exterro®
Data Risk Management

FTK 8.2 SP2 MAC AGENT – DEPLOYMENT GUIDE (VIA JAMF PRO)

OCTOBER 2025

Table of Contents

Overview

Exterro was founded with the simple vision that applying the concepts of process optimization and data science to how companies manage digital information and respond to litigation would drive more successful outcomes at a lower cost. We remain committed to this vision today. We deliver a fully integrated Data Risk Management platform that enables our clients to address their privacy, regulatory, compliance, digital forensics, and litigation risks more effectively and at lower costs. We provide software solutions that help some of the world's largest organizations, law enforcement and government agencies work smarter, more efficiently, and support the Rule of Law.

Purpose of the Document

The purpose of the document is to provide users with the step-by-step instructions required to deploy the Mac Agent via JAMF Pro application.

1 Mac Agent – agentinstall.config Configuration

This section provides you with the step to update the installation config file to create the Mac agent package used for Jamf Pro.

To update the agentinstall.config file:

1. Open the **agentinstall.config** file provided by the Exterro team and edit the following options based on your environment:

Configuration	Default Value	Description
ServerPollIntervalSeconds	1800	Time interval for agent check-in
CollectionFailedFileCount	0	The maximum number of failed files allowed during the collection process. If the number of files exceeds this value, the collection will fail.
ServerBaseUris	FTKC dns/Server name	Server to which the agent has to be connected with. Multiple FTKC server DNS/ServerName with port can be added by separating it with commas (,). ***Example:*** *ServerBaseUris=<FTKC_IP/HOSTNAME>:####,<FTKC_IP/HOSTNAME>:####*
ValidateCertificate	true	If **validateCertificate** is set to true, the agent would expect calling an agent API to present a cert that matches the client cert (named client.CER which is the public key of a .PFX associated to the configuration key: **agentCertificateFileName** found in the **ADG Weblabselfhost** configuration file).

Configuration	Default Value	Description
		The **validateCertificate** key is also used to ignore the cert failures when the agent tries to contact FTKC server for offline jobs (which has invalid cert)
ClientCertificatePath *(Optional field)*	-	If the client has their own SSL certificate, provide the file path where it is stored. ***Example:*** *The path should be enclosed in double quotes:* */path/to/the/client/certificate*

2. Save the file.

Important Note: The saved file should be sent to the Exterro Support Team (support@exterro.com). The Exterro Team will use the provided file to build a customized Mac Agent package for use in JAMF.

2 Deploying the Mac Agent via JAMF Pro

2.1 Prerequisites

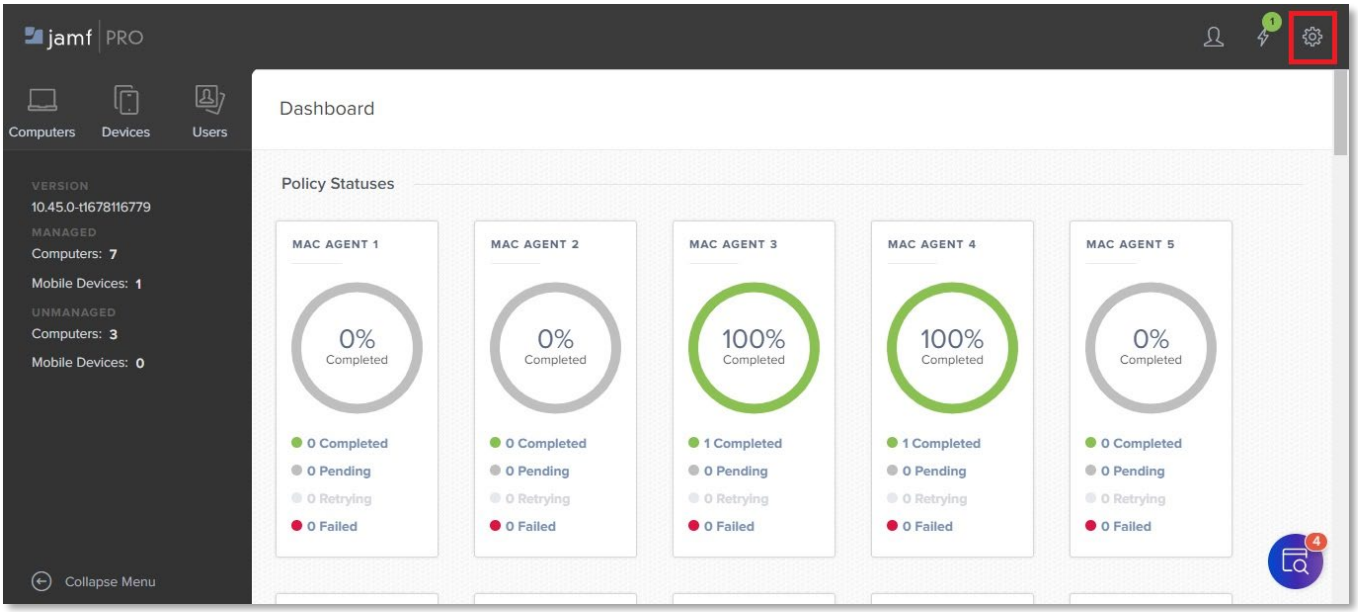
- The targeted machines should be enrolled in JAMF with the ability to manage Policies and Configuration Profiles.
- A Mac with a manually installed Agent is required to obtain baseline information.

