SLASHNEXT

USER GUIDE V1.0.1

SlashNext macOS Jamf Guide

TABLE OF CONTENTS

1 | INTRODUCTION

In this guide, the process of browser extensions deployment via Jamf UEM is explained. It consists of three steps as given below.

1. User configuration (.plist) deployment
2. Package deployment using policies
3. Profile/Installer deployment

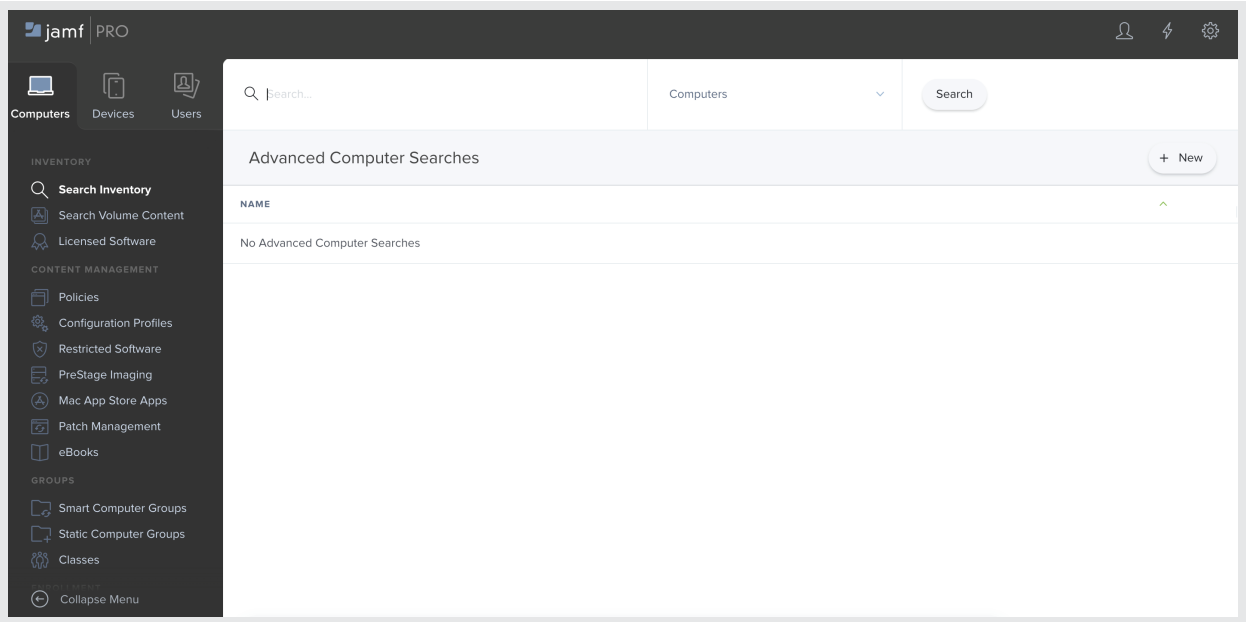
Note

The order of execution for the above steps is mandatory. They should be executed as listed from top to bottom, otherwise, auto-activation will not be performed and users have to do it manually.

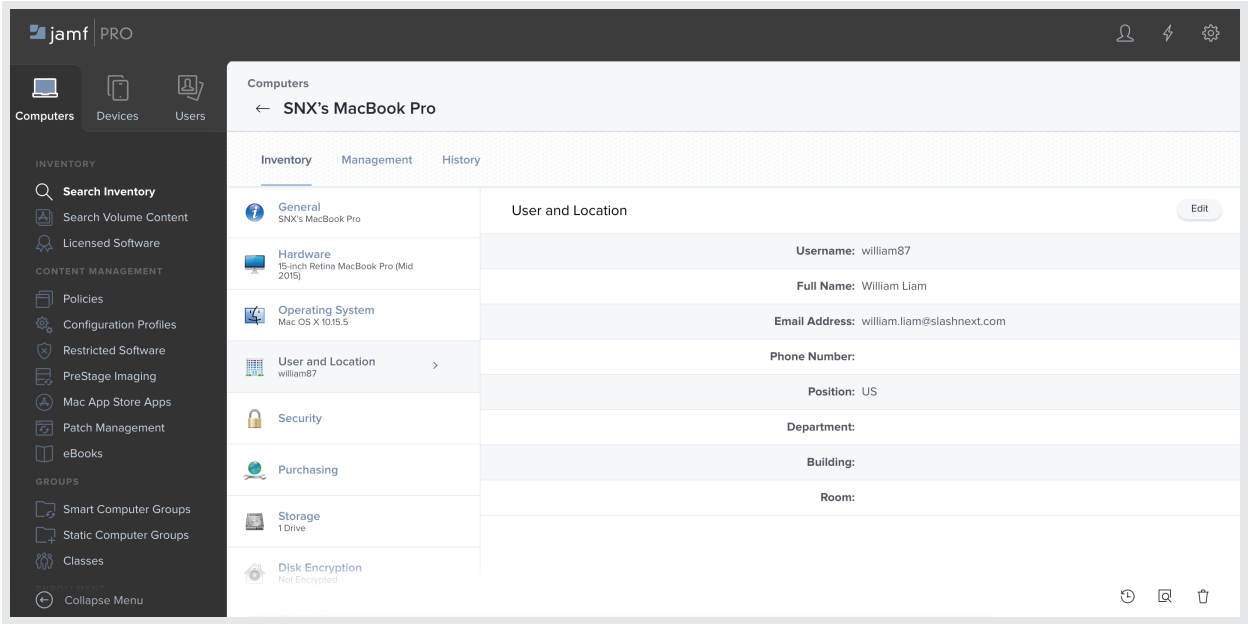
2 | USER CONFIGURATION (.PLIST) DEPLOYMENT

A property list file that contains enrolled user information such as (Email, Username, and company Id), when this file will be deployed to the machine of an enrolled user, the user information that is associated with that particular enrolled machine is also gets deployed to the machine. This information is required to perform auto-activation based on the keys enclosed in the property list file. Make sure that the user information is associated with the enrolled machine on Jamf Portal. To check if it is associated, follow the below steps.

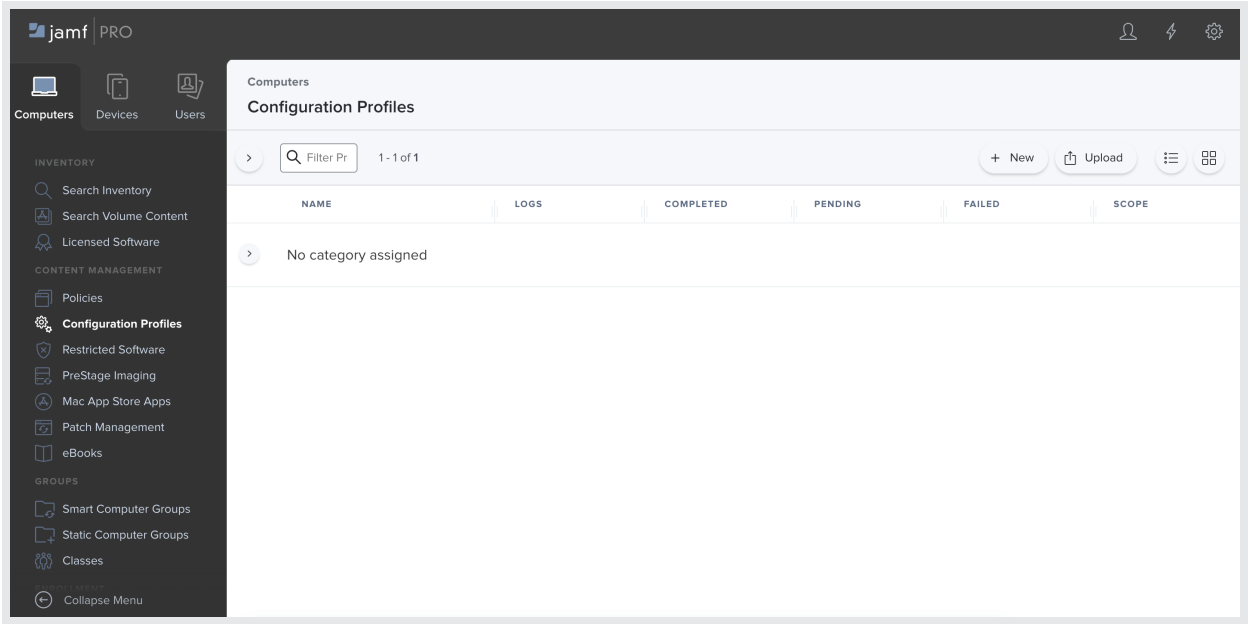
1. Select **Computers** and click on **Search Inventory**.



