Getting Started with FileVault in FileWave

> MDM enrollment is required. FileWave manages FileVault on macOS devices enrolled through Automated Device Enrollment (formerly DEP) or through a manually installed MDM profile.

These advanced steps are for system administrators and others who are familiar with the command line and FileWave.

What you need to begin

- A supported FileWave release
- A supported macOS device enrolled in FileWave MDM
- An approved recovery-key strategy: Personal Recovery Key (PRK), Institutional Recovery Key (IRK), or both

What is FileVault 2

FileVault full-disk encryption (FileVault 2) uses XTS-AES-128 encryption with a 256-bit key to help prevent unauthorized access to the information on your startup disk.

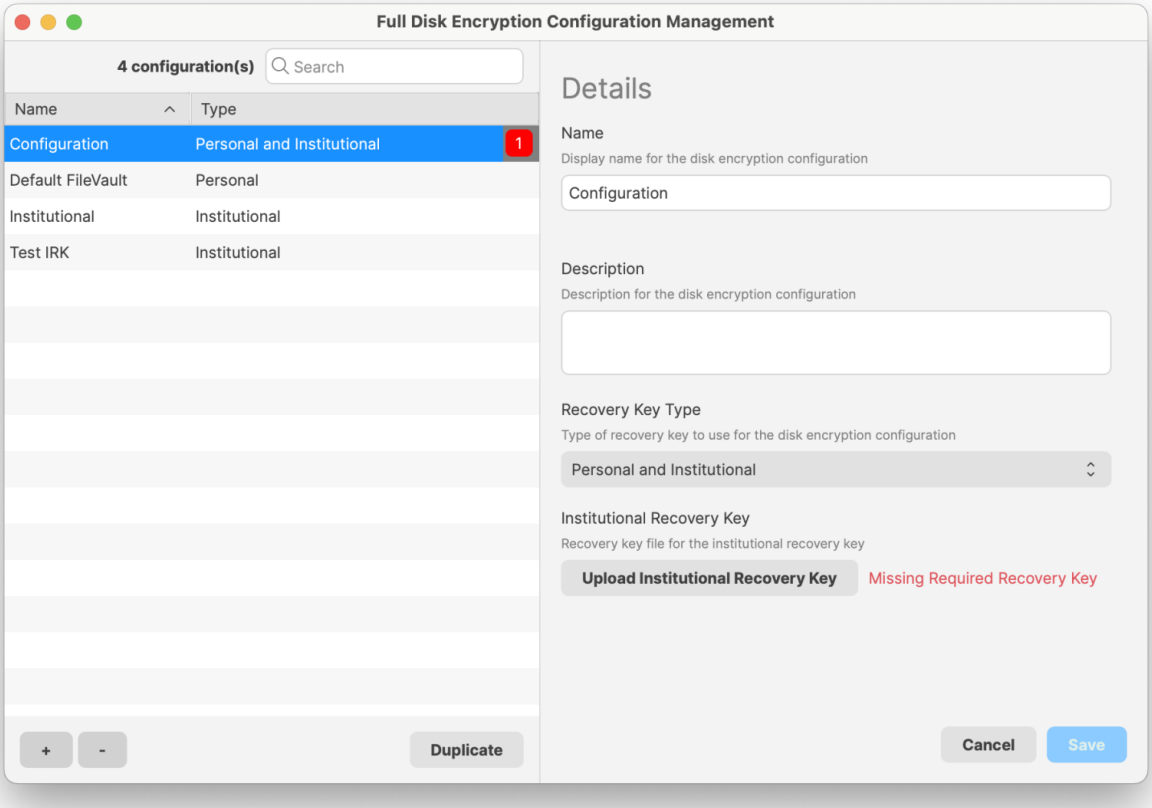
FileVault 2 has three different decrypting mechanisms:

- If a user is a part of "FileVault users", successful login unlocks FileVault
- A Personal Recovery Key (PRK) can be generated for each user and used to unlock FileVault
- An Institutional Recovery Key (IRK) - which is actually a cryptographic key pair - can be used to unlock FileVault

Setup

Full Disk Encryption Assistant

- Open FileWave Central.
- Go to Assistants → Full Disk Encryption Management → FDE Configuration Management...



