Jamf Pro - FileVault 2 Encryption

Jamf Pro - FileVault 2 Encryption

To encrypt your Macs with FileVault 2 follow these steps. Note that all FV2 enabled accounts will now show up at the login screen which may cause some initial confusion for the end user.

To encrypt:

- Log in to the JSS. Go to computers, then policies. Click **New**.
    - Give the policy a name, such as "DepartmentName Encryption."
    - Assign a category.
    - Click on **Disk Encryption** on the left, then configure.
        - Ensure IS&T FileVault 2 is selected from the **Disk Encryption Configuration** drop-down.
    - Click on **Restart Options** on the left.
    - Change **User Logged in Action** to restart immediately.
    - Click on **Scope** at the top.
        - Assign an appropriate scope, such as "all computers." Otherwise, target individual machines or smart groups.
    - Click on **Self Service** at the top. This will add the policy to self-service and can then be run at the end users convenience.
        - Check *Make the policy available in Self Service*.
        - Add a description if desired. You may want to also click the **Ensure that users view the description** box is checked.
        - Check *Feature the policy on the main page.* This will ensure users can find it easily.
    - Click on **User Interaction** at the top.
        - Change the restart message to something like "Your machine will restart immediately. Please save any open work."
    - Click **Save**.

User Issues

By default, the only account that will be able to unlock the disk will be the user who encrypts the machine. This means the local admin account will no longer be able to log in. This can be fixed manually on the target computer:

- Open System Preferences
- Go to *Security & Privacy*
- Click on **FileVault**, then click the **Enable Users** button.
    - If you do not see the "Enable Users" button, that means that all users are already enabled.

Access Recovery Key

- Log in to the JSS
- Go to Computers.
    - Search for the computer name or serial number in the search box, then click on it.
- If user doesn't know hostname or serial, go to **Users** and search for Kerberos ID. Select user and select their machine.
    - Once you have found machine, go to the **Management** tab at the top.
        - Click **FileVault 2** on the left.
        - Click **Get FileVault 2 Recovery Key**.