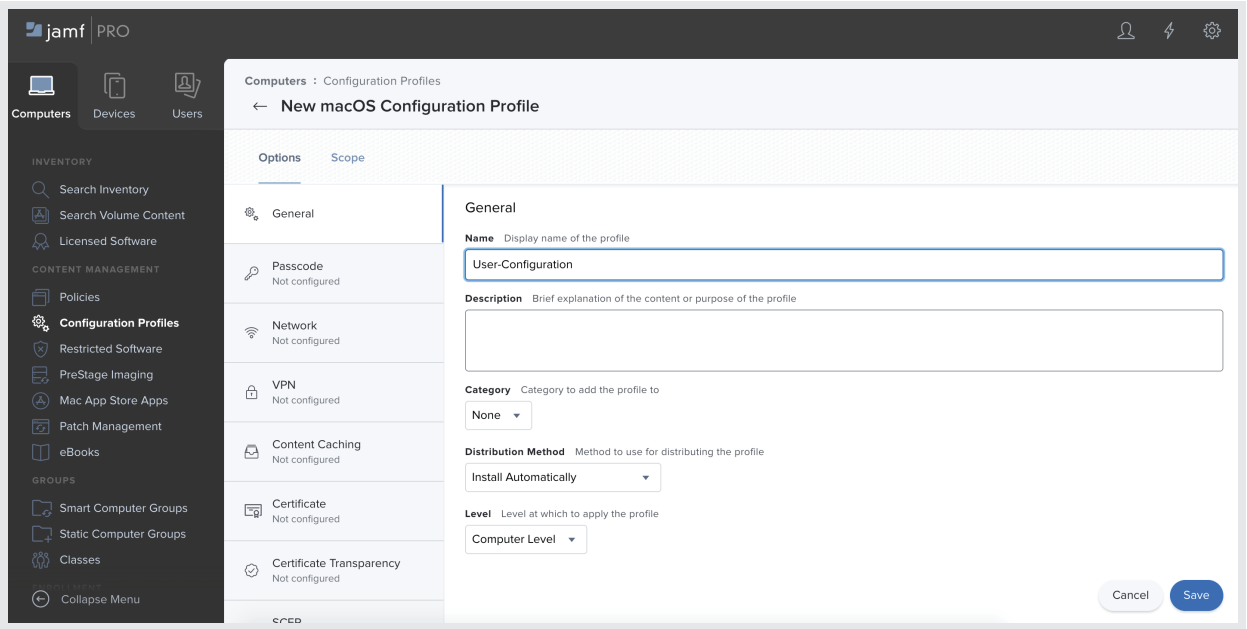
2. Select **Computers** from the drop down and click on **Search**. A list of available computers will show up in the list. Select the target computer and click on its **User and Location**. Now check if the user information is associated or not. If it's not then **Edit** the fields and add useful information such as (email, username, full name, and position). Once all completed, the window should appear as below screenshot.



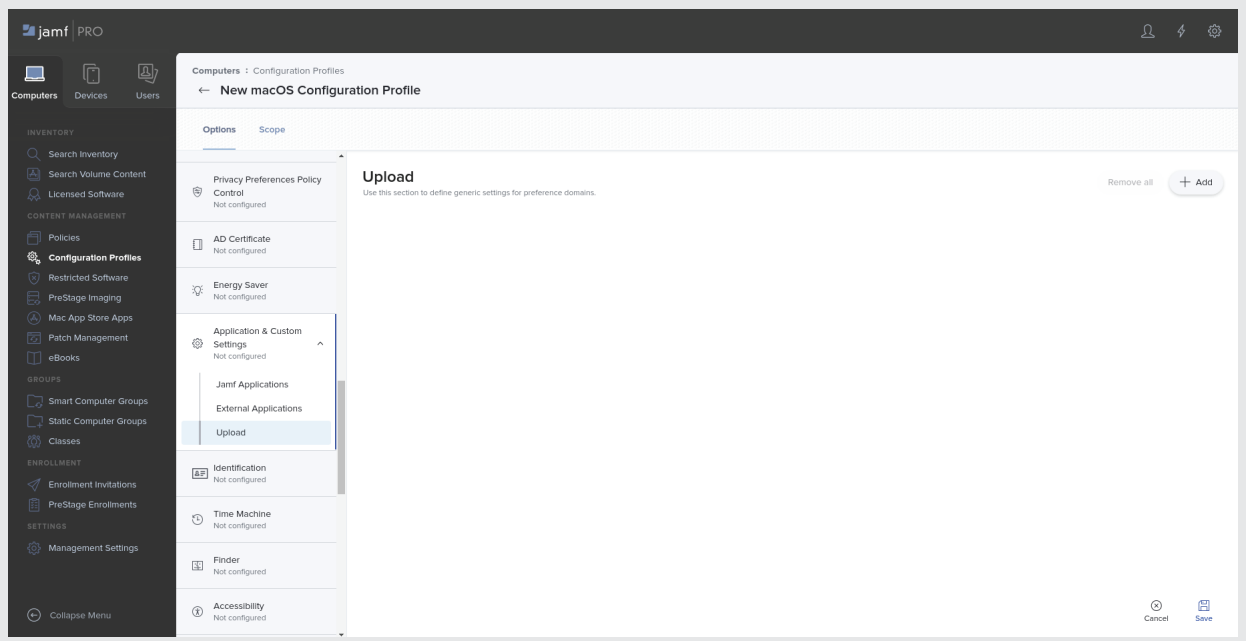
3. The next step is to upload .plist file. For that go to **Configuration Profiles** under the **Computers** option.



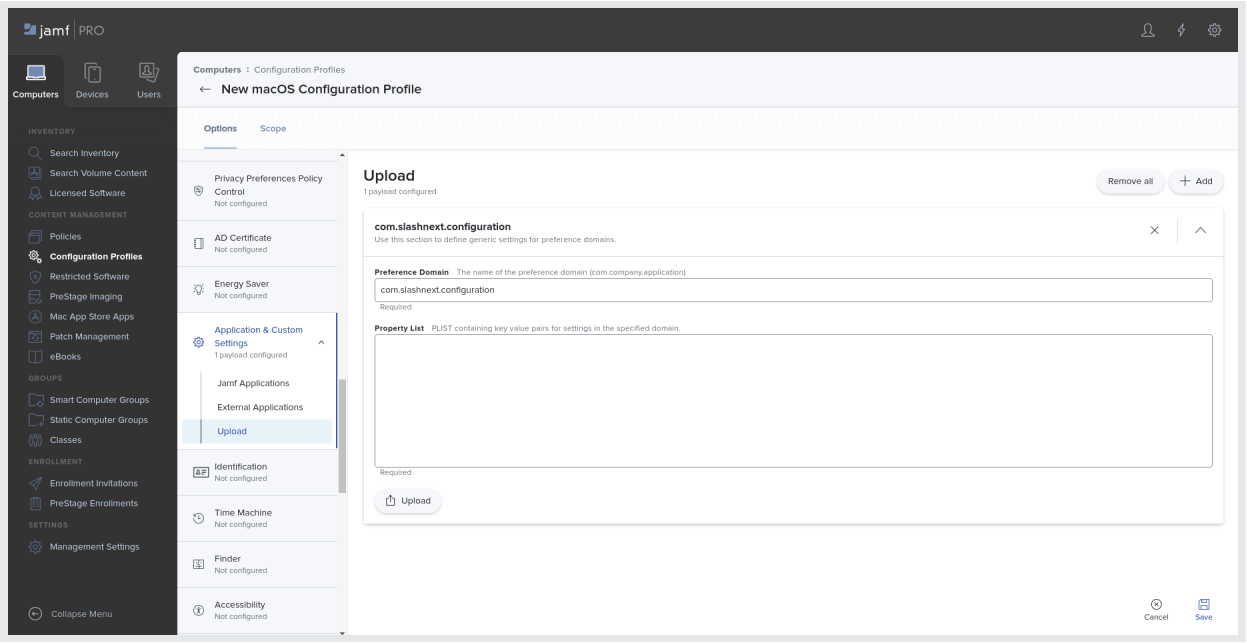
4. Now click on **New** to add a new configuration. A window will appear to add certain settings under this configuration. Add the name of the configuration and leave other fields as it is.



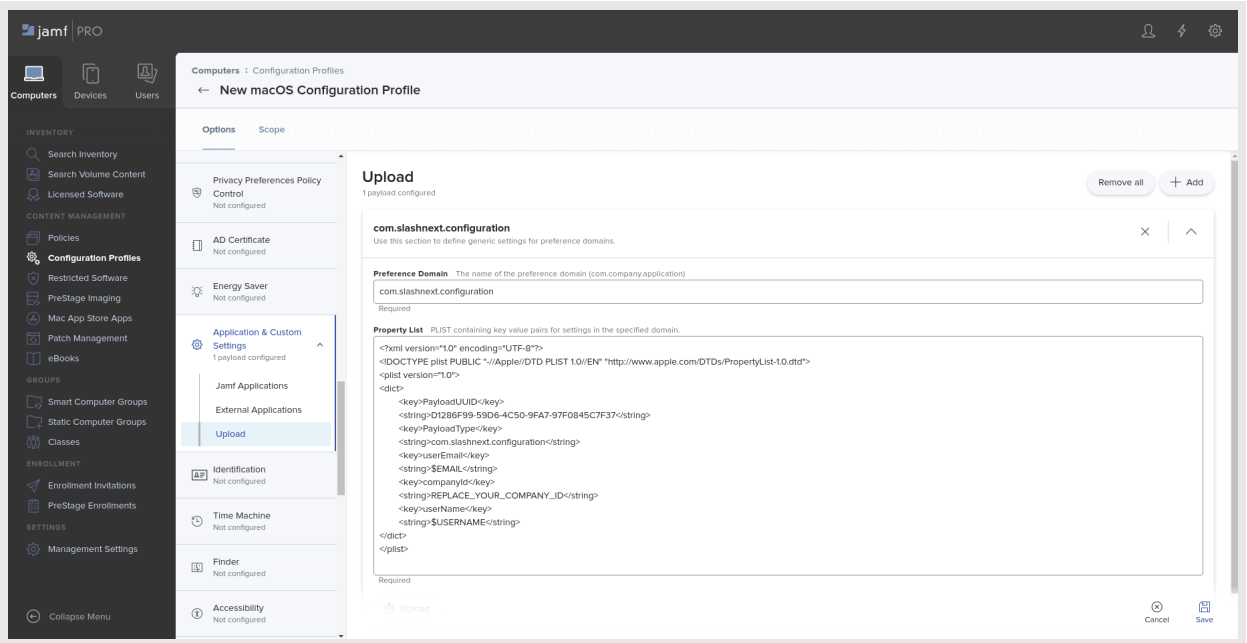
5. Scroll down in the options section, select **Upload** under **Application & Custom Settings** and click on the **+Add** button.