- Once you click the "+" on the bottom left you will then be able to select the recovery key type on the right
  - Personal (PRK): This will prompt the user their "FileVault Recovery Key" that the end-user will need to keep for decryption (FileWave will be able to escrow this key later)
  - Institutional (IRK): A key will need to be created on your macOS device and then imported into the Disk Encryption Configurations window. Please follow the steps below

Institutional Key Creation and Import

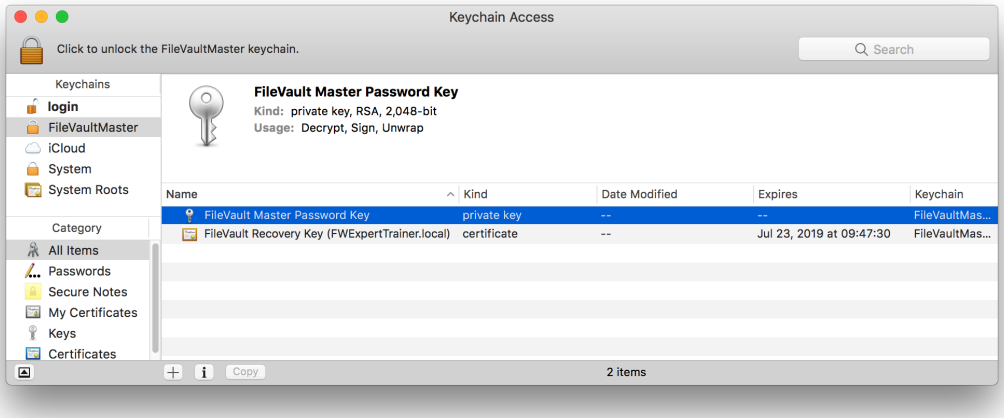
Create an IRK keychain using the following command

```
sudo security create-filevaultmaster-keychain ~/Desktop/FileVaultMaster.keychain
```

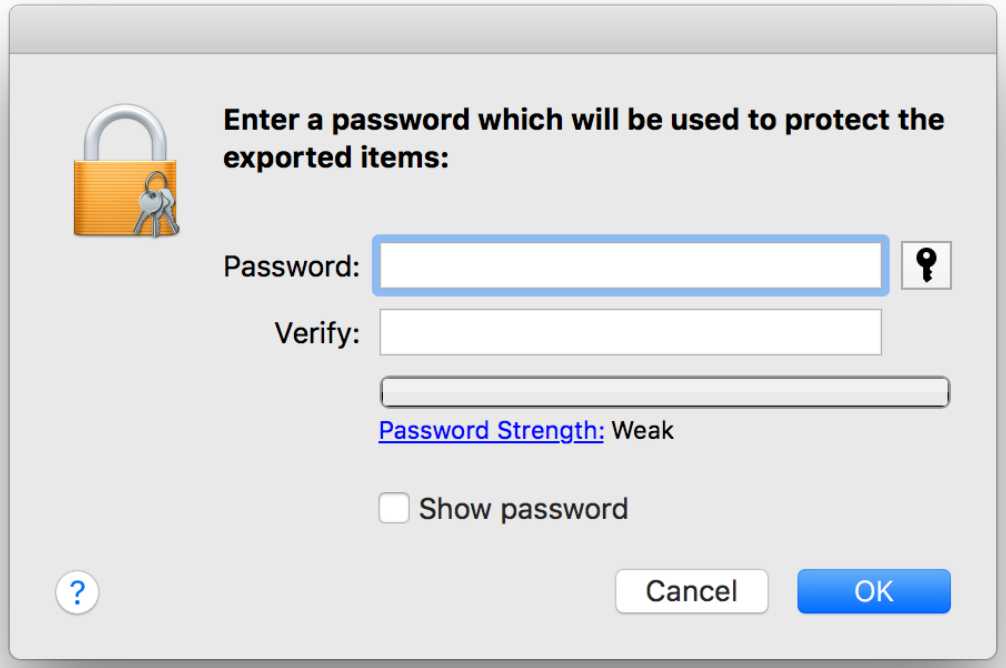
- Unlock the keychain

```
security unlock-keychain ~/Desktop/FileVaultMaster.keychain
```

