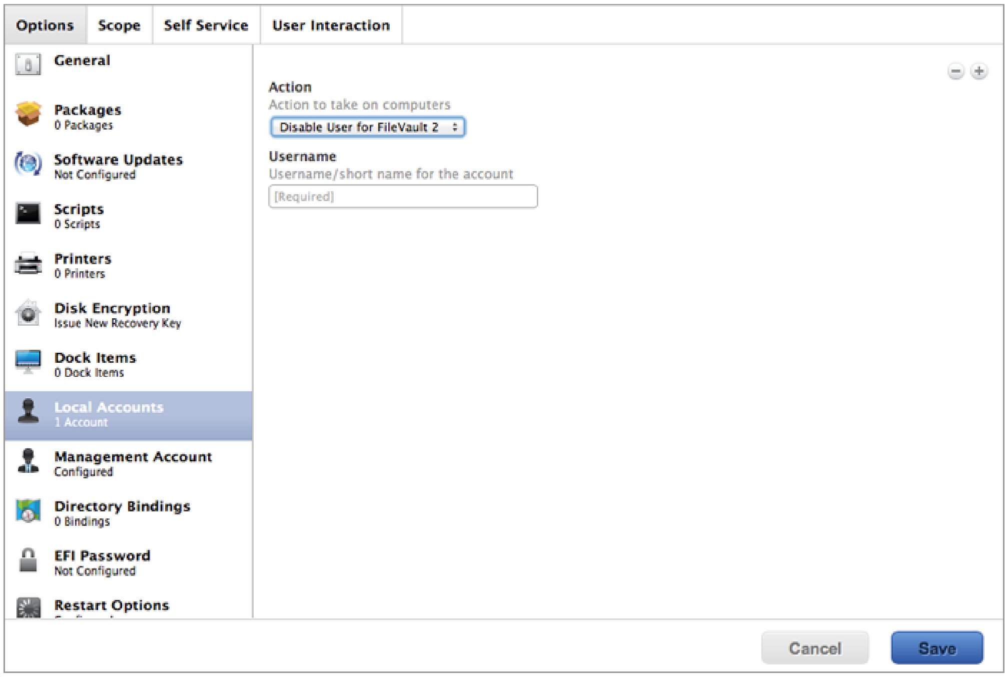
□ Enrollment Complete
Immediately after a computer completes the enrollment process

□ Recurring Check-in

6. Select a trigger and execution frequency.

7. Select the Local Accounts payload and click **Configure**.

8. Choose “Disable User for FileVault 2” from the **Action** pop-up menu.



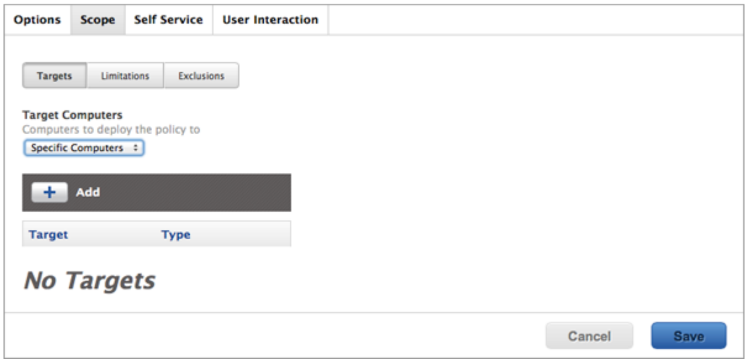
Action
Action to take on computers
Disable User for FileVault 2

Username
Username/short name for the account
[Required]

9. Enter the username of the user you want to disable for FileVault.

10. (Optional) Select the Maintenance payload and then select the **Update Inventory** checkbox so that the FileVault-enabled status for the local account is updated in inventory immediately when the policy runs.

11. Click the **Scope** tab and configure the scope of the policy.
Note: If applicable, you can use the smart computer group you created in “Creating a Smart Group of Computers for Which a Specified User is Enabled for FileVault” as the scope for the policy.



Target Computers
Computers to deploy the policy to
Specific Computers

Target	Type

No Targets

12. Click **Save**.

The policy runs on computers in the scope the next time they check in with the JSS and meet the criteria in the General payload.

Enabling or Disabling the Management Account for FileVault

You can enable or disable the management account for FileVault.

