Administering FileVault on macOS 10.13 with Jamf Pro

Technical Paper
Jamf Pro 9.81 or Later
5 November 2020

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

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

Jamf 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 macOS 10.13 with Jamf Pro.

Important Concepts

Administrators using this guide should be familiar with the following Jamf Pro-related concepts:

- Deployment
- Smart computer groups

Additional Resources

For more information on related topics, see the *Jamf Pro Administrator's Guide*.

Overview

This paper provides a complete workflow for administering FileVault on computers with macOS 10.13.

FileVault disk encryption can be activated using a configuration profile or by performing 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 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

Performing the administrative tasks in this paper requires the following:

- Jamf Pro 9.81 or later
- An administrator computer with macOS 10.11 or later
- Target computers with macOS 10.13 and a “Recovery HD” partition

Important: Some administrative FileVault tasks in this guide cannot be performed on macOS 10.13.2–10.13.x. These limitations are noted throughout the guide, where applicable.

Activating FileVault Disk Encryption Using a Configuration Profile

You can activate FileVault disk encryption using a configuration profile. Disk encryption configuration will deploy at next user logout.

1. Log in to Jamf Pro.
2. Click **Computers** at the top of the page.
3. Click **Configuration Profiles**.
4. Click **New** + New .
5. Use the General payload to configure basic settings, which includes the distribution method. This configuration profile payload can only be applied at the Computer Level. Only payloads and settings that apply to the selected level are displayed for the profile.
6. Use the Security & Privacy payload to configure FileVault settings.
   a. Click the **FileVault** tab.
   b. Select the **Require FileVault 2** checkbox.
   c. Select **Use institutional recovery key**, **Create personal recovery key**, or both.
   d. (Optional) If you are using an institutional key, select the certificate that contains the public key from institutional recovery keychain. You can use the Certificate payload to upload an institutional recovery key to Jamf Pro.

      > **Note**: You cannot use an institutional recovery key with the private key.

   e. (Optional) If you are using a personal recovery key on macOS 10.13 or later, select **Enable Escrow Personal Recovery Key** to enable the device to encrypt the personal recovery key with the provided certificate and report it to Jamf Pro.
7. (Optional) Use the rest of the payloads to configure the settings you want to apply.
8. Click the **Scope** tab and configure the scope of the profile.
9. (Optional) If you chose to distribute the profile in Self Service, click the **Self Service** tab to configure Self Service settings for the profile.
10. Click **Save**.

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:

- **Personal (also known as "Individual")**—Uses a unique alphanumeric recovery key for each computer. The personal recovery key is generated on the computer and sent back to Jamf Pro for storage when the encryption takes place. This type of recovery key can function as a password and can be used to unlock the computer.
- **Institutional**—Uses a shared recovery key. This requires you to create the recovery key with Keychain Access and upload to Jamf Pro for storage. This type of recovery key cannot be used to unlock a user's startup disk.

You can choose to use both recovery keys (personal and institutional) together in Jamf Pro.

If you plan to use an institutional recovery key, you must first create an 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 Jamf Pro. If you export without the private key, you must store it in a secure location so you can access it when needed.

> **Note** : You cannot use an institutional recovery key with a private key to activate FileVault Disk Encryption using a configuration profile in Jamf Pro. You must create and deploy the disk encryption configuration using a policy in Jamf Pro.