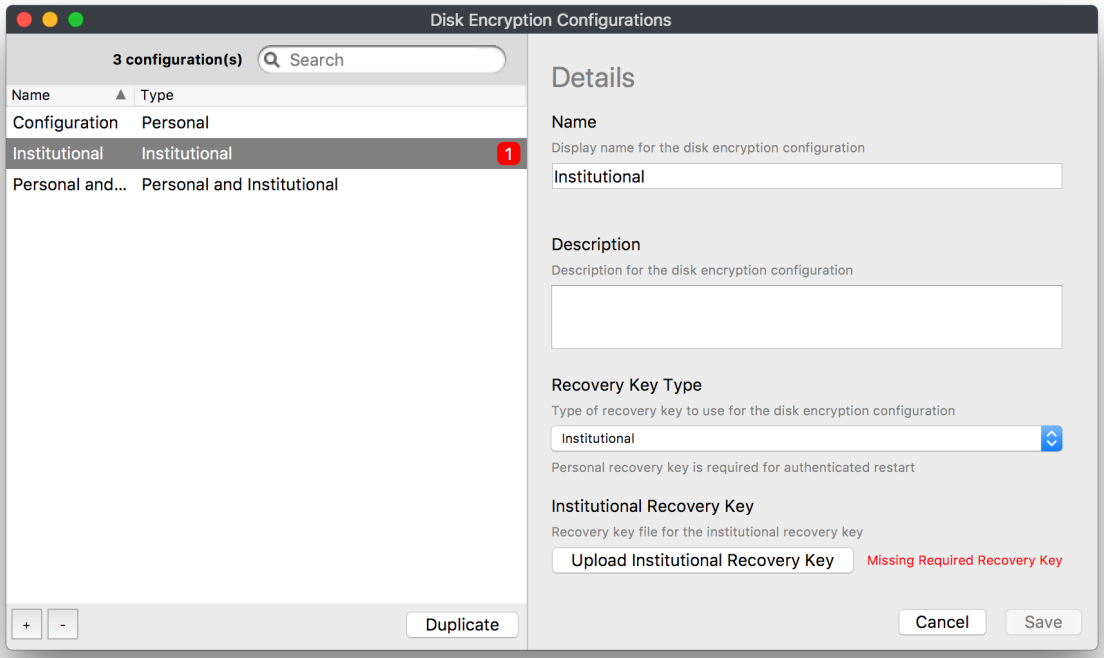
- Open Keychain Access Utility and Add (File > Add) the keychain you just created above



- Select the keychain you just added - it should contain both certificate and private key; select both and export both as .p12 file - protect the file with a password



- Back in the Disk Encryption Configurations window upload the p12 key you just created.