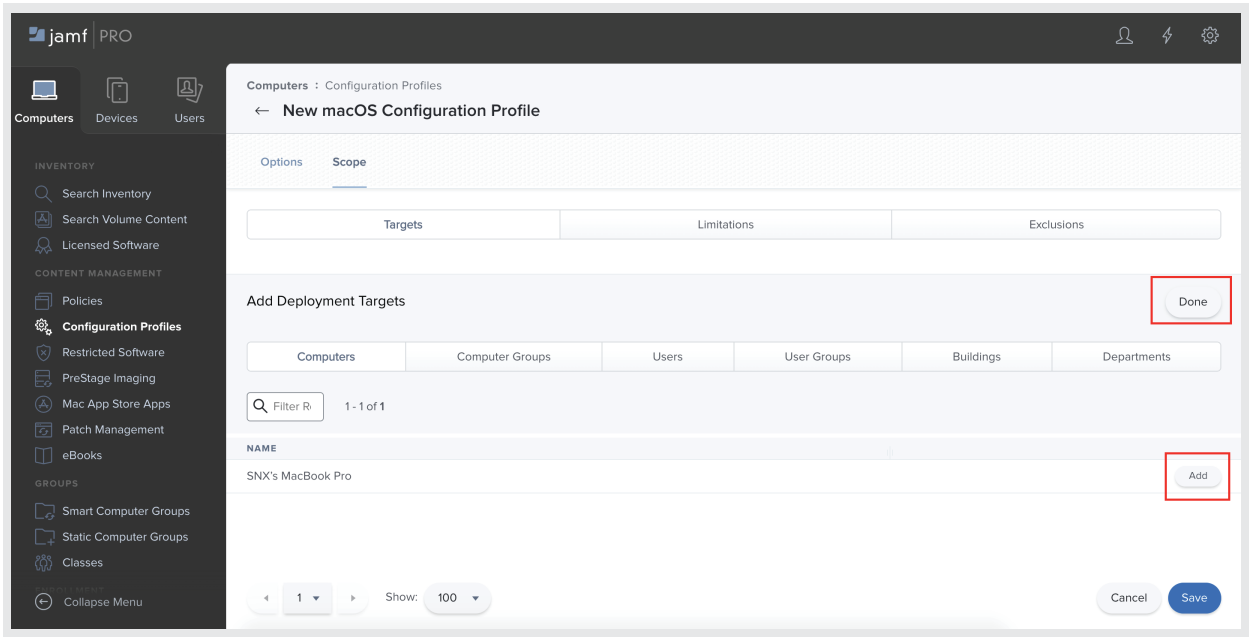
6. Enter the preference domain name as **"com.slashnext.configuration"**, this name should be the same as it will be used for reading purpose. Next, click on **Upload** and select the .plist file from the provided macOS app bundle.



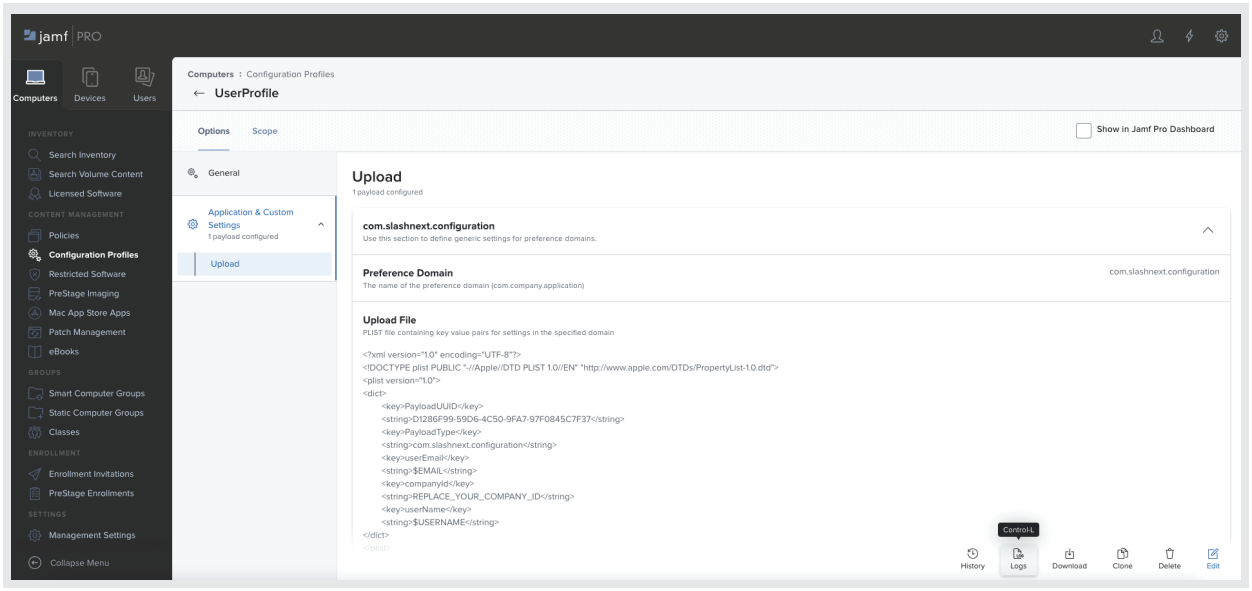
7. Once done, the window will appear as below screenshot.



8. The next step is to assign this configuration to any enrolled machine. To achieve this select **Scope** and click on **Add**. The available machines will show in the list, select the target machine, and click on **Add** and then **Done**. In the last click on **Save**.

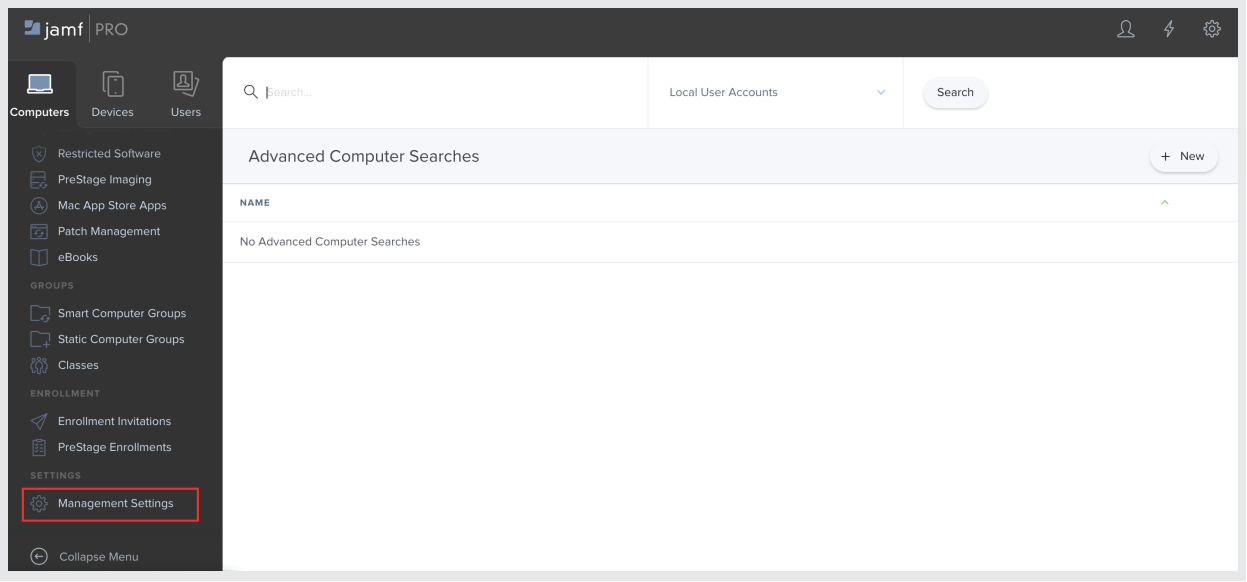


9. Before going to the next step make sure that user configuration (.plist) is deployed. This can be verified by clicking on the **logs** as mentioned in below screen shot.