Creating and Exporting an Institutional Recovery Key with the Private Key

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

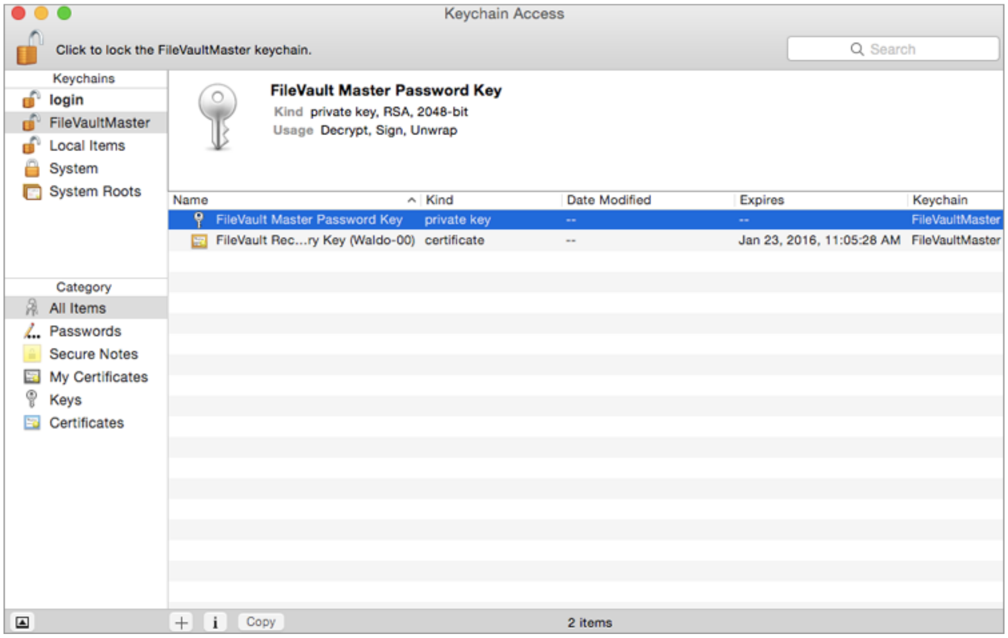
   ```
   sudo security create-filevaultmaster-keychain /Library/Keychains/
   FileVaultMaster.keychain
   ```

2. When prompted, enter a password for the new keychain.
3. To unlock the keychain, open Terminal and execute the following command:

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

4. Perform a backup of the keychain and save it in a secure location.
5. Open Keychain Access.
6. From the menu bar, choose "Add Keychain" from the **File** pop-up menu. Then, 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 "Export Items" from the **File** pop-up menu. Then, 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 to enter this password when uploading the recovery key to Jamf Pro.

12. Quit Keychain Access.

13. Store the keychain (`FileVaultMaster.keychain`) in a secure location so you can use it to access encrypted data at a later time. Without the keychain, you will not be able to decrypt the computer.

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:

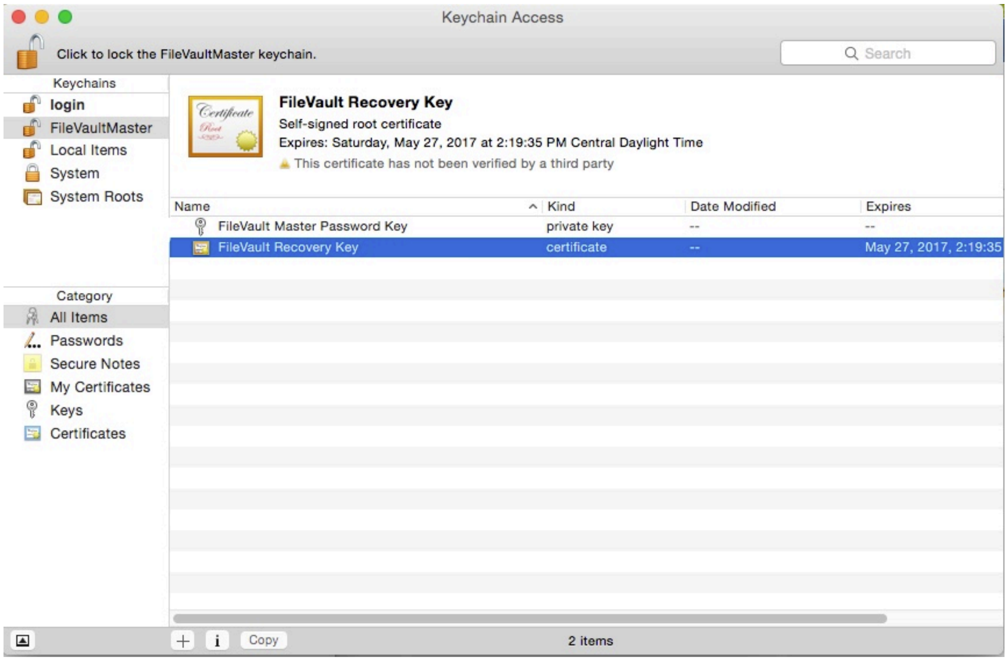
```
sudo security create-filevaultmaster-keychain /Library/Keychains/
FileVaultMaster.keychain
```

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 "Add Keychain" from the **File** pop-up menu. Then, 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.



Click to lock the FileVaultMaster keychain.

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

2 items

8. From the menu bar, choose "Export Items" from the **File** pop-up menu. Then, save the recovery key as a .pem file or .cer file.
   You will need to upload this file to Jamf Pro when creating the disk encryption configuration.
9. Quit Keychain Access.
10. 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.