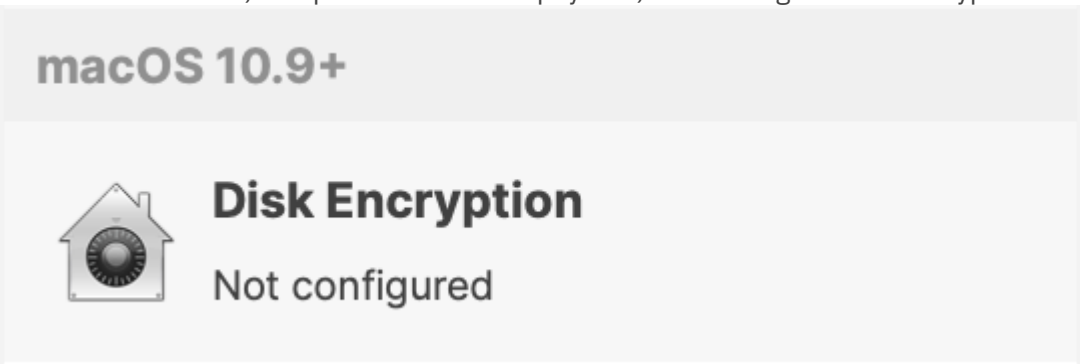


    - Personal and Institutional (IRK and PRK): Provides the end user a personal key and the institutional key can be used as well
- Save