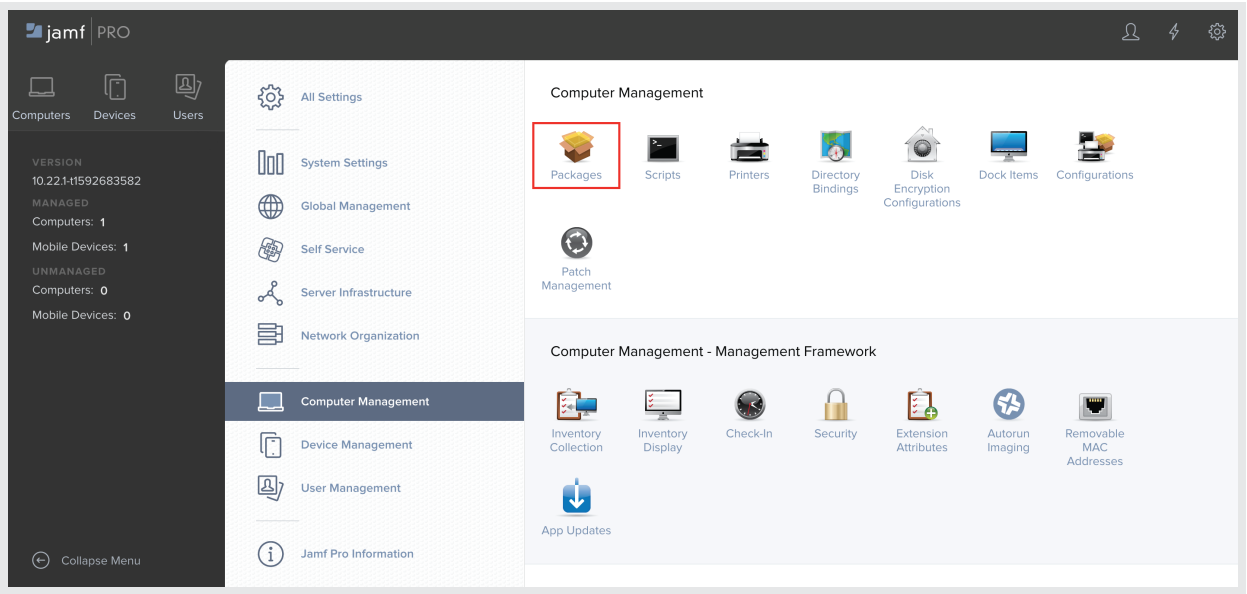


3 | PACKAGE DEPLOYMENT USING POLICIES

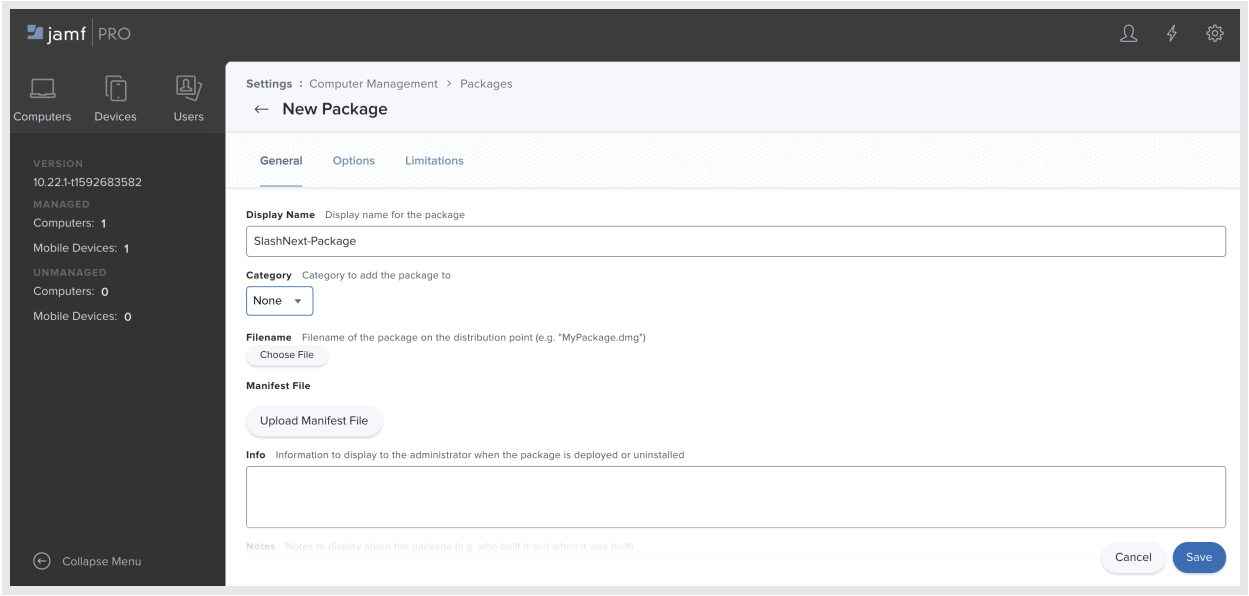
1. Once the .plist file is deployed successfully, go to **Management Settings** under **Computers**.



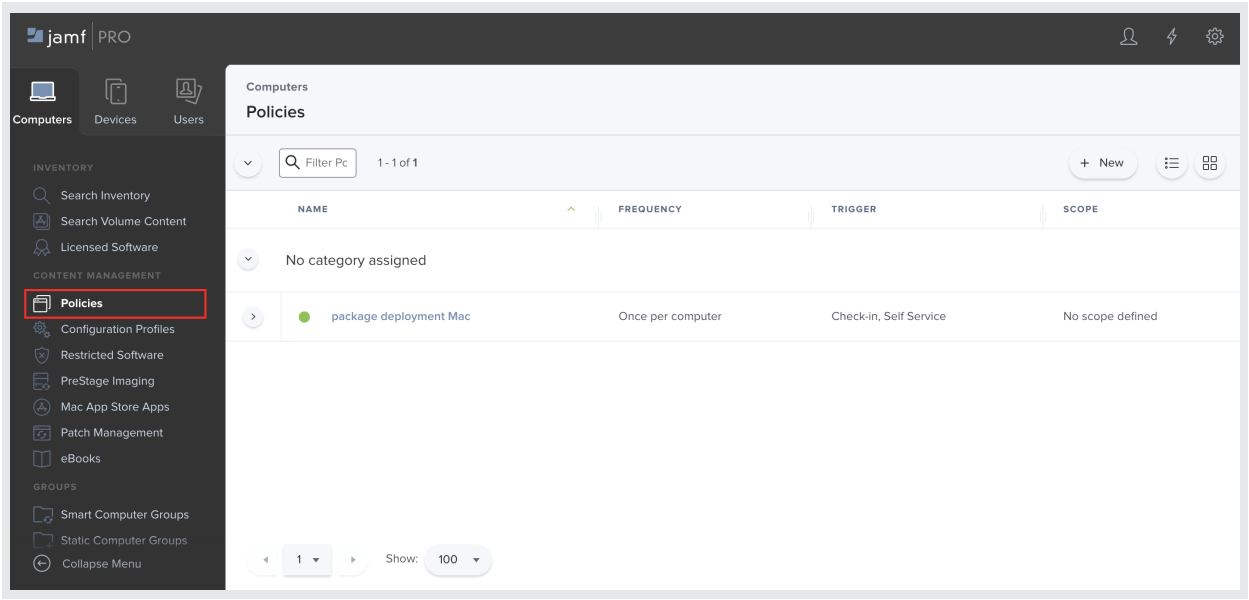
2. A setting window will open, on it select **Computer Management** and then select **Packages**.



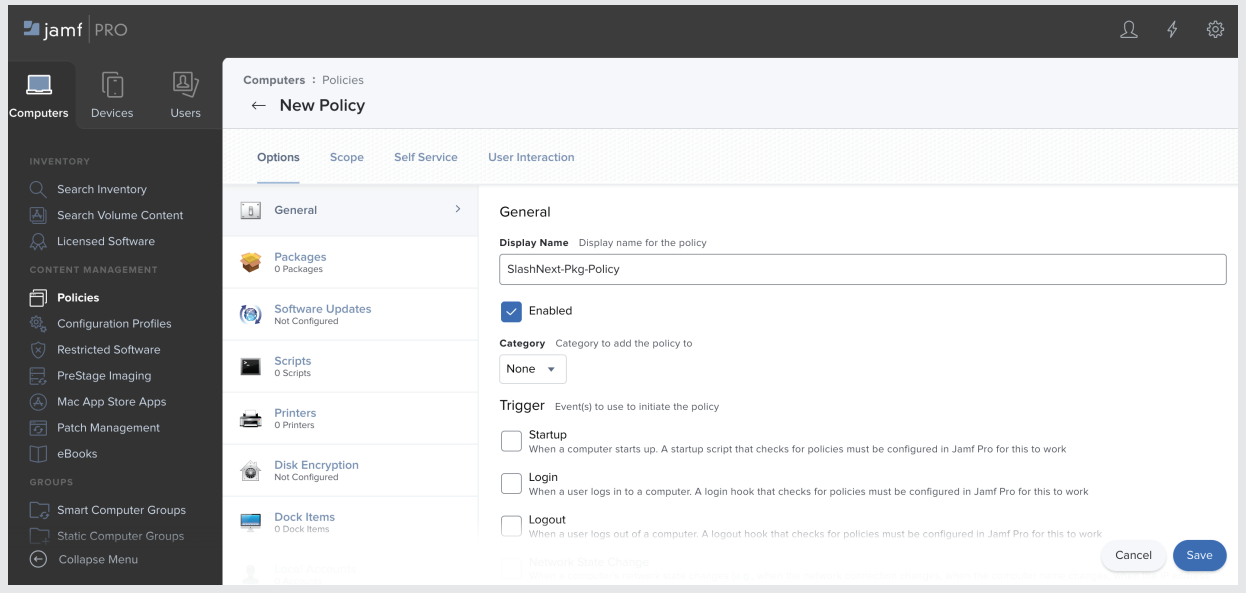
3. Under the **Packages** option click on **New** to upload Package file on Jamf distribution point. A window will appear for adding package details, add package name, and select the package file from the provided macOS app bundle. Click **Save** and the package will appear in the listing.