2.2 Creating an Agent Installation Package

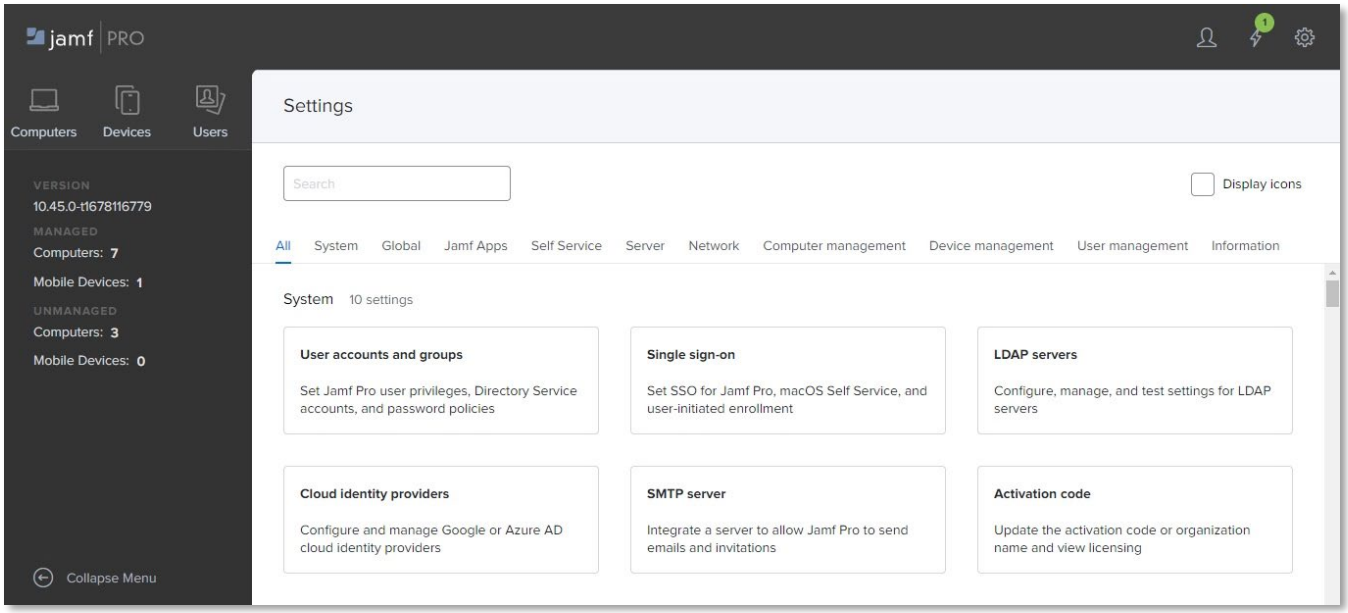
A separate Package is required for each version of the Mac Agent. Subsequent sections must correspond to the version of the Agent used in the installation package.

To create an Agent Installation Package:

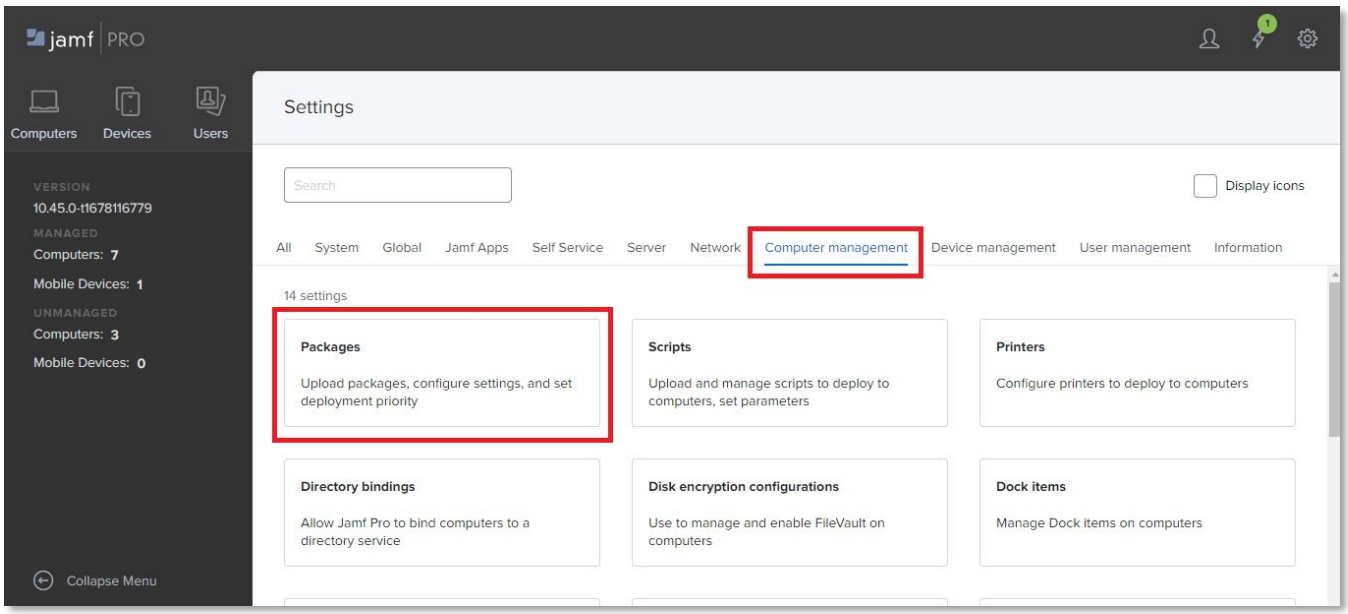
1. Log into JAMF Pro application.
2. Click on Settings  from the top-right corner.



- The **Settings** page is displayed.