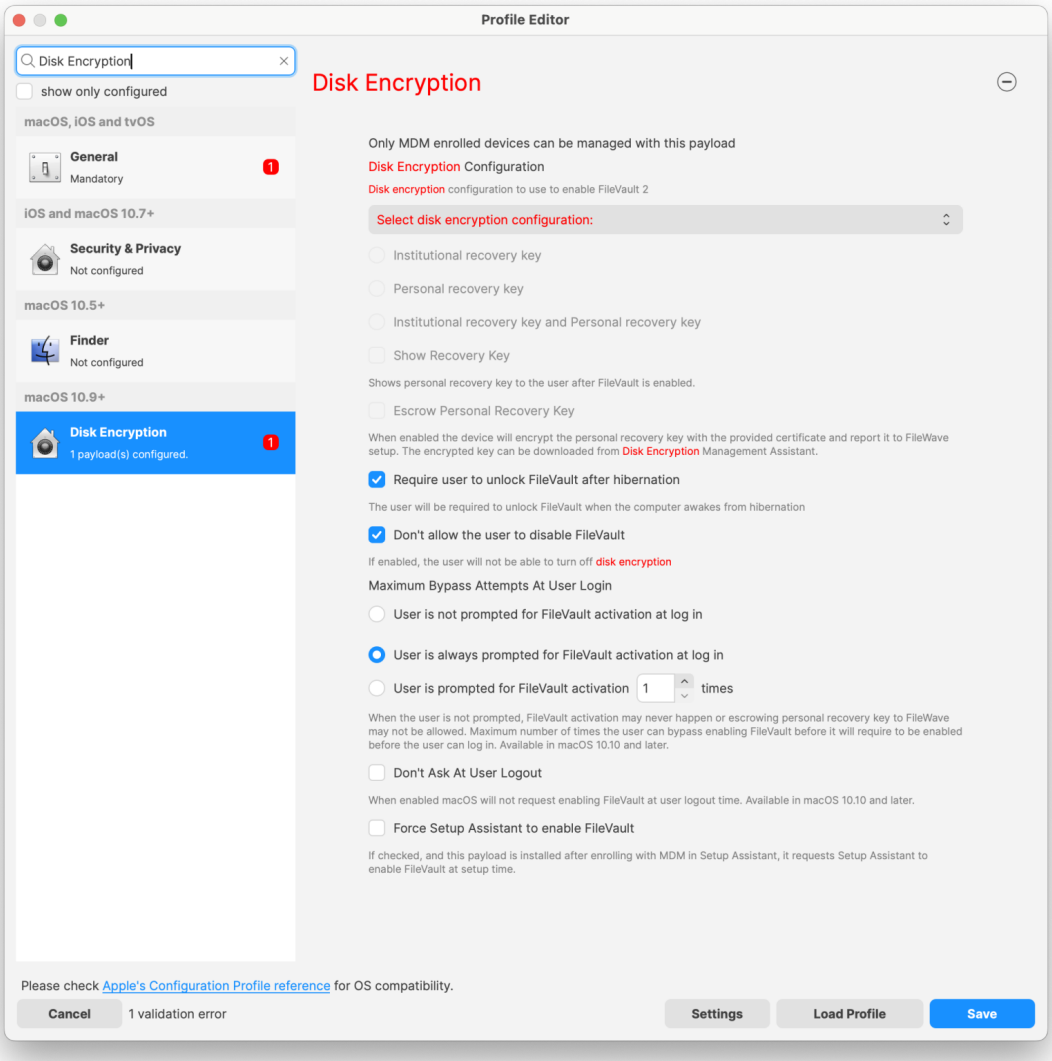
Disk Encryption Profile

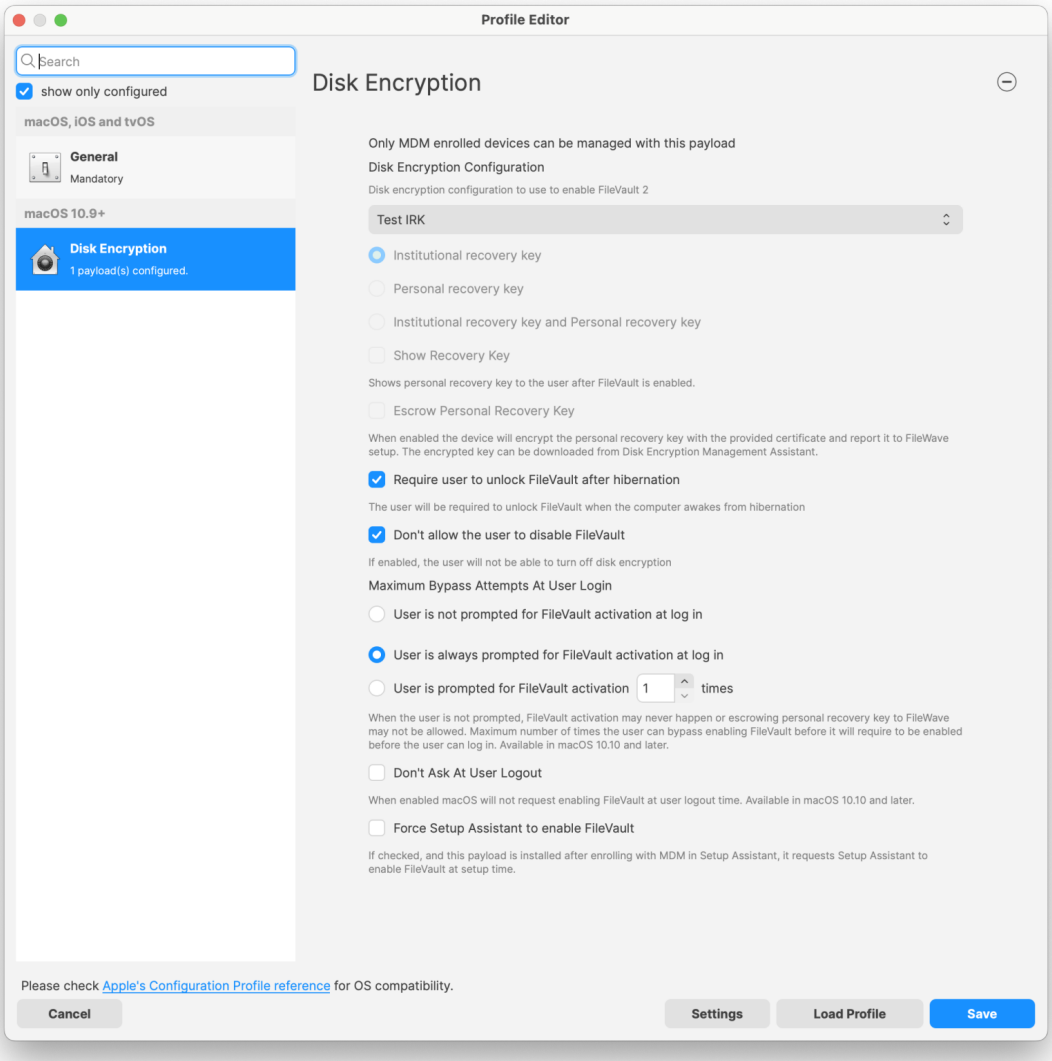
Next, we will need to set up the Apple Profile that will configure and set up FileVault 2. Again your devices need to be MDM enrolled for this payload.