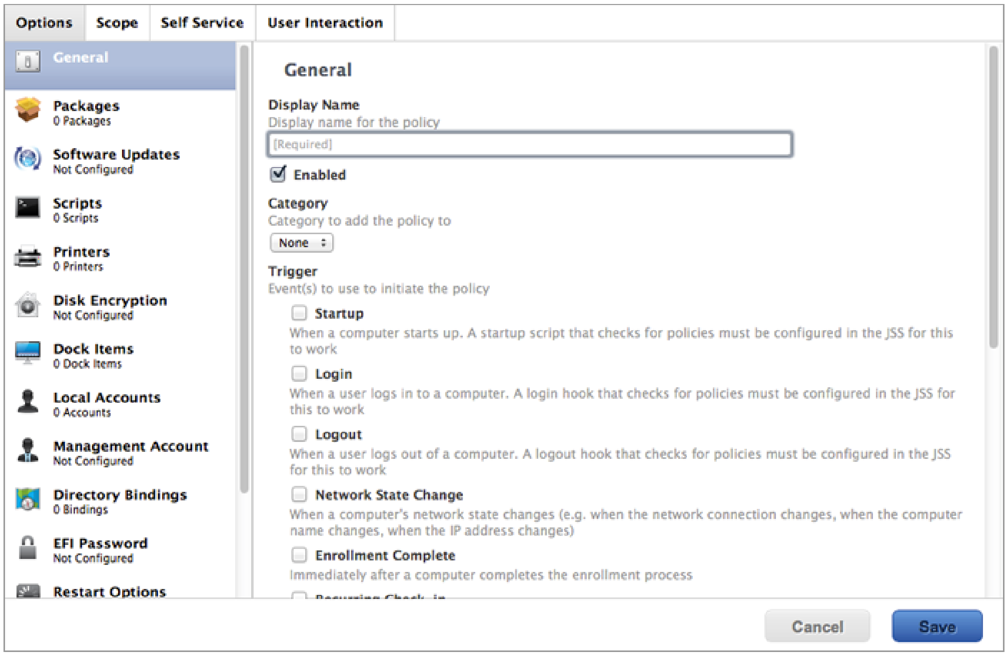
Requirements

To enable the management account for FileVault, the computer must have OS X v10.11 and have an existing, valid individual recovery key that matches the key stored in the JSS.

To disable the management account for FileVault, the computer must have OS X v10.11.

Enabling or Disabling the Management Account for FileVault

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Policies**.
   On a smartphone, this option is in the pop-up menu.
4. Click **New** + .
5. In the General payload, enter a display name for the policy. For example, “Enable Management Account for FileVault“.



General

Display Name
Display name for the policy
[Required]

☑ Enabled

Category
Category to add the policy to
None

Trigger
Event(s) to use to initiate the policy

□ Startup
When a computer starts up. A startup script that checks for policies must be configured in the JSS for this to work

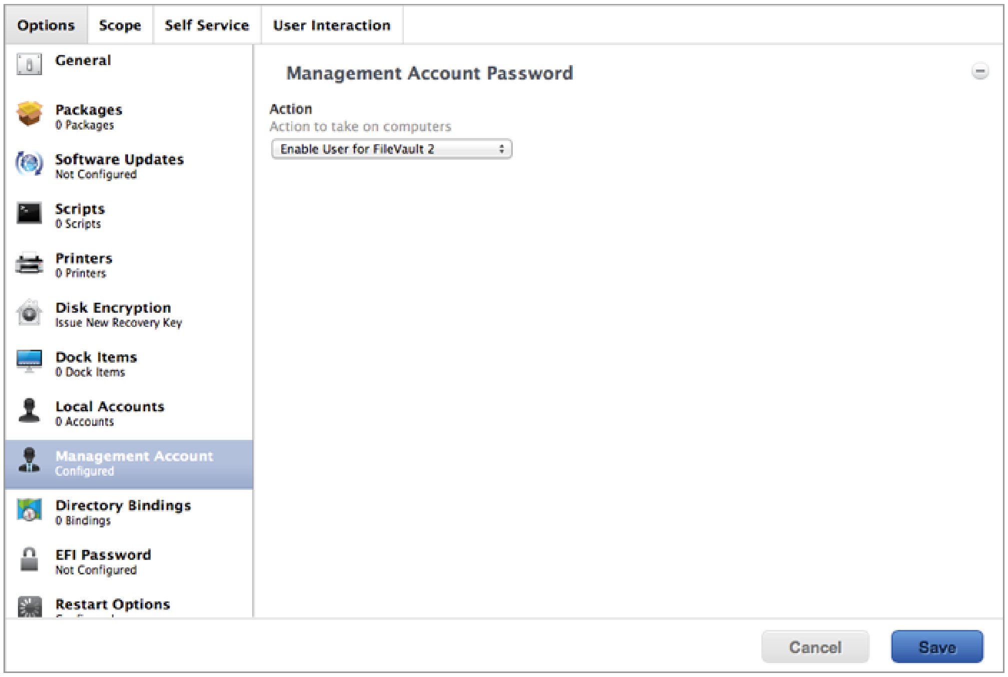
□ Login
When a user logs in to a computer. A login hook that checks for policies must be configured in the JSS for this to work

□ Logout
When a user logs out of a computer. A logout hook that checks for policies must be configured in the JSS for this to work

□ Network State Change
When a computer's network state changes (e.g. when the network connection changes, when the computer name changes, when the IP address changes)

□ Enrollment Complete
Immediately after a computer completes the enrollment process

6. Select a trigger and execution frequency.
7. Select the Management Account payload and click **Configure**.
8. Choose “Enable User for FileVault 2” or “Disable User for FileVault 2” from the **Action** pop-up menu.