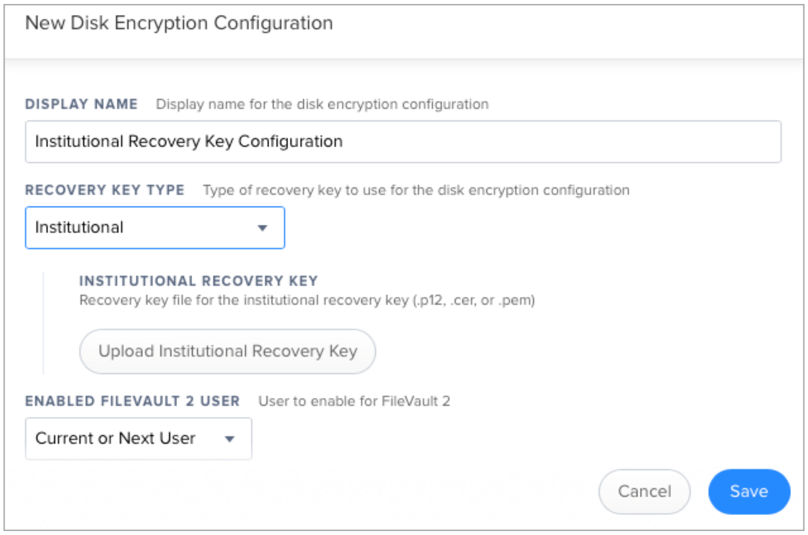
Creating a Disk Encryption Configuration

Creating a disk encryption configuration in Jamf Pro 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 Jamf Pro.
2. In the top-right corner of the page, click **Settings** ⚙ .
3. Click **Computer Management**.
4. In the “Computer Management” section, click **Disk Encryption Configurations** .
5. Click **New** + New .
6. Enter a name for the disk encryption configuration in the **Display Name** field.
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 Jamf Pro.
   The recovery key must be a .p12 or .cer file.
   If you upload a .p12 file, you are prompted to enter the password that you created when exporting the key from Keychain Access.



New Disk Encryption Configuration

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)

Upload Institutional Recovery Key

ENABLED FILEVAULT 2 USER User to enable for FileVault 2

Current or Next User

9. Choose "Current or Next User" or "Management Account" from the **Enabled FileVault 2 User** pop-up menu.
   - **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.
10. Click **Save**.

> **Important:** On macOS 10.13.2, you cannot select the management account on a computer as the enabled FileVault user.

Deploying the Disk Encryption Configuration

The event that activates FileVault depends on the enabled FileVault user specified in the disk encryption configuration and whether the computer is APFS enabled. If the enabled user is “Management Account” and the computer is APFS enabled, FileVault is activated on a computer at the next login without needing to reboot. If the computer is HFS+ formatted with the "Management Account" enabled user, FileVault is activated on a computer the next time the computer restarts. If the enabled user is “Current or Next User”, you can modify when FileVault is activated on a computer. Options include the following:

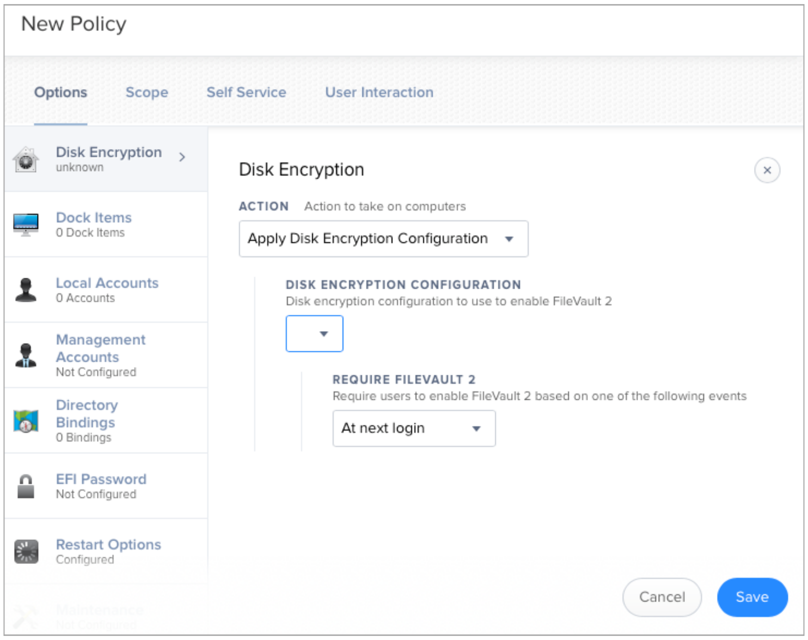
- The next time the computer restarts.
- The next time the current user logs out
- The next login or after multiple user logins, ranging from two to six logins.

