### Code42 Backups

#### **Requirements For Install**

* Valid username in Jamf. The username must exist in Okta. the username must correlate to the email address of the user.
* “code42 - backupEngine - ALL” Configuration Profile
  + Provides all the needed PPPC requirements
* “code42 - userAssignment - ALL” Configuration Profile
  + Takes the email address data from the “User and Location” to assign the computer to the user listed

#### **Install**

Code42 is installed on every endpoint (excluding mac minis) at the Collective that meets certain requirements:

1. Have a valid username in the jamf record
2. The profiles “code42 - backupEngine - ALL” and “code42 - userAssignment - ALL” are present.
   1. The above profiles depend on a valid username in the Jamf record.

The backup agent is installed during the initial computer setup process using the policy “[Install\_Code42\_ARM](https://emersoncollective.jamfcloud.com/legacy/policies.html?id=224&o=r)” or “[Install\_Code42\_Intel](https://emersoncollective.jamfcloud.com/legacy/policies.html?id=264&o=r)” for the respective CPUs. Both have the same custom trigger “install\_code42”. The Intel install policy excludes the Apple Silicon(ARM) policy and the Apple Silicon policy excludes the Intel policy.

The policy runs when the custom trigger is used (ex: During the Set Up Your Mac script) or at check-in. If the policy fails, it will retry up to 6 times at the computer’s next check-in.

**Note: Jamf does not assign a user to the computer if a member of the IT team sets up the computer. This is by design to avoid computers getting assigned to the wrong user.**

If the policy fails, check the logs by following these steps:

1. Find the computer in Jamf
2. Select “History” in the top row
3. Select Policy Logs
4. Find the policy and select “Details”. It will show you the outcome of the script potentially showing a reason it failed.

#### **Verify Functionality**

#### **Uninstall**

***Uninstalling manually should only be done by a system administrator and not performed without a reinstallation of the backup agent.***

Copy and paste the following commands.

 sudo launchctl unload /Library/LaunchDaemons/com.code42.service.plist   
 sudo chflags noschg /Applications/Code42.app  
 sudo chmod -R 755 "/Library/Application Support/CrashPlan/"



Open a Finder window and delete the following files and folders:

/Library/LaunchDaemons/com.code42.service.plist  
 /Applications/Code42/  
 /Library/Caches/CrashPlan/  
 /Library/Application Support/CrashPlan/



#### **Repair**

If a backup agent isn’t reporting incorrectly, it must be repaired. Before trying to repair the agent, make sure the computer is reporting into jamf, the employee hasn’t been offboarded, and offboarding is in process and finally, check for zendesk tickets if the computer has been replaced. Often a computer isn’t reporting in due to one of the factors listed above. The best way to repair an agent is to uninstall and reinstall. We do have a Jamf policy that will accomplish this.

1. Go to Static Groups in Jamf.
2. Find [Code42 Backup - Repush](https://emersoncollective.jamfcloud.com/legacy/staticComputerGroups.html?id=474&o=r)
3. Add the necessary computer to the group.
   1. If the computer is already added, go to the computer record and find the policy “[Install\_Code42\_Arm one off](https://emersoncollective.jamfcloud.com/legacy/policies.html?id=387&o=r)” or “[Install\_Code42\_Intel one off](https://emersoncollective.jamfcloud.com/legacy/policies.html?id=387&o=r)” in the policy history and flush the policy. If the policy isn’t listed in the history, it hasn’t run and may indicate a different issue with the Jamf agent.

#### **Replace a computer**

1. Open the Code42 admin console
2. Select “Administration” then Users
3. Search for the user needed
4. Find the new computer and select “Additional Details” for the Backup Agent.
5. Once in the new computer record, select “Actions” on the right-hand side then “Replace a Computer”
6. Find the old computer, select it, and select “Replace”. Depending on the amount of data, this could take more than a day to complete. However, usually completes in approximately 6 hours. Temporarily, it will appear as though the backup agent on the new computer is gone. This is expected behavior and will return once the replacement is complete. **This process will also deactivate the old backup agent. The deactivated agent will stay in Cold Storage for 180 days.**

#### **Data Restoration**

This can be done from the agent on the computer or from the Admin console.

##### From the agent on the computer

1. Go to Spotlight and open “Code42”. Be cautious not to open “Code42-AAT”. That is the DLP agent.
2. Select “Restore Files” in the top right corner.
3. Select the date you needed files restored from by selecting “As of Today” in the top right.
4. Find the files you want to restore. Select “Restore”.
5. Select the destination, whether or not to rename the file, and the permissions. The default of “Current’ for permissions is usually the best option. Selection of “Original” can have adverse effects especially when restoring to a different computer or account.
6. Select OK.
7. Verify the restore by checking the destination location.

##### From the Admin Console

1. Select ‘Administration” then “Devices”
2. Find the necessary computer in the list or use the search bar in the top right corner.
3. Select the restore icon on the right side of the computer record.
4. Select the type of restore desired (Zip file Download or direct to a device).
   1. Zip File
      1. Select the restore date and necessary files
      2. Select “Restore”
      3. Once the console processes the request, the download will begin.
   2. Direct to Device
      1. Select the target device by entering the computer name. If the console says ”Authority can’t connect to device, restore unavailable”, you may have selected the Insider Risk or DLP agent.
      2. Select the restore path (original location or a specific target).
         1. If “Original Location” is selected, best practice is to select “Current” for Permissions. Selecting “original” can cause unforeseen file/folder permissions issues.
      3. Select the desired action of the file exists (overwrite or rename).
      4. Select the restore date and necessary files
      5. Select “Restore” Depending on the internet connection and amount of data, this may take a significant amount of time.

#### **Decommission an agent**

### Code42 DLP

#### **Install**

#### **Uninstall**

#### **Decommission an agent**

#### **Repair**

### Crowdstrike Falcon

#### **Install**

#### **Uninstall**

#### **Repair**

### Jamf

#### **Install (macs)**

#### **Uninstall (macs)**

#### **Repair (macs)**

#### **Install (mobile)**

#### **Uninstall (mobile)**

#### **Repair (mobile)**

### Software updates

#### **User Endpoints**

#### **Infrastructure Machines**

### Endpoint setup Process