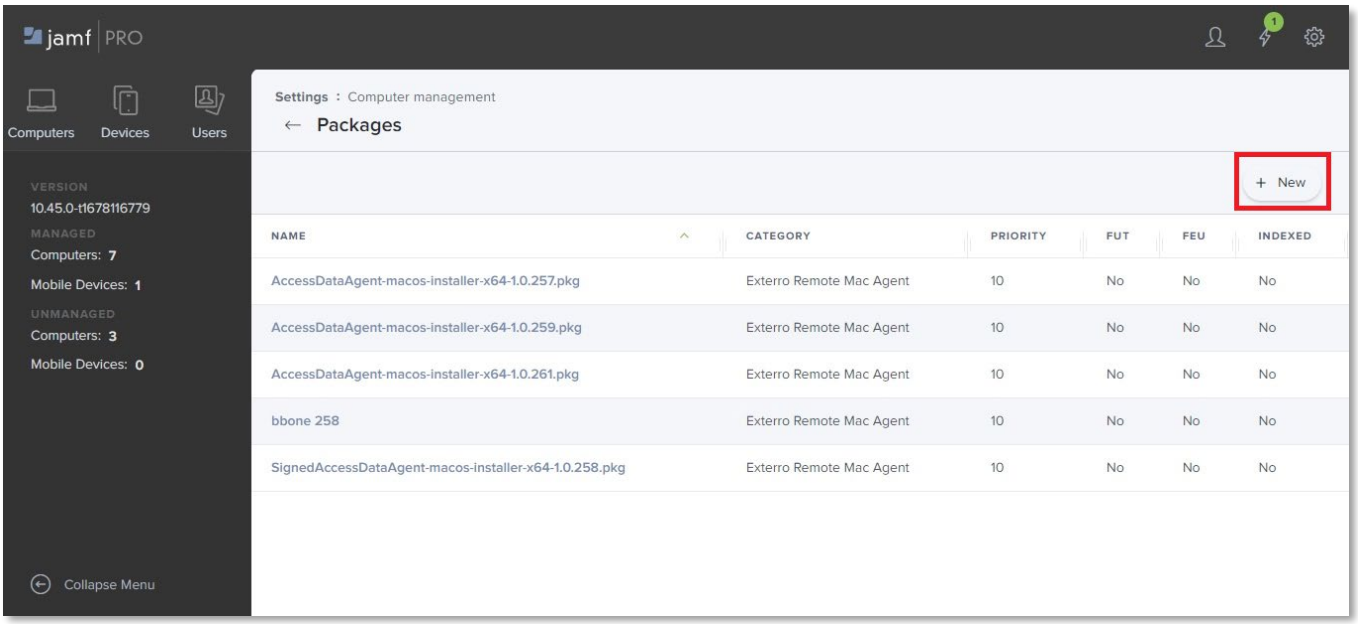


3. Select the **Computer management** tab and click on **Packages**.

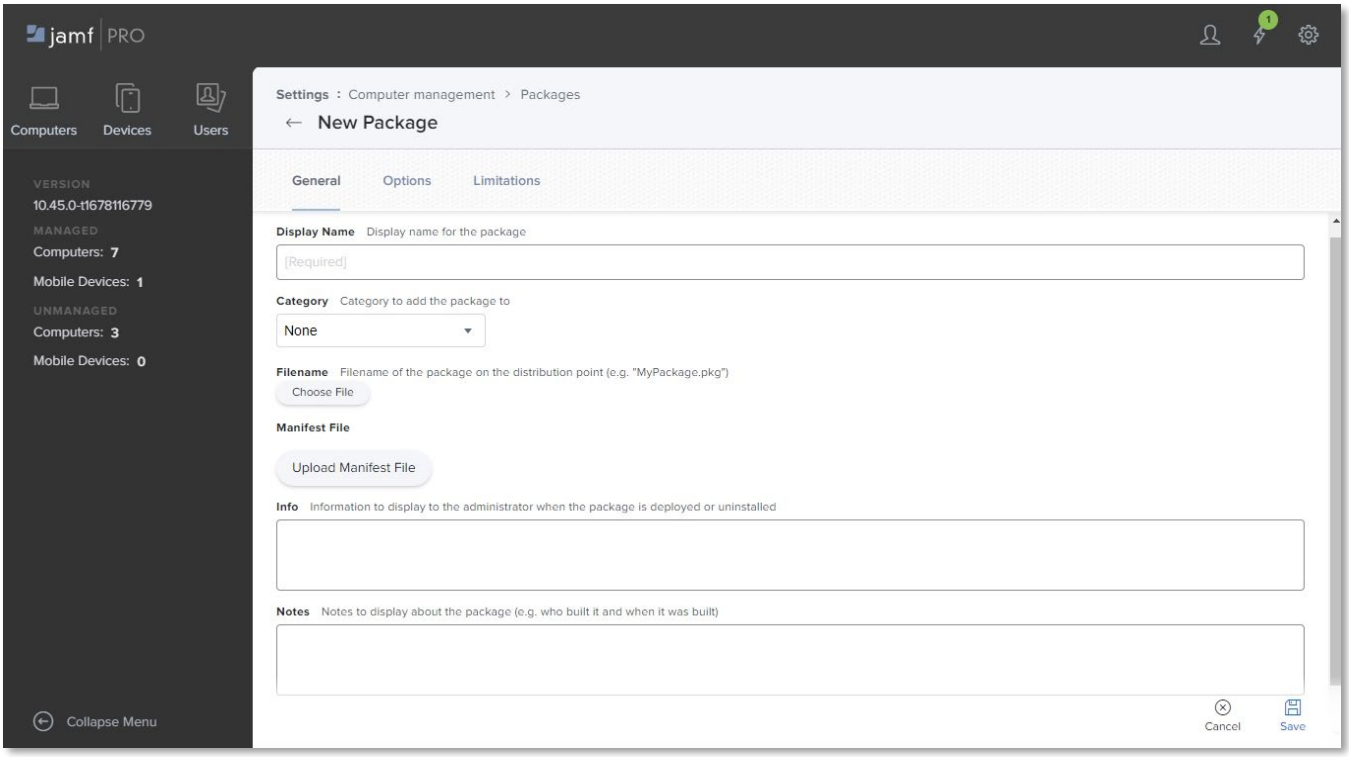


4. Click **New**.

Note: The package file provided by Exterro team should be added here.



5. Provide the package's **Display Name**.



6. Select the package's **Category**.
7. Browse and select the required Agent PKG file for the **Filename** field.

Note: *The remaining fields are optional and can be configured based on the user's requirements.*