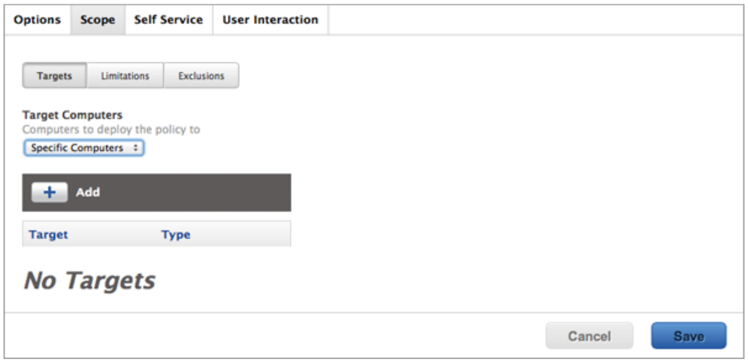


Management Account Password

Action
Action to take on computers
Enable User for FileVault 2

9. (Optional) Select the Maintenance payload and then select the **Update Inventory** checkbox so that the FileVault Enabled status for the management account is updated in inventory immediately when the policy runs.

10. Click the **Scope** tab and configure the scope of the policy.
    Note: If applicable, you can use the smart computer group you created in “Creating a Smart Group of Computers that are FileVault Encrypted” as the scope for the policy.



Target Computers
Computers to deploy the policy to
Specific Computers

No Targets

11. Click **Save**.

    The policy runs on computers in the scope the next time they check in with the JSS and meet the criteria in the General payload.

Accessing Encrypted Data

FileVault allows you to access and recover the data on a user's encrypted drive without the user's login credentials. The way you access encrypted data depends on the number of accounts that are authorized to unlock the encrypted drive.

If more than one account is authorized to unlock the drive, there are two ways to access encrypted data:

- Reset the password for the user's account using an alternate authorized account. This allows you to recover data by simply logging in to the user's account.
- Decrypt the drive using an alternate authorized account. This requires you to use the command line to recover data.

If only one account is authorized to unlock the encrypted drive, you must decrypt the drive using the recovery key. Then, you can:

- Reset the account password using the Reset Password utility and recover data by simply logging in to the user's account.
- Recover data using the command line.

Resetting an Account Password Using an Alternate Authorized Account

You can use this method to access encrypted data if more than one account is authorized to unlock the drive.

1. Restart the target computer.
2. When prompted with the FileVault pre-boot screen, enter credentials for a secondary authorized account.
3. Make sure that you are logged in as an administrator.
4. Open System Preferences and click **Users & Groups**.
5. If needed, click the lock and enter your password to make changes.
6. Select the primary account in the sidebar and click the **Reset Password** button.
7. Enter a new password, and then enter it again to verify it. Then, click the **Reset Password** button.

You can now recover data by restarting the computer and entering credentials for the user's account when prompted with the FileVault pre-boot screen.

Decrypting a Drive Using an Alternate Authorized Account

You can use this method to access encrypted data if more than one account is authorized to unlock the drive.

1. Restart the target computer while pressing Command + R.
   This boots the computer to the "Recovery HD" partition.
2. Open Disk Utility.
3. From the menu bar, choose **File > Unlock "Macintosh HD" or File > Turn Off Encryption**.
4. Enter the password for the alternate authorized account.

   The system begins to decrypt the drive. The computer can be used normally during decryption.

   To view the decryption status, open System Preferences and click **Security & Privacy**. Then, click the **FileVault** tab.

   After the drive is decrypted, you can recover data using the command line.

Decrypting a Drive Using the Recovery Key

Use this method to access encrypted data if only one account is authorized to unlock the drive.

Note: If you used an institutional recovery key with the private key, and you no longer have the keychain, you need to download the `RecoveryKey.p12` file from the JSS and convert it to a .keychain file. For instructions, see the following Knowledge Base article:
Converting a RecoveryKey.p12 File to a FileVaultMaster.keychain File

1. Restart the target computer while pressing Command + R.
   This boots the computer to the "Recovery HD" partition.
2. Open Terminal.
3. Unlock the recovery key by executing a command similar to the following:

```
security unlock-keychain <path to the secure copy of the
FileVaultMaster.keychain file>
```

4. Locate the Logical Volume UUID of the encrypted disk by executing:

```
diskutil cs list
```

5. Unlock the encrypted drive with the Logical Volume UUID and recovery key by executing a command similar to the following:

   ```
   diskutil cs unlockVolume <UUID> -recoveryKeychain <path to the secure copy
   of the FileVaultMaster.keychain file>
   ```

6. Turn off encryption by executing a command similar to the following:

   ```
   diskutil cs revert <UUID> -recoveryKeychain <path to the secure copy of
   the FileVaultMaster.keychain file>
   ```

   After the drive is decrypted, you can reset the account password using the Reset Password utility and recover data by simply logging in to the user's account. Or, you can recover data using the command line.

1. Restart the target computer while pressing Command + R.
   This boots the computer to the "Recovery HD" partition.
2. Open Terminal and launch the Reset Password utility by executing:

   ```
   resetpassword
   ```

3. Use the Reset Password utility to reset the account's password.
4. Restart the computer and log in using the new password.