Note: If the restart is done via a built-in policy, FileVault will not be activated.

Deploying the disk encryption configuration involves the following steps:

1. Log in to Jamf Pro.
2. Click **Computers** at the top of the page.
3. Click **Policies**.
4. Click **New** + New .
5. On the General payload, enter a display name for the policy. For example, “FileVault Disk Encryption“.
6. Select a trigger.
7. Choose “Ongoing” 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

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.

    > **Note:** Select "Restart" from the appropriate pop-up menu to include a restart prompt. Select "Restart immediately" to restart without prompting. "Restart" option does not work if set to encrypt at logout.

    b. (Optional) If you are using Jamf Pro 9.63 or later, select **Perform authenticated restart on computers with FileVault 2 enabled** to allow computers with macOS 10.8.2 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.

> **Important:** You cannot perform an authenticated restart on computers with FileVault 2 enabled on macOS 10.13.2–10.13.x.

13. Click the **Scope** tab and configure the scope of the policy. For more information, see Scope in the *Jamf Pro Administrator's Guide.*

> **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 Jamf Pro and match the selected trigger in the General payload.

Creating Smart Computer Groups for FileVault

You can use Jamf Pro 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 personal (also known as "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 Smart Group and Advanced Search Criteria for FileVault Knowledge Base article.

Creating a Smart Group for FileVault Eligible Computers that are Not Yet Encrypted

1. Log in to Jamf Pro.
2. Click **Computers** at the top of the page.
3. Click **Smart Computer Groups**.
4. Click **New** + 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** + Add .
9. Click **Show Advanced 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”.
11. Click **Add** + Add .
12. Click **Show Advanced 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”.
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 Jamf Pro and meet or fail to meet the specified criteria.

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

Creating a Smart Group 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 Jamf Pro.
2. Click **Computers** at the top of the page.
3. Click **Smart Computer Groups**.
4. Click **New** + 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** + Add .
9. Click **Show Advanced Criteria**, and then click **Choose** for “FileVault 2 Partition Encryption State”. When the criteria is displayed, make sure the operator is set to “is”.
10. Click **Browse** ⋯ , and then click **Choose** for the encryption state you want to base the group on.
11. Click **Save**.

    Group memberships are updated each time computers check in with Jamf Pro 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 are not eligible for FileVault Encryption.

1. Log in to Jamf Pro.
2. Click **Computers** at the top of the page.
3. Click **Smart Computer Groups**.
4. Click **New** + 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** + Add .
9. Click **Show Advanced 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”.
12. Click **Save**.

Group memberships are updated each time computers check in with Jamf Pro 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 personal (also known as "individual") recovery key on computers matches the key stored in Jamf Pro.

1. Log in to Jamf Pro.
2. Click **Computers** at the top of the page.
3. Click **Smart Computer Groups**.
4. Click **New** + 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** + Add .
9. Click **Show Advanced 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”.
11. Click **Save**.

Group memberships are updated each time computers submit inventory with Jamf Pro 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 Jamf Pro.
2. Click **Computers** at the top of the page.
3. Click **Smart Computer Groups**.
4. Click **New** + 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** + Add .
9. Click **Show Advanced 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.
11. Click **Save**.

Group memberships are updated each time computers check in with Jamf Pro 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
- Personal (also known as "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 Jamf Pro.
2. Click **Computers** at the top of the page.
3. Click **Smart Computer Groups**.
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 Jamf Pro.
2. Click **Computers** at the top of the page.
3. Click **Smart Computer Groups**.
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 **Inventory** tab.
6. Select Disk Encryption in the list of categories, and then click **Show Key**.
    - If the recovery key is a "Personal" (also known as “Individual”) recovery key, it is displayed in Jamf Pro.
    - If the recovery key is an “Institutional” recovery key, click **Download** to download it.
    - If the recovery key is a “Personal and Institutional” recovery key, the personal recovery key is displayed in Jamf Pro. To download the institutional recovery key, click **Download**.

Note: When a user views the FileVault Recovery Key, it logs their username and the date and time viewed in the "Viewed FileVault Encryption Key".