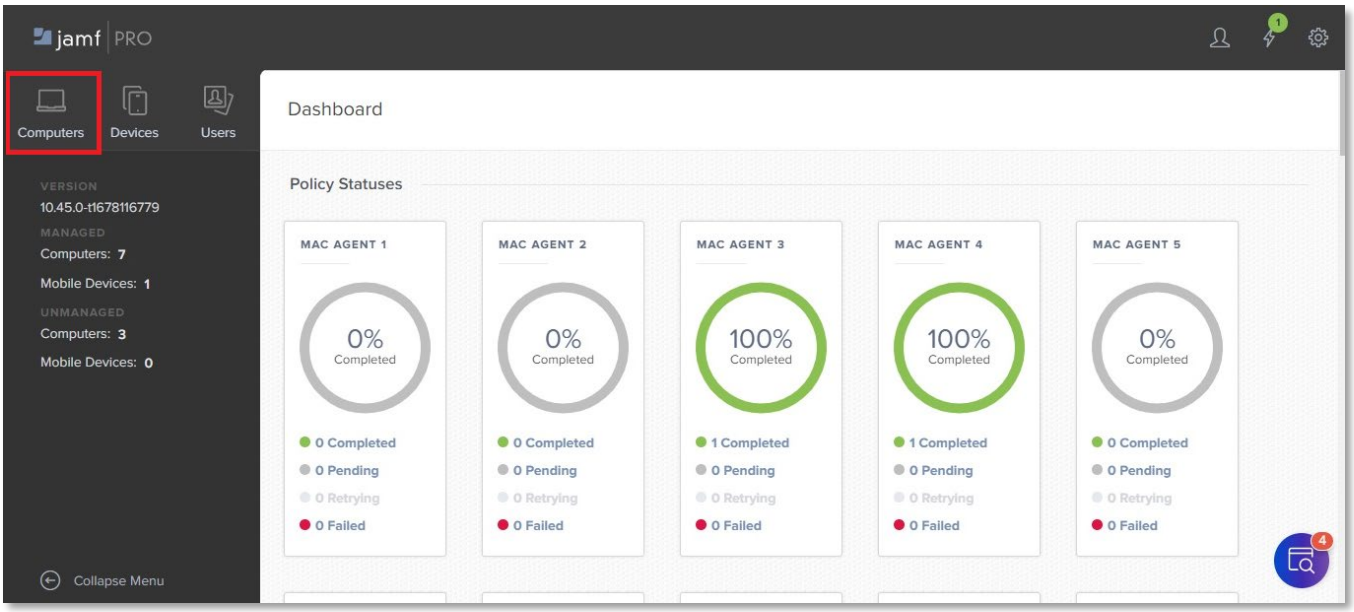
8. Click **Save**.

2.3 Creating an Agent Deployment Policy

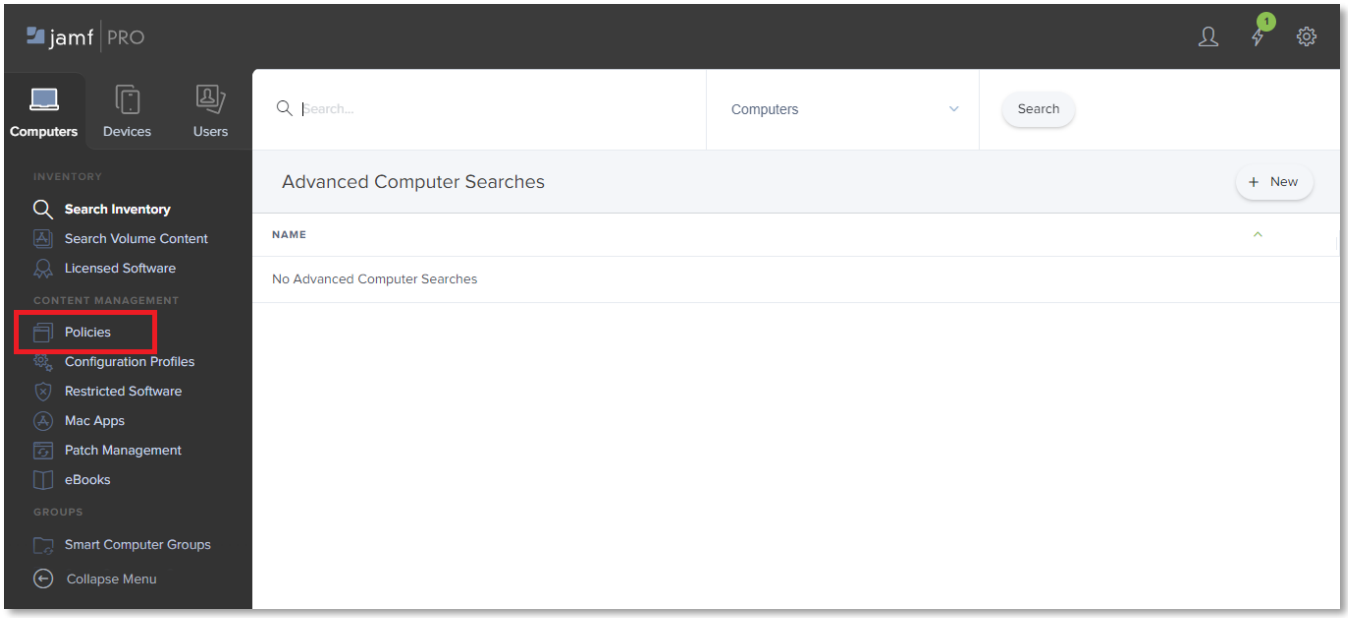
A Policy will be used to uninstall any existing Agent on a target machine and then install the specified Agent version.

To create an Agent Deployment Policy:

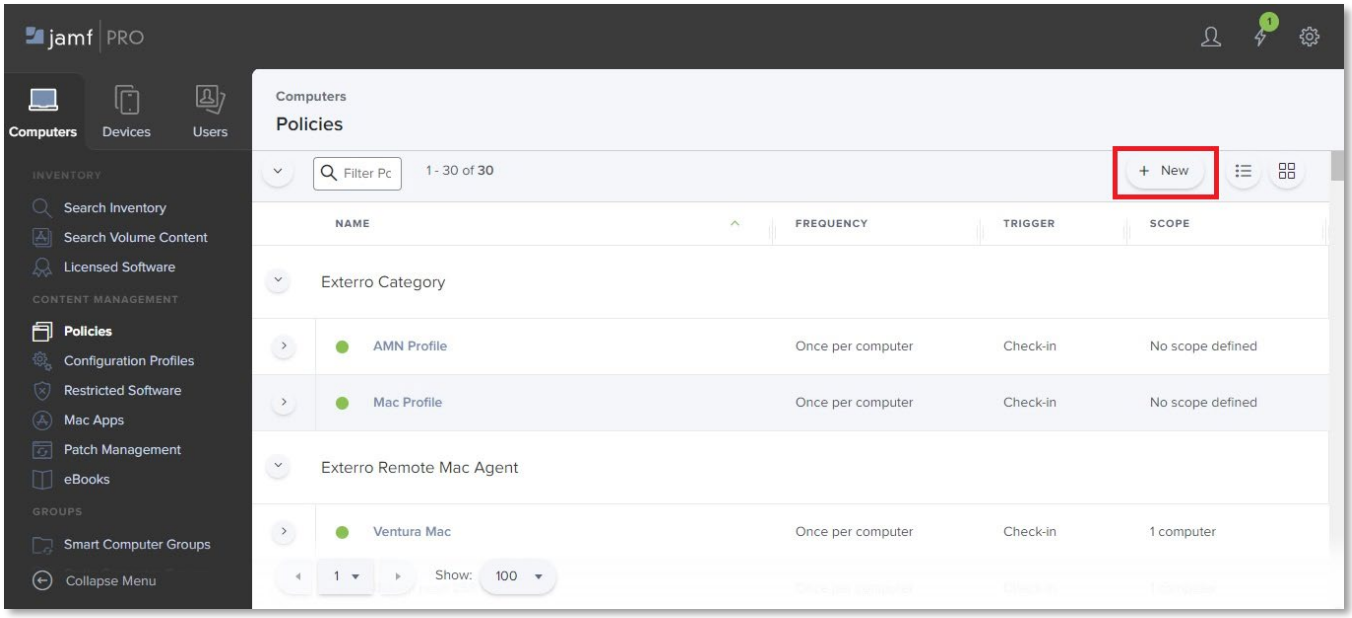
1. Log into the JAMF Pro application.
2. Click on **Computers**.



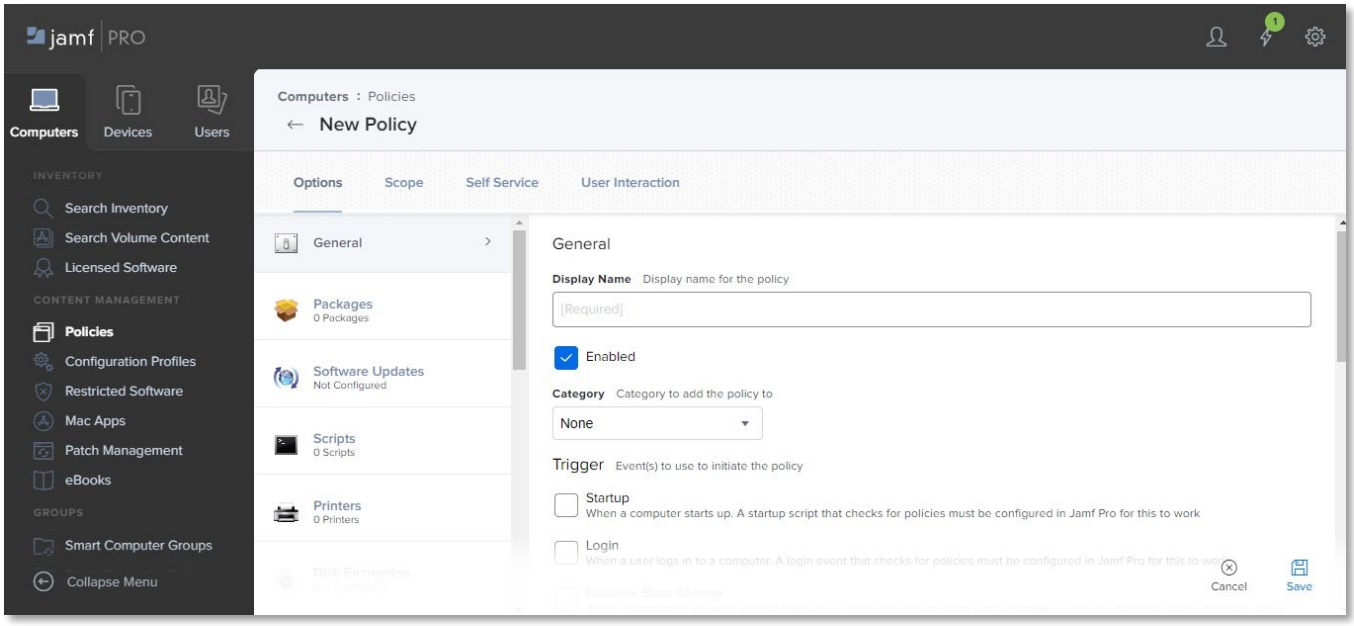
3. Click on **Policies** from the left pane.



4. Click on **New**.



- The **New Policy** page is displayed.