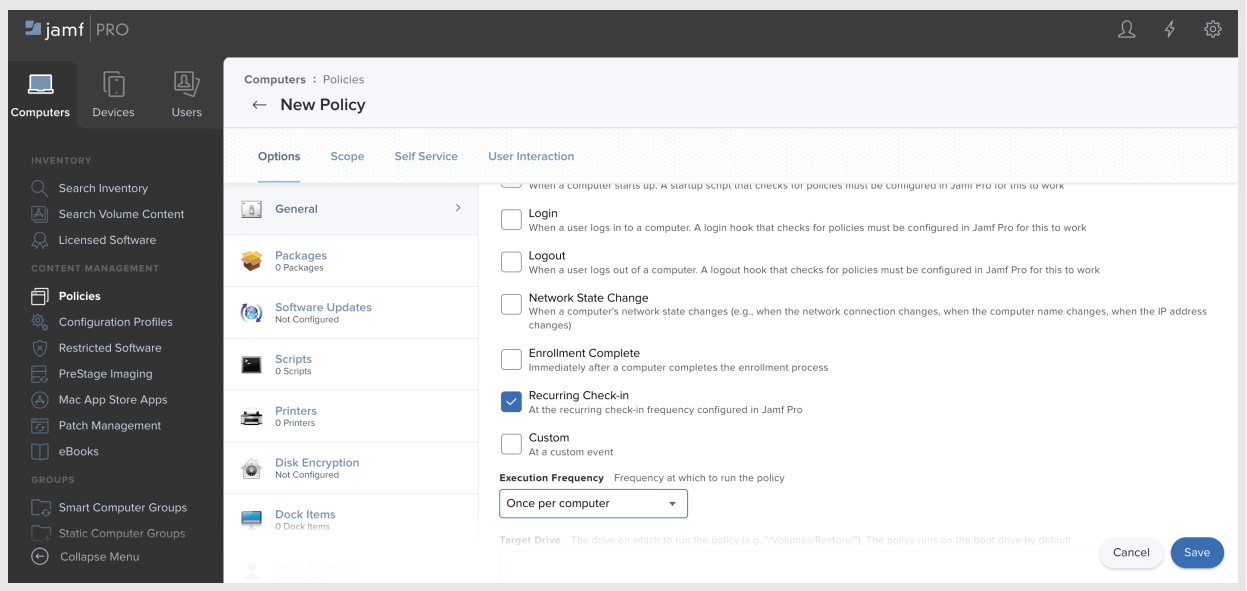
4. The next step is to create a policy that contains the uploaded package. This policy will install the enclosed package on the enrolled machine. To create policy select **Computers** and click on **Policies**.



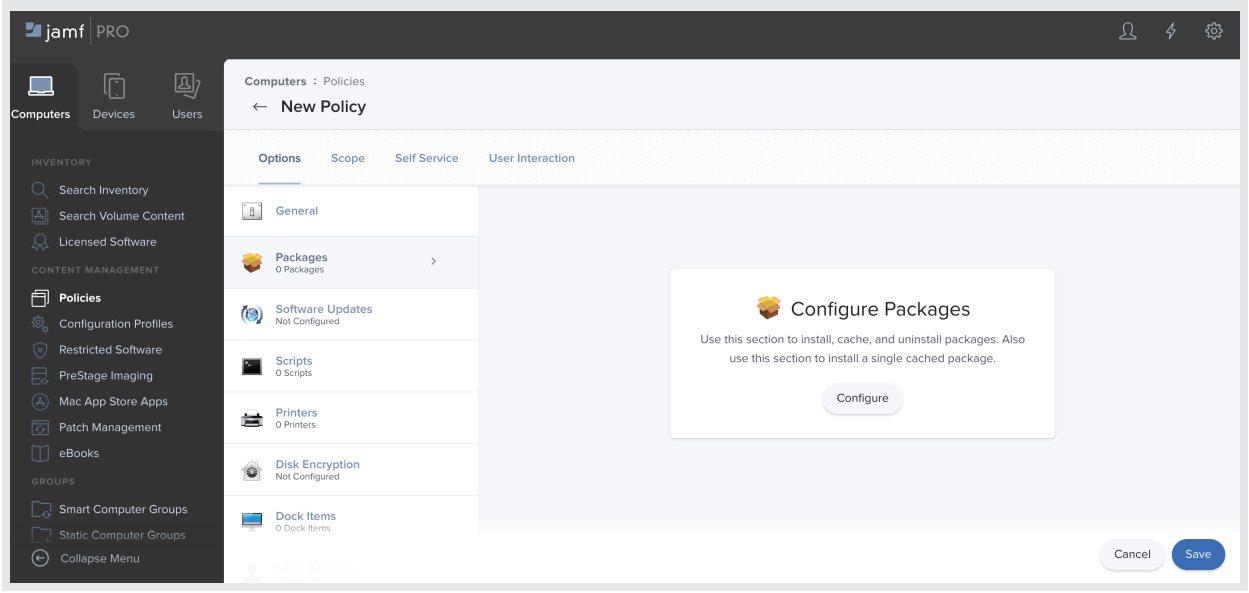
5. Next, click on **New**. A policy detail window will open where to add policy Name.



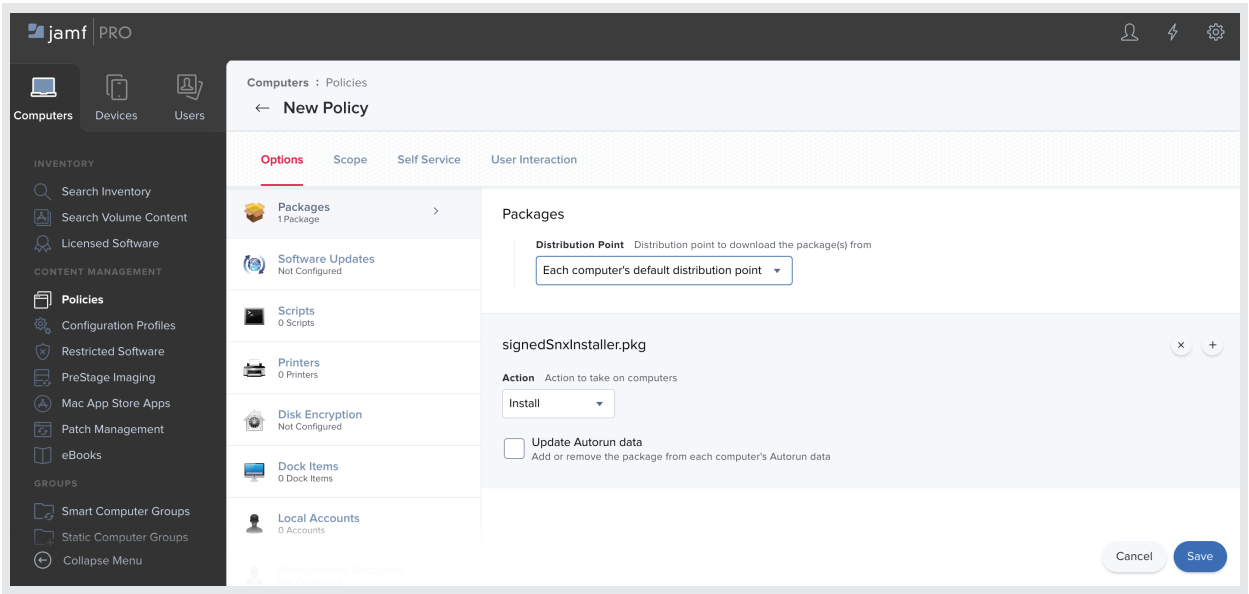
6. Scroll down in the **Trigger** section and click on **Recurring Check-in**. This will run the policy when the device gets checked-in.



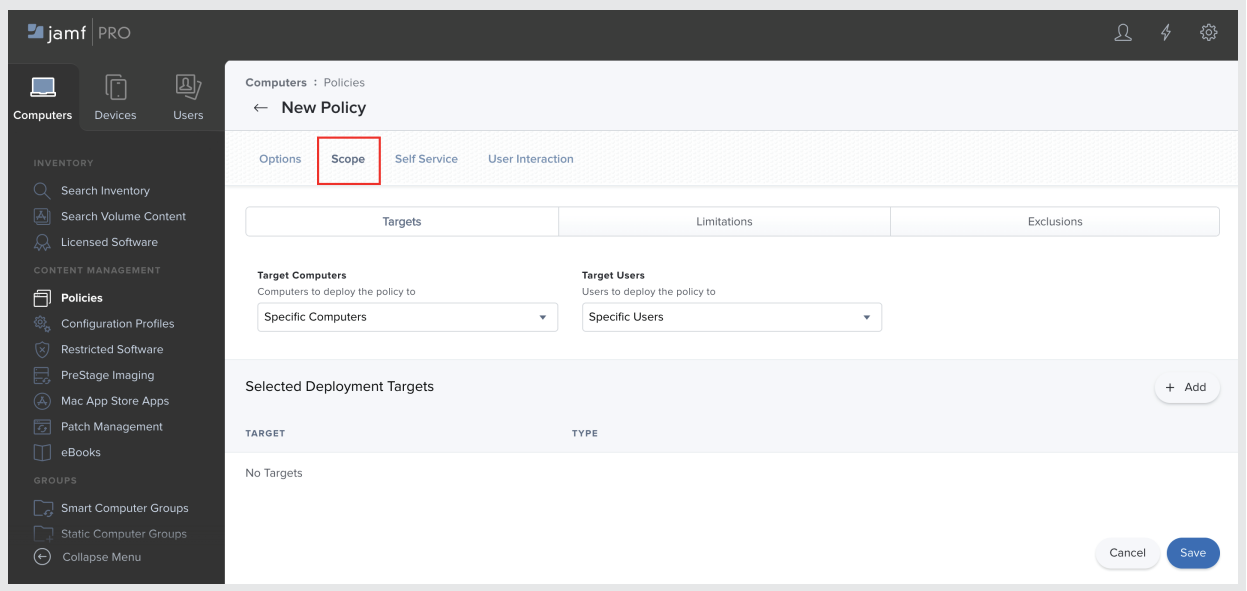
7. Next, select **Packages** that are available below the **General** option. Click on **Configure** under the packages option.