Issuing a New FileVault Recovery Key

You can use a policy to issue a new FileVault recovery key to computers with macOS 10.13 that have FileVault activated. This allows you to do the following:

- Replace personal (also known as "individual") recovery key that has been reported as invalid and does not match the recovery key stored in Jamf Pro.
- 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 personal recovery key to a computer, the computer must have:

- macOS 10.13
- A “Recovery HD” partition
- FileVault 2 enabled
- A FileVault enabled user with a SecureToken
  For more information on SecureToken, see Using SecureToken in Apple's *Deployment Reference for Mac*.

> **Important:** Personal recovery keys cannot be issued to computers with macOS 10.13.2–10.13.x.

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

- macOS 10.13
- A “Recovery HD” partition
- FileVault enabled

Issuing a New FileVault Recovery Key to Computers

1. Log in to Jamf Pro.
2. Click **Computers** at the top of the page.
3. Click **Policies**.
4. Click **New** + New .
5. In the General payload, enter a display name for the policy. For example, “FileVault New Personal Recovery Key“.
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.

9. Choose the type of recovery key you want to issue from the **Recovery Key Type** pop-up menu:
   - **Individual—**A new personal (also known as "individual") recovery key is generated on each computer and then submitted to Jamf Pro for storage.
   - **Institutional—**A new institutional recovery key is deployed to computers and stored in Jamf Pro.
   - **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.
10. Click the **Scope** tab and configure the scope of the policy. For more information, see Scope in the *Jamf Pro Administrator's Guide*.
11. Click **Save**.

    The policy runs on computers in the scope the next time they check in with Jamf Pro, prompting enabled users.

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 the following:

- macOS 10.13
- An existing valid personal (also known as "individual") recovery key that matches the key stored in Jamf Pro.

To disable an existing account for FileVault, the computer must have macOS 10.13.

> **Important:** Local accounts cannot be enabled or disabled for FileVault on computers with macOS 10.13.2 or later.

Enabling a New Local Account for FileVault

1. Log in to Jamf Pro.
2. Click **Computers** at the top of the page.
3. Click **Policies**.
4. Click **New** + New .
5. In the General payload, enter a display name for the policy. For example, “Add Local Account for FileVault“.
6. Select a trigger and execution frequency.
7. Select the Local Accounts payload and click **Configure**.
8. Select **Create New Account**.
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.
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. For more information, see Scope in the *Jamf Pro Administrator's Guide*.

    > **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 Jamf Pro and meet the criteria in the General payload.

Disabling an Existing Local Account for FileVault

1. Log in to Jamf Pro.
2. Click **Computers** at the top of the page.
3. Click **Policies**.
4. Click **New** + New .
5. In the General payload, enter a display name for the policy. For example, “Disable Local Account for FileVault“.
6. Select a trigger and execution frequency.
7. Select the Local Accounts payload and click **Configure**.
8. Select **Disable User for FileVault 2**.
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. For more information, see Scope in the *Jamf Pro Administrator's Guide*.

    > **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.

12. Click **Save**.

    The policy runs on computers in the scope the next time they check in with Jamf Pro 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 macOS 10.13 and have an existing, valid personal recovery key that matches the key stored in Jamf Pro.

To disable the management account for FileVault, the computer must have macOS 10.13.

Important: Management Accounts cannot be enabled or disabled for FileVault on computers with macOS 10.13.2 or later.

Enabling or Disabling the Management Account for FileVault

1. Log in to Jamf Pro.
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** + New .
5. In the General payload, enter a display name for the policy. For example, “Enable Management Account for FileVault“.
6. Select a trigger and execution frequency.
7. Select the Management Account payload and click **Configure**.
8. Select one of the following:
   a. **Enable User for FileVault 2**
   b. **Disable 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. For more information, see Scope in the *Jamf Pro Administrator's Guide*.

    > **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.

11. Click **Save**.

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

Accessing Encrypted Data

FileVault allows you to access and recover 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 icon 🔓 and enter your password to make changes.
6. Select the primary account in the sidebar and click the **Reset Password** button.
7. Enter and verify the new password. 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 "Unlock “Macintosh HD” or "Turn Off Encryption" from the **File** pop-up menu. Choose
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 Jamf Pro and convert it to a . keychain file. For more information, see the Converting a RecoveryKey.p12 File to a FileVaultMaster.keychain File Knowledge Base article.

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.