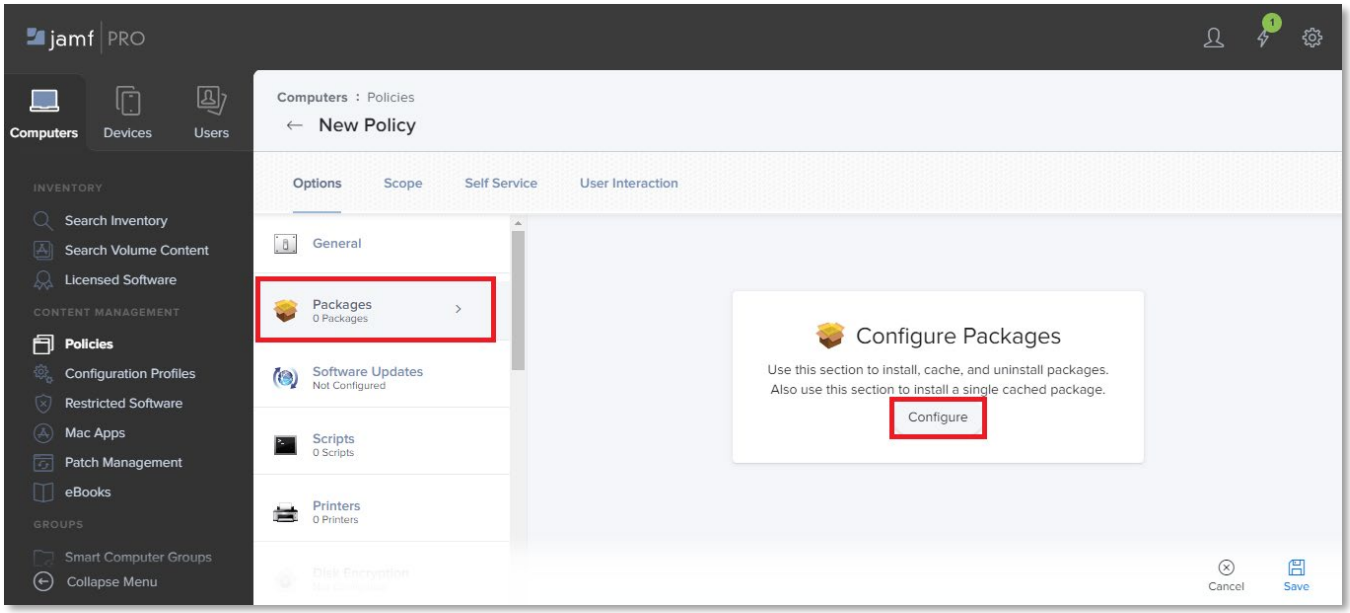


5. Provide a policy's **Display Name**.
6. Check the **Enabled** option.
7. Select the policy's **Category**.
8. Select the required **Trigger** events during when the policy should be deployed.

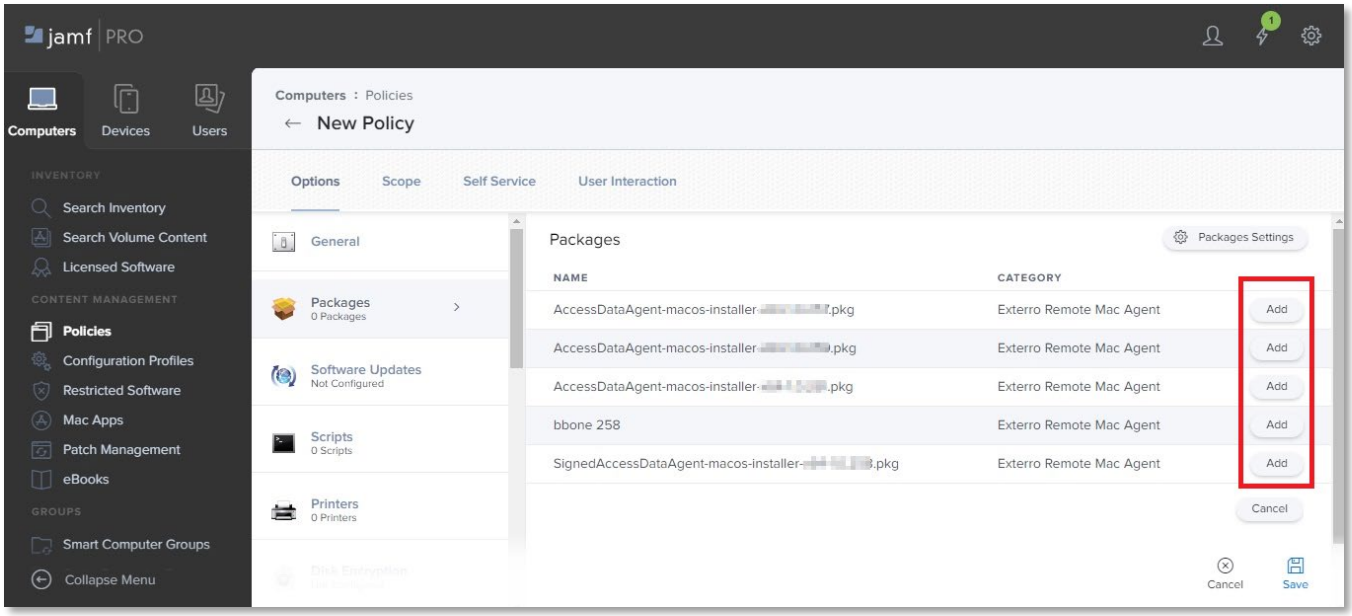
   Note: *You are recommended to select the* ***Recurring Check-in*** *trigger event.*

9. Select the **Once per computer** option from the **Execution Frequency** dropdown.
10. Check the **Automatically re-run policy on failure** option.

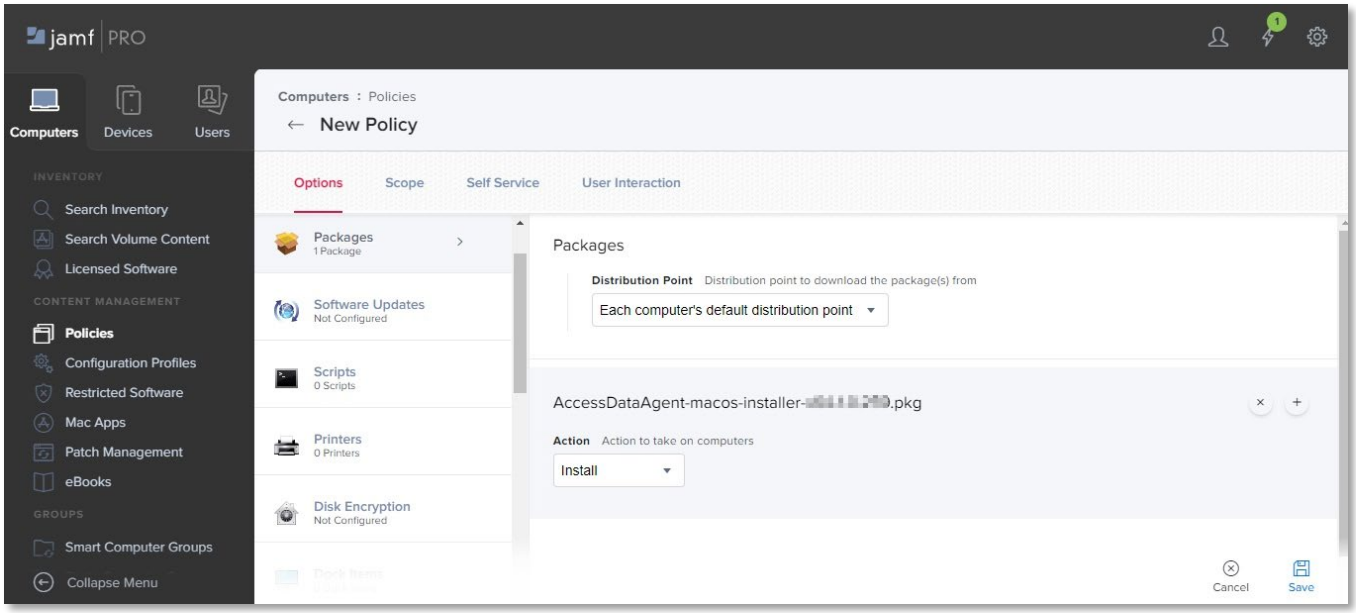
11. Select the **Packages** tab from the middle pane and click on **Configure**.