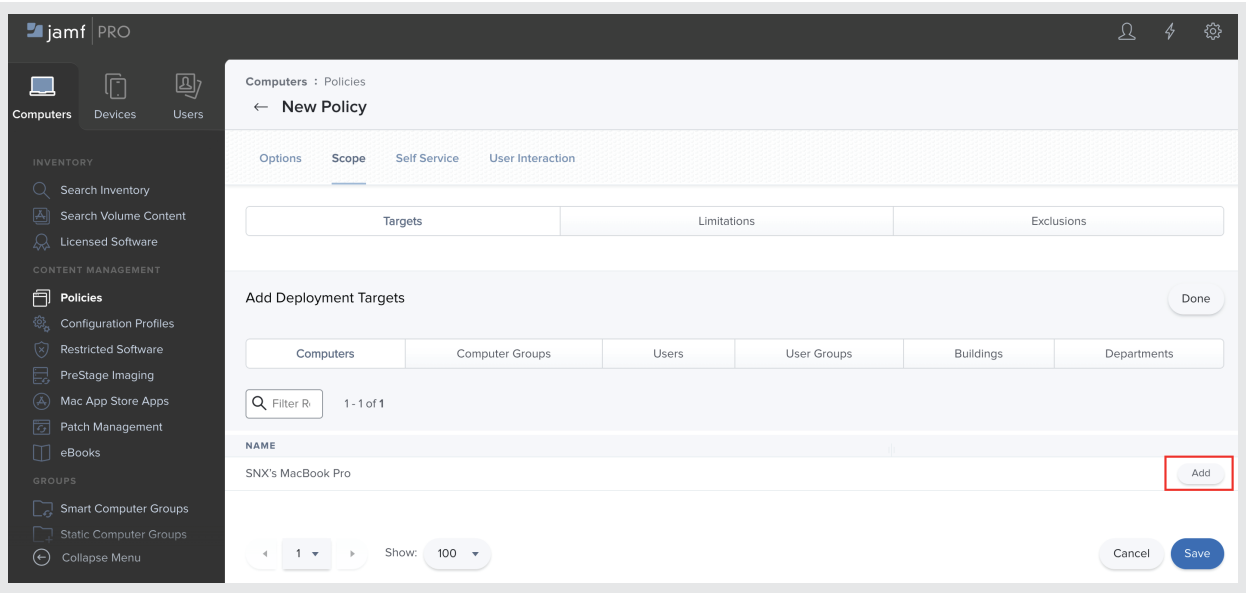
8. On clicking **Configure**, a list of packages available on the distribution point will be displayed. Click on the **Add** button displayed in front of the package name. Once clicked, the package distribution criteria window will open. In the distribution point select **"Each computer's default distribution point"**. In **Action** drop-down select **"Install"**. Once completed, click on **Save**.



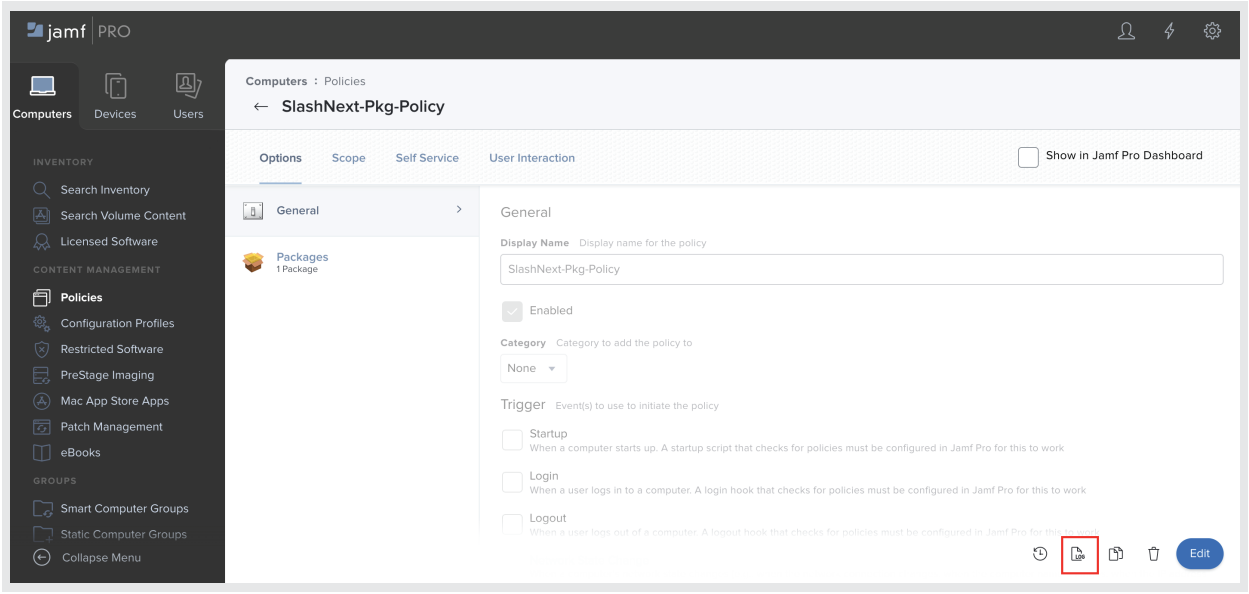
9. The next step is to assign this policy to enrolled machines. This can be done by selecting **Scope**.



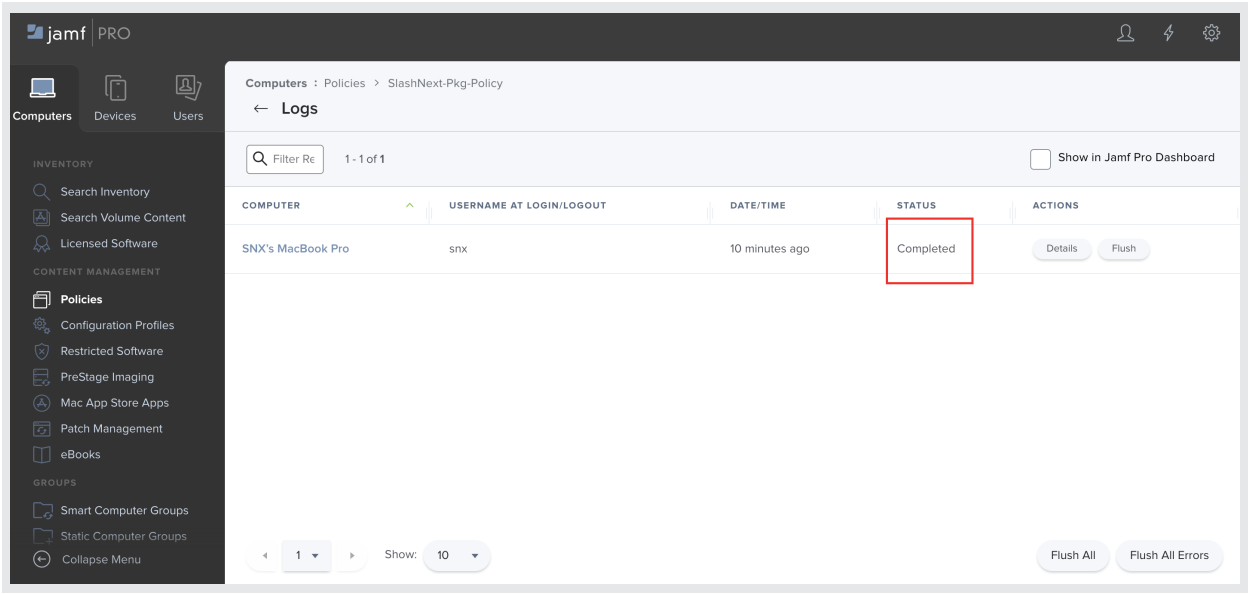
10. Click on **Add**, a list of available devices will be shown under **Target**. Click on **Add** again to add target device for policy deployment. In the end, click on **Done** and save the configurations by clicking on the Save button.



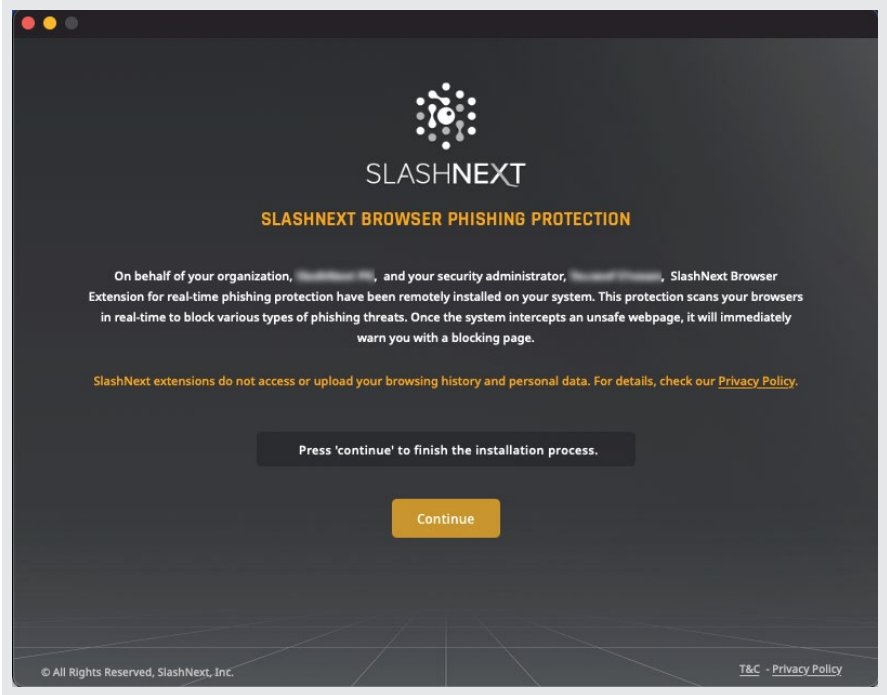
11. At this step the policy will be deployed to the machine on the next check-in of the device. To view the deployment status of policy click on **logs**, which is available under the **Options** menu.