- Go to Filesets → New Desktop Filesets → Profile
- In the Profile Editor, complete the General payload, then configure Disk Encryption.



- Now is the time to configure your FileVault 2 payload
  If you are using the Escrow Personal Recovery Key you are required to put a description in the Escrow Location Description (macOS 10.13+) pane. This description can be informing the user where the key gets stored by default, which is /var/db/FileVaultPRK.dat. Or the description can be letting the user know to contact the technology department for more information.


Profile Editor
Disk Encryption
show only configured
macOS, iOS and tvOS
General
Mandatory
1
iOS and macOS 10.7+
Security & Privacy
Not configured
macOS 10.5+
Finder
Not configured
macOS 10.9+
Disk Encryption
1 payload(s) configured.
1
Disk Encryption
Only MDM enrolled devices can be managed with this payload
Disk Encryption Configuration
Disk encryption configuration to use to enable FileVault 2
Select disk encryption configuration:
Institutional recovery key
Personal recovery key
Institutional recovery key and Personal recovery key
Show Recovery Key
Shows personal recovery key to the user after FileVault is enabled.
Escrow Personal Recovery Key
When enabled the device will encrypt the personal recovery key with the provided certificate and report it to FileWave setup. The encrypted key can be downloaded from Disk Encryption Management Assistant.
Require user to unlock FileVault after hibernation
The user will be required to unlock FileVault when the computer awakes from hibernation
Don't allow the user to disable FileVault
If enabled, the user will not be able to turn off disk encryption
Maximum Bypass Attempts At User Login
User is not prompted for FileVault activation at log in
User is always prompted for FileVault activation at log in
User is prompted for FileVault activation 1 times
When the user is not prompted, FileVault activation may never happen or escrowing personal recovery key to FileWave may not be allowed. Maximum number of times the user can bypass enabling FileVault before it will require to be enabled before the user can log in. Available in macOS 10.10 and later.
Don't Ask At User Logout
When enabled macOS will not request enabling FileVault at user logout time. Available in macOS 10.10 and later.
Force Setup Assistant to enable FileVault
If checked, and this payload is installed after enrolling with MDM in Setup Assistant, it requests Setup Assistant to enable FileVault at setup time.
Please check Apple's Configuration Profile reference for OS compatibility.
Cancel
1 validation error
Settings
Load Profile
Save



Important configuration limits
* Avoid User is not prompted for FileVault activation at login; FileVault may never fully activate when the user is not prompted.
* Keep the FileVault payload in its own profile rather than combining it with other payloads.
* Create FileVault settings through the Assistant and Full Disk Encryption payload. Imported profiles containing FileVault settings cannot be used directly.
* Escrow Personal Recovery Key is required for Authenticated Restart and for FileWave to store the PRK.

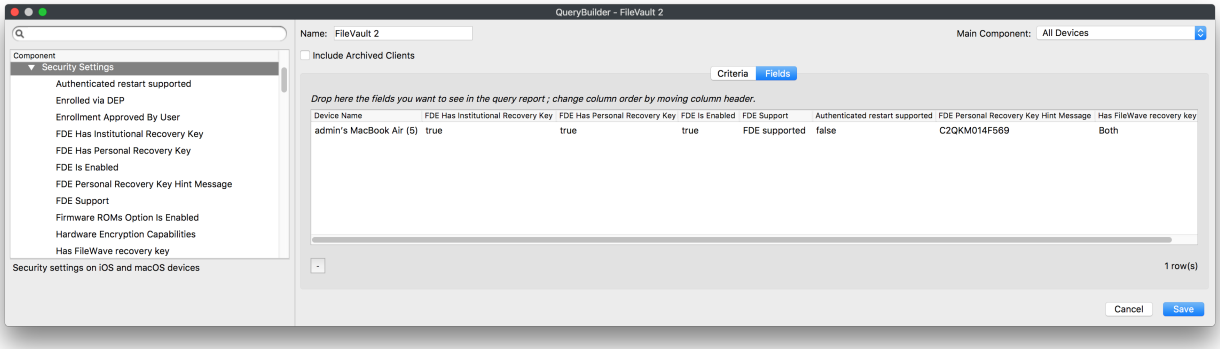
- From this point, you are ready to deploy this profile to your MDM enrolled macOS devices.