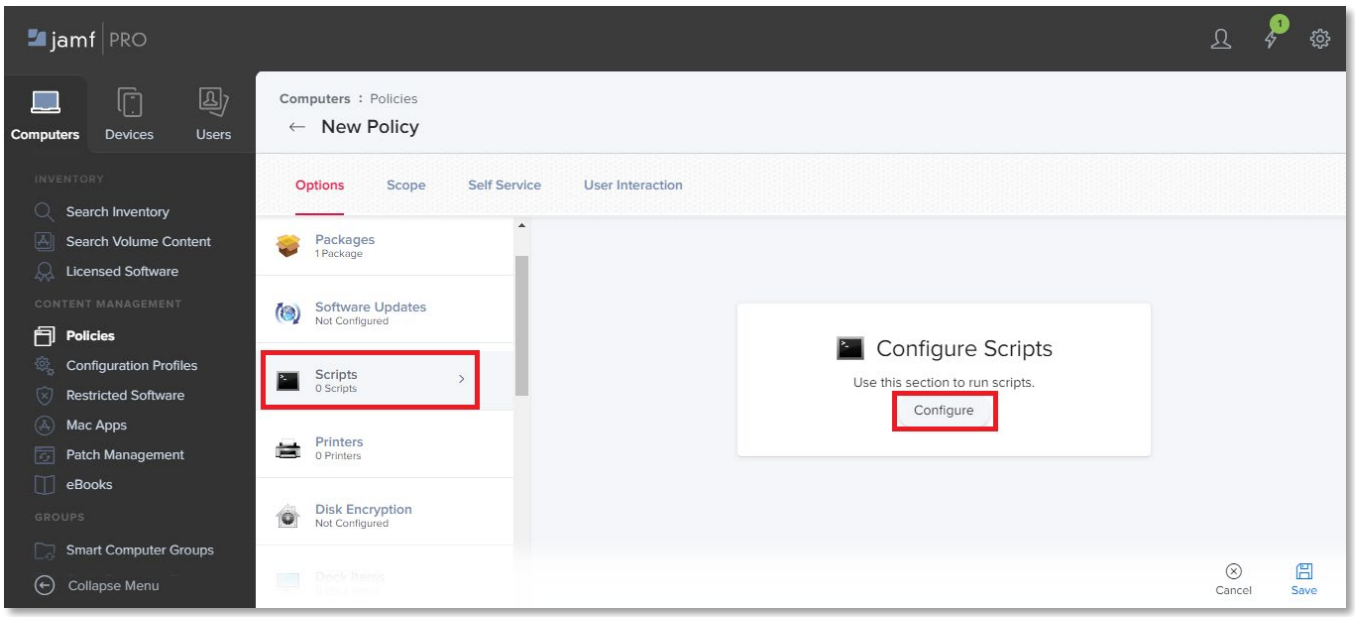
12. Click **Add** against the required package.



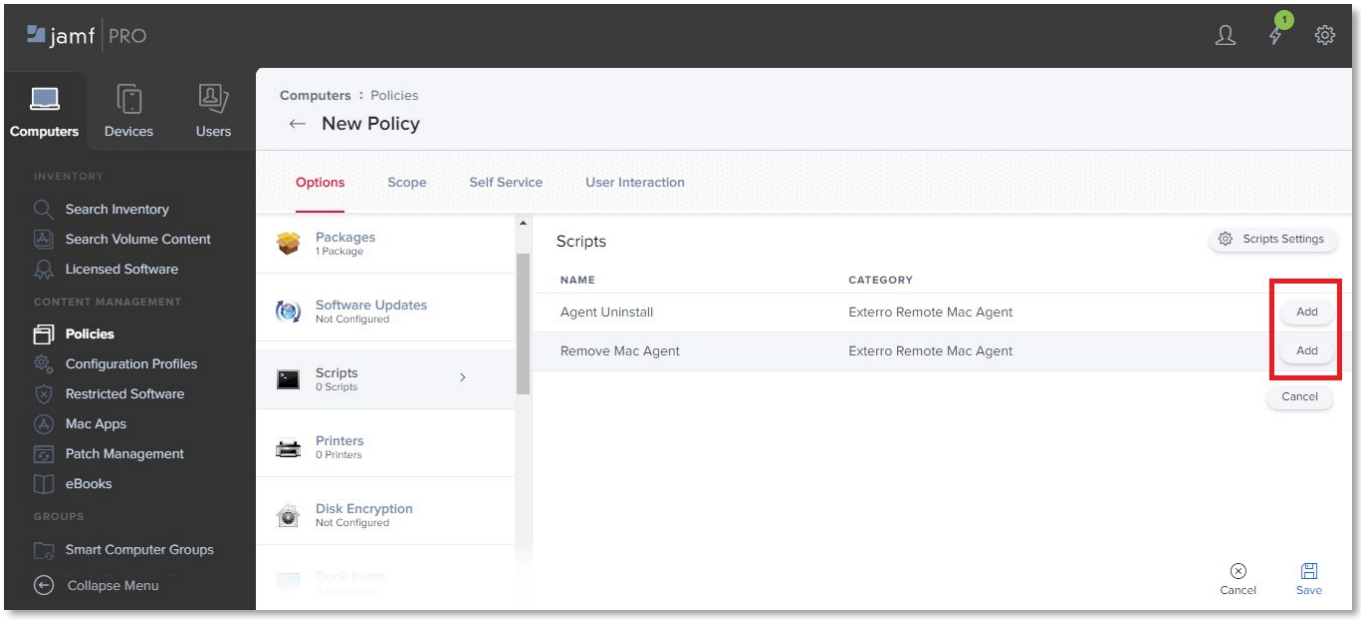
13. Select the **Install** option from the **Action** dropdown.



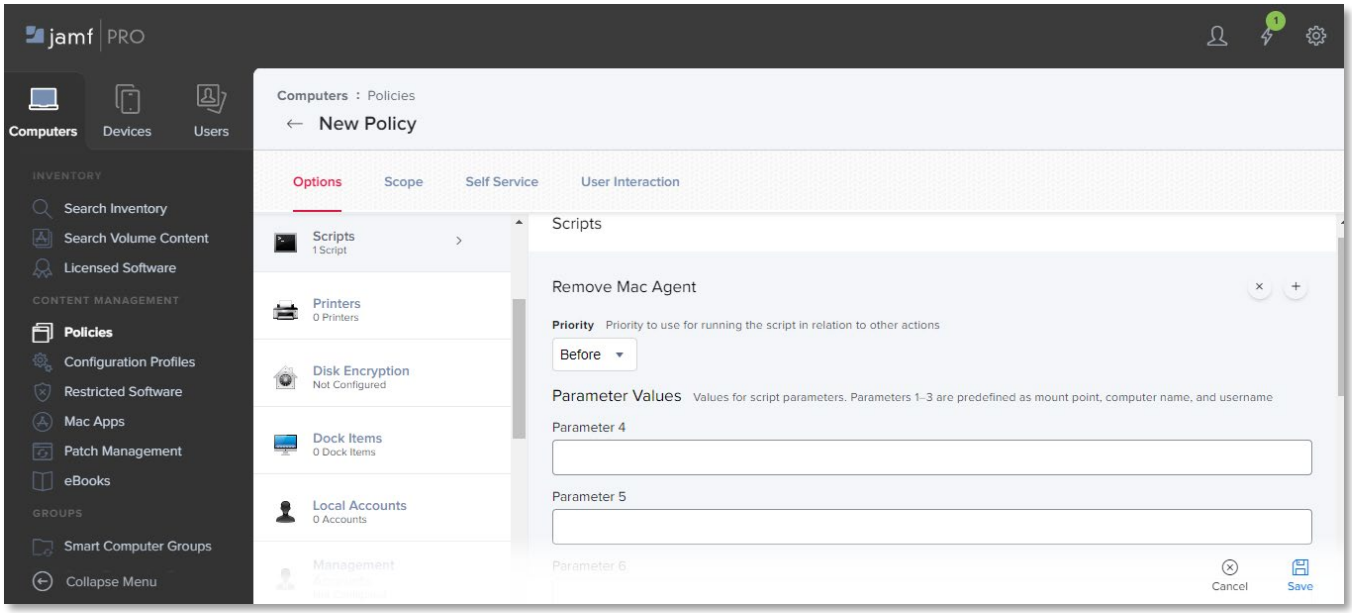
14. Select the **Scripts** tab from the middle pane and click on **Configure**.



15. Click **Add** against the required Agent Uninstallation Script.

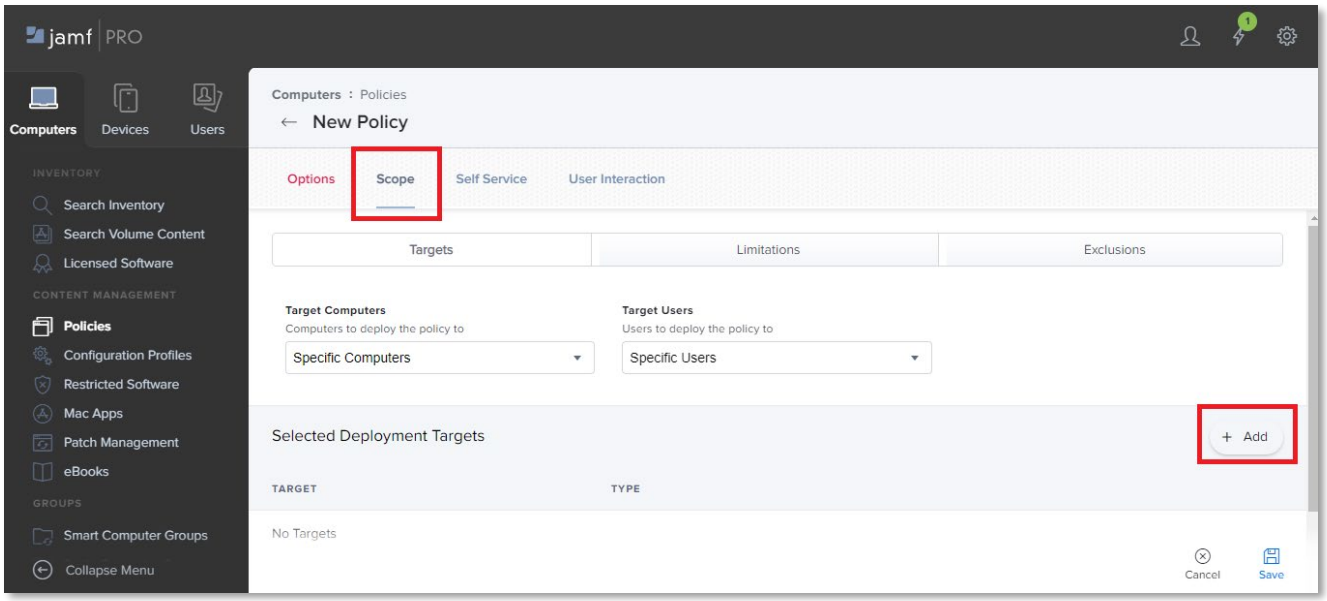


16. Select the **Before** option from the **Priority** dropdown.