12. On clicking the **logs**, a new window will open and deployment status will be shown there. Initially the status will be **pending** and it will turn to **complete** once the policy will be deployed. The change of status may take some time.



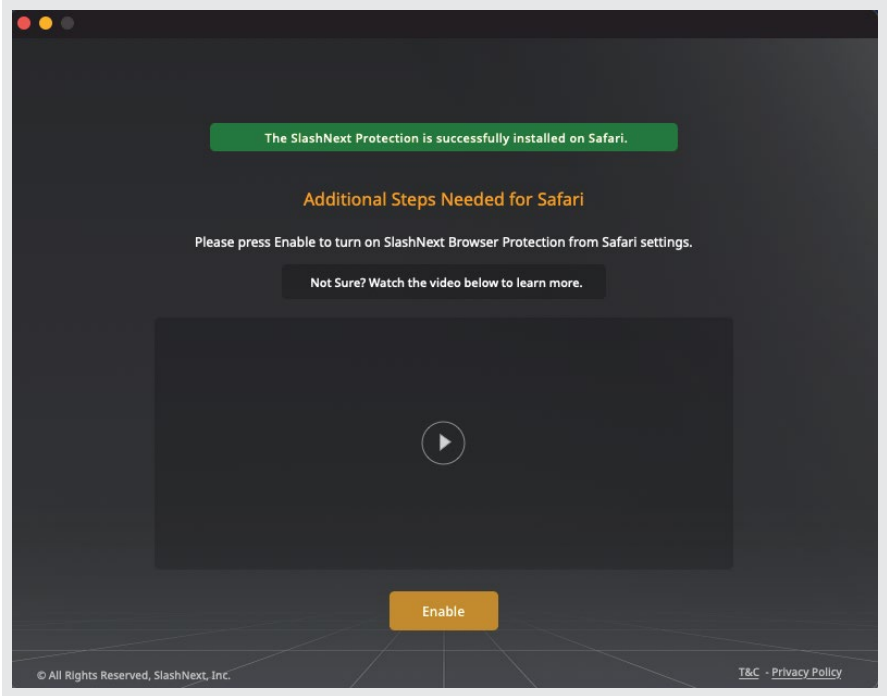
13. Once the package is deployed successfully, it will auto launch the SlashNext Browser Phishing Protection application. The application will auto activate the user if the user email exist on the server. If the application is launching first time on the machine then a welcome screen will appear upon successful installation.



TroubleShoot Step

If the continue button is not responsive then relaunch the application from the Applications directory (/Applications/SlashNext Phishing Protection Enterprise) of the machine.

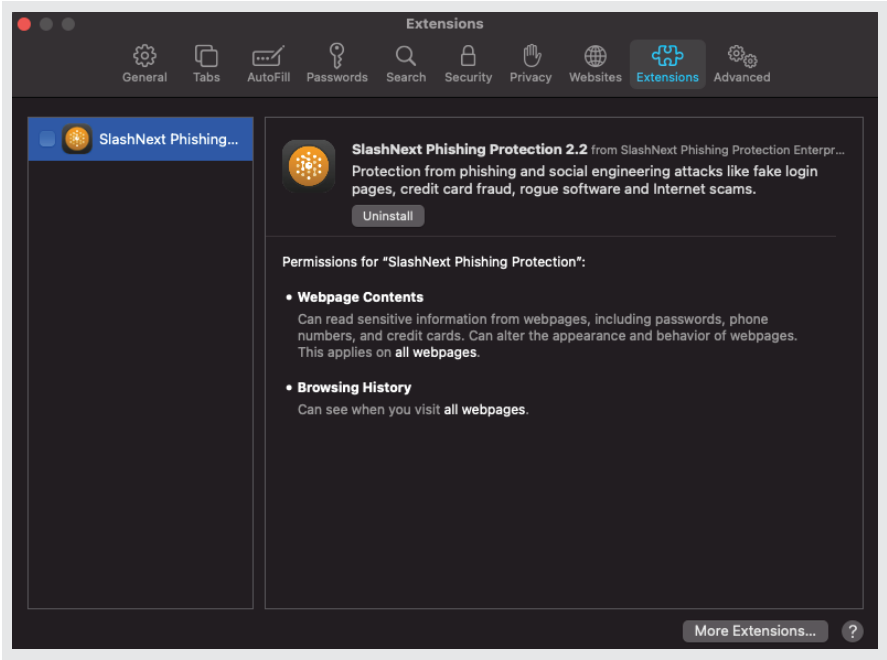
14. Clicking on **Continue**, A new screen will appear to enable the extension in safari browser.



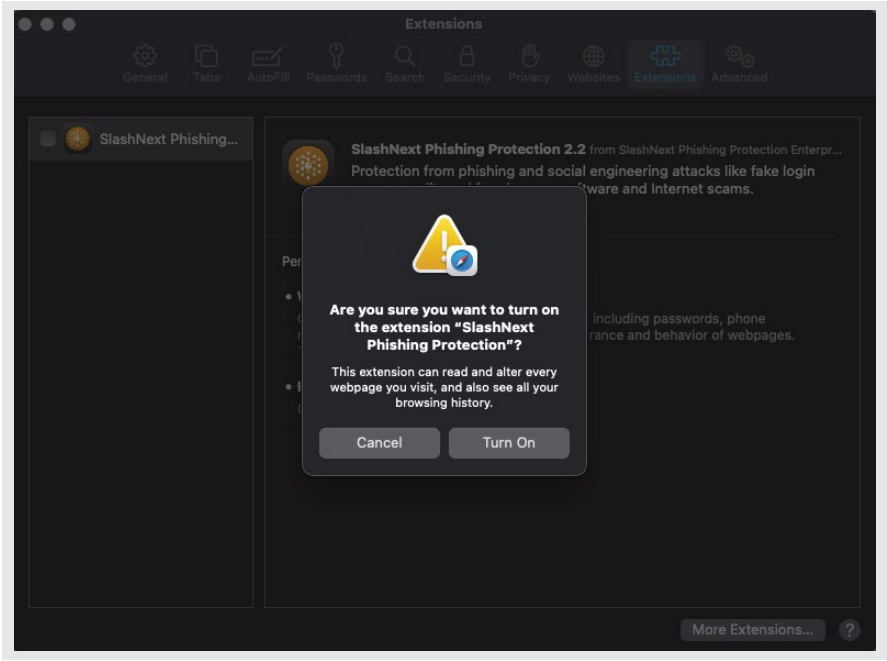
TroubleShoot Step

- If the Enable button is not responsive then relaunch the application from the Applications directory (/Applications/SlashNext Phishing Protection Enterprise) of the machine.
- Also if restarting does not fix the problem then check if the extension is available in the safari browser extension menu by opening the safari preferences and navigating to the Extensions tab, If the SlashNext Phishing Protection extension exist there, then check the checkbox to enable it.

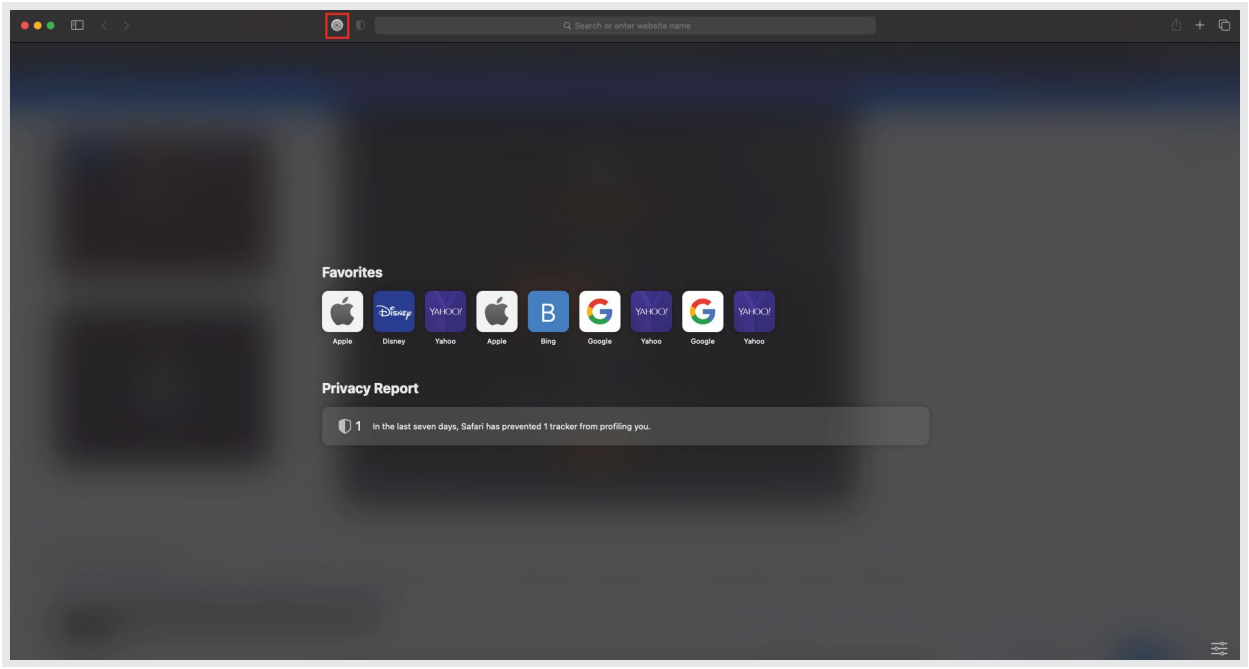
15. To enable the extension click on **Enable**. Upon clicking, safari browser extension popup will be shown as below screen shot.