Disk Encryption Inventory Information

Now that you have FileVault 2 enabled on your device(s) you can view inventory pulled from the device(s) regarding the FileVault 2 settings:

- FDE Has Institutional Recovery Key
- FDE Has Personal Recovery Key
- FDE Is Enabled

- FDE Support
- Authenticated restart supported
- FDE Personal Recovery Key Hint Message
- Has FileWave recovery Key



Disk Encryption Recovery Key Escrow

When FileVault 2 is enabled FileWave will keep track of the configuration applied to the corresponding keys such as the Institutional Recovery Key (IRK) used to encrypt the disk and the Personal Recovery Key (PRK).

To manage these keys go to Assistants → FDE Recovery Key Management...

Once you select a device you will be able to Show Personal Recovery Key... or Download Institutional Recovery Key... depending on what configuration was used to set up FileVault on that machine.

You can also delete outdated entries but keep in mind if a device has FDE managed by FileWave, it's not possible to remove FDE keys from the assistant. You have to disable FDE or remove the device from FileWave first.

Status can be:

- Disabled
- Enabled
- Pending - this is the state reported by a device between the profile installation and when FDE actually being enabled

PRK Status can be:

- Valid
- Cannot decrypt
- Invalid - no key or not a valid key

Authenticated Restart

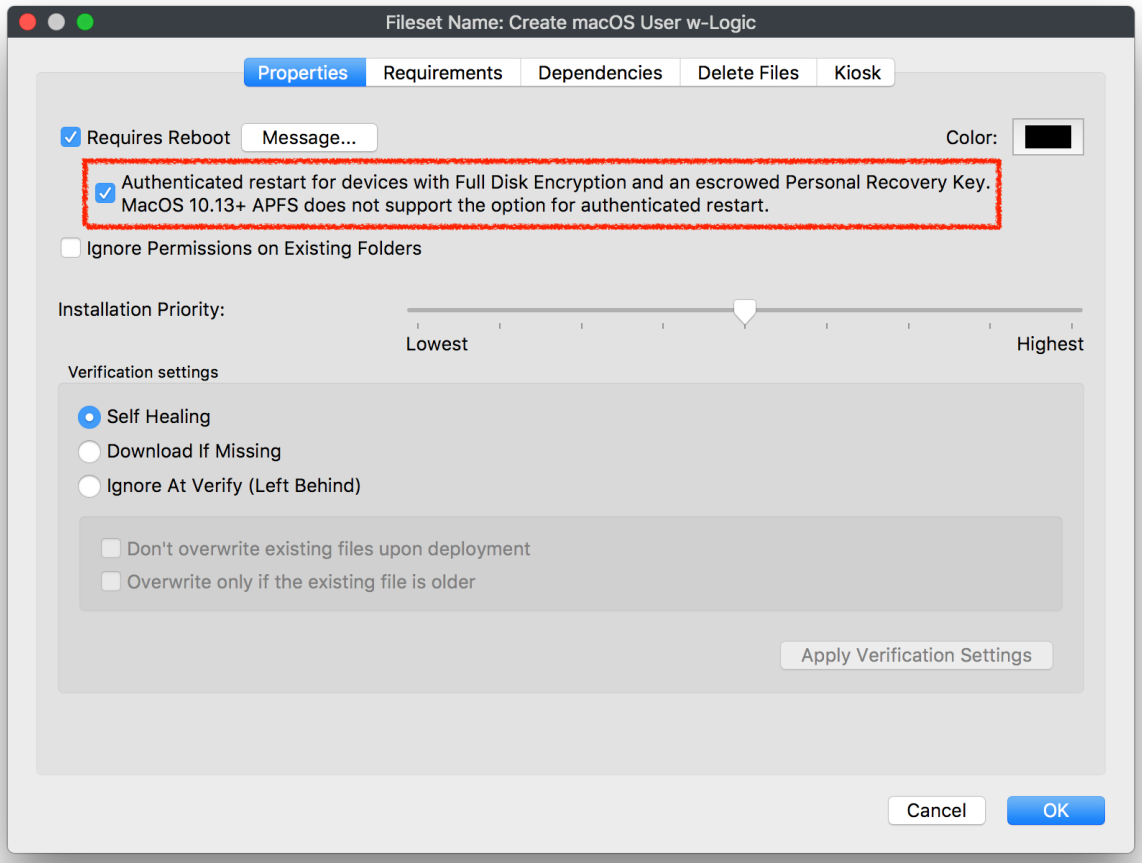
> macOS 10.13 NOT SUPPORTED
> Authenticated restart using Personal Recovery Key does not work on macOS 10.13+ on APFS
> This option is for Personal Recovery Key only; Institutional Keys are not supported with this option