16. Click on the checkbox to enable the extension, It will show a confirmation dialogue to turn on the extension. Clicking on **Turn On** will enable the extension in safari browser.



17. Once the extension is enabled in the browser, an extension icon on the safari toolbar will be appeared.



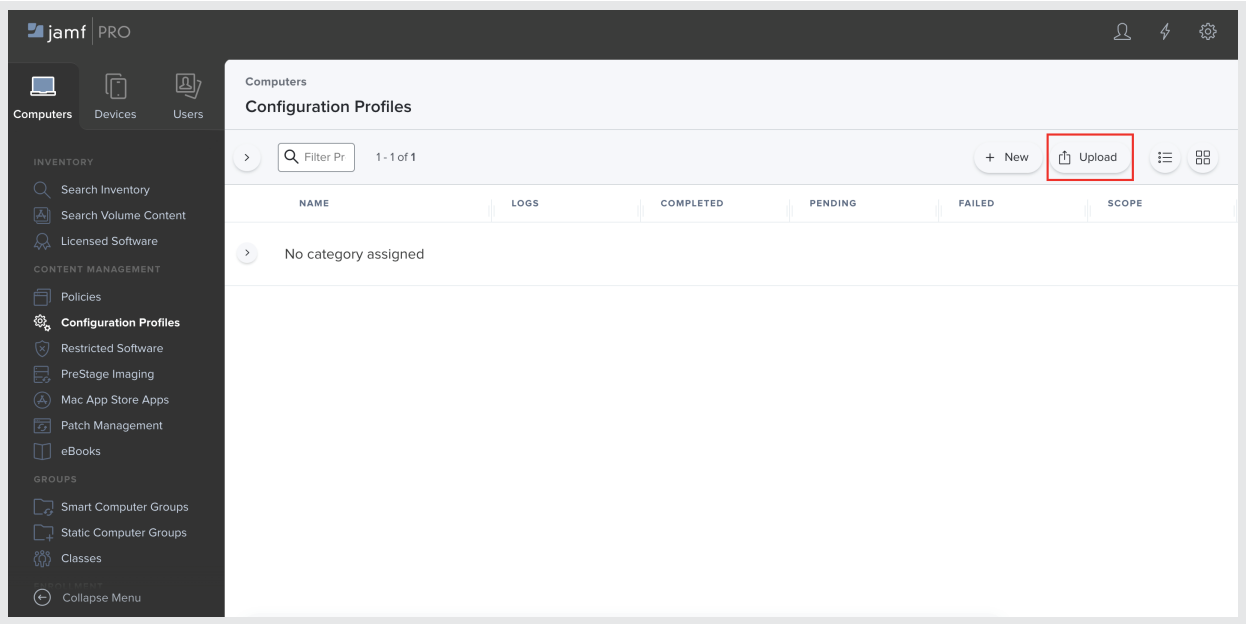
TroubleShoot Step

- In some cases if the extension icon does not show in safari browser in the above step, then restarting the safari browser will fix this issue.
- If restarting the browser did not fix the problem then right click on the toolbar and open the customize toolbar, the icon will be available in customize toolbar, drag the icon and drop it on the main toolbar will put the icon there.

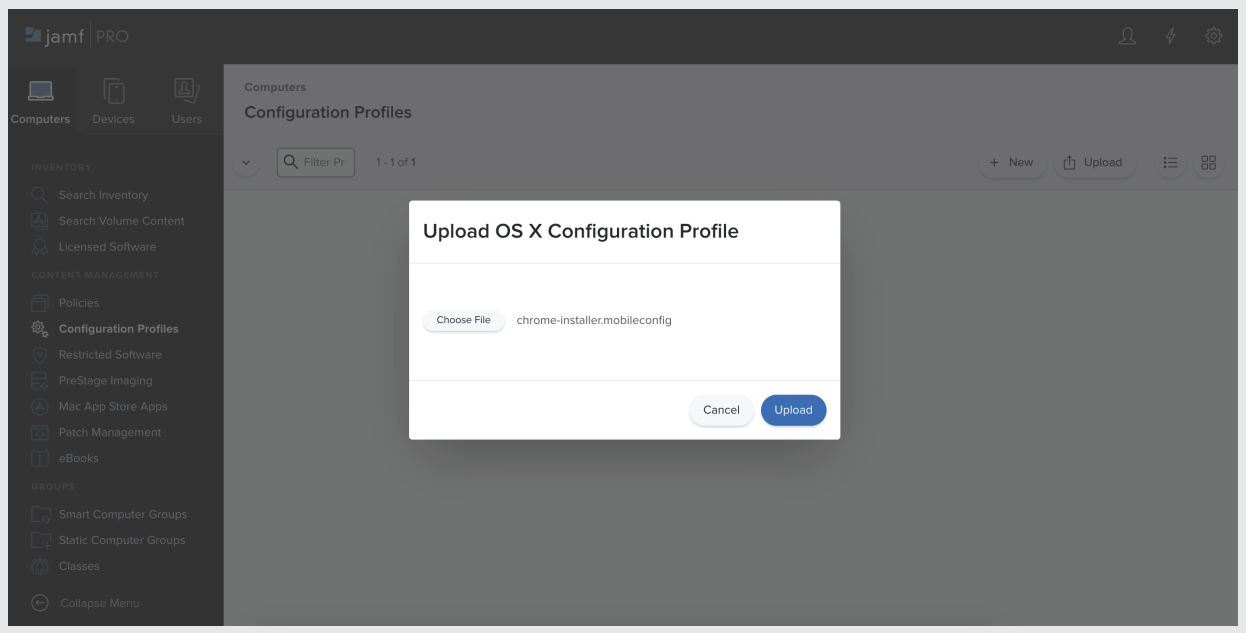
4 | PROFILE/INSTALLER DEPLOYMENT

Before the execution of this step, make sure the package which is deployed in above step has been successfully deployed in the end users machines. Profile deployment is more or less the same as (.plist) deployment which is explained in the first step of the guide. The only difference is that instead of creating a new configuration, we will upload the (.mobileConfig) file directly.

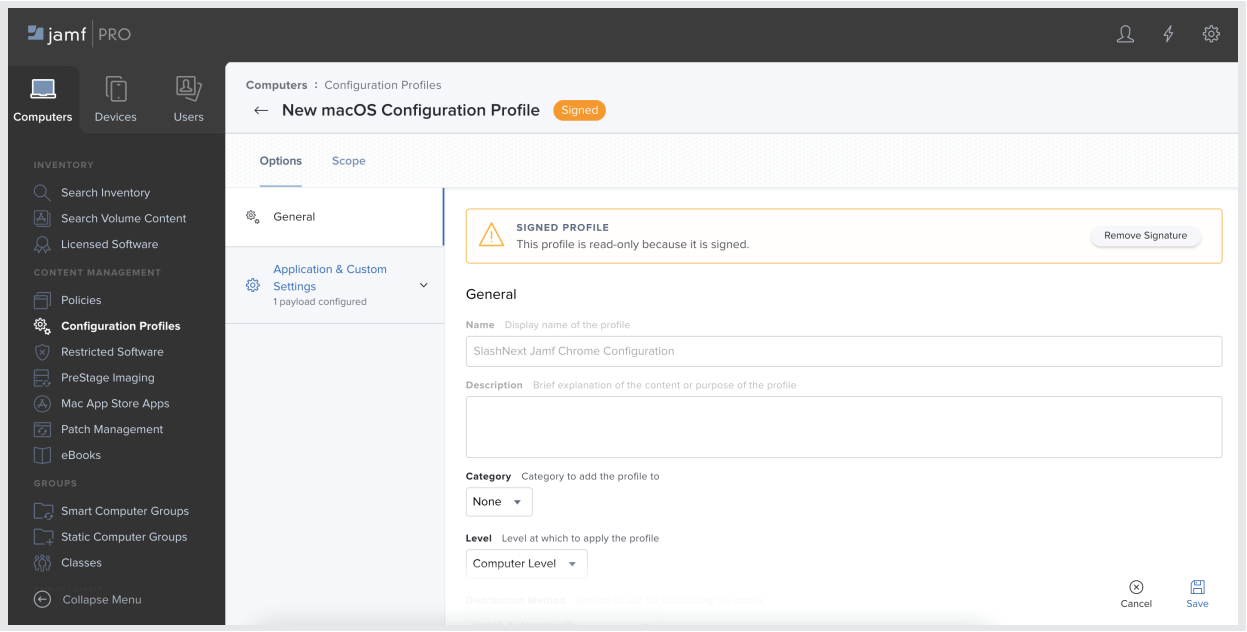
1. To do so, open **Configuration Profiles** under **Computers** and click on **Upload**.



2. Select the **"chrome-installer.mobileconfig"** file from the provided macOS app bundle and upload it on the Jamf portal to install extension in Chrome browser.



3. Once the profile is uploaded, the window should appear as the given screenshot.



4. Select **Scope** and add the target machine, once done click on **Save**. After some time the profile will be deployed on the machine and you should see the **SlashNext Extensions** icon in the browser on restart.

Note

There is a separate configuration profile for each individual browser (Chrome, Firefox, Edge Chromium) having self-explanatory names. Repeat step 1-4 for each of the profile in order to deploy extension on all three browsers.