When FileVault 2 is enabled, the device will be locked on startup. At this stage, FileWave does not connect to the device until the drive is unlocked. You need to be aware of this if you have FileVault 2 enabled on a device and then send out a Fileset that requires a reboot! After the reboot, the end-user will have to unlock the drive before the deployment can finish.

FileWave may be able to help with this using Authenticated Restart as a Fileset option. If you selected the option Escrow Personal Recovery Key when you created the Disk Encryption Profile to enable FileVault 2 then FileWave will be able to use the authenticated restart to unlock the drive without user interaction.

This option is located in the Fileset Properties for any Fileset you are requiring a reboot for.

Right-click on Fileset → Properties → Select Requires Reboot



Possible Security Risk
Keep in mind using this option can be seen as a security risk and should be used accordingly. The device will reboot unlocked so access to encrypted data is possible and until the device reboots, an escrow key is stored in memory but still encrypted.

Recent versions of macOS for FileVault IRKs

The use of Institutional FileVault keys, also known as Institutional Recovery Keys (IRK), is no longer recommended in recent versions of macOS, including macOS Ventura. The utility of IRKs for organizations has become limited, particularly on Macs with Apple Silicon, where IRKs provide no functional value. This is because IRKs can't be used to access recoveryOS, and because Target Disk Mode is no longer supported, the volume can't be unlocked by connecting it to another Mac.

Instead, the use of a Personal Recovery Key (PRK) is now recommended. A PRK provides an extremely robust recovery and operating system access mechanism, unique encryption per volume, escrow to MDM, and easy key rotation after use.

Moreover, there is only one PRK per encrypted volume. During FileVault enablement from MDM, the PRK can optionally be hidden from the user. When configured for escrow to MDM, MDM provides a public key in the form of a certificate, which is then used to asymmetrically encrypt the PRK in a CMS envelope format. The encrypted PRK is returned to MDM in the security information query, which can then be decrypted for viewing by an organization. Many MDM vendors provide the option to manage these keys to allow for viewing directly in their products. MDM can also optionally rotate PRKs as often

as is required to help maintain a strong security posture—for example, after a PRK is used to unlock a volume

> Additional information managing FileWave in macOS: Managing FileVault in macOS
> Information regarding recent versions of macOS managing FileVault: Manage FileVault with mobile device management

Related Content

- Bootstrap Token Management on macOS
- Deprecation of Institutional Recovery Keys

Revision #8
★Created 2023-07-14 20:13:26 UTC by Josh Levitsky
Updated 2026-08-07 12:55:53 UTC by Josh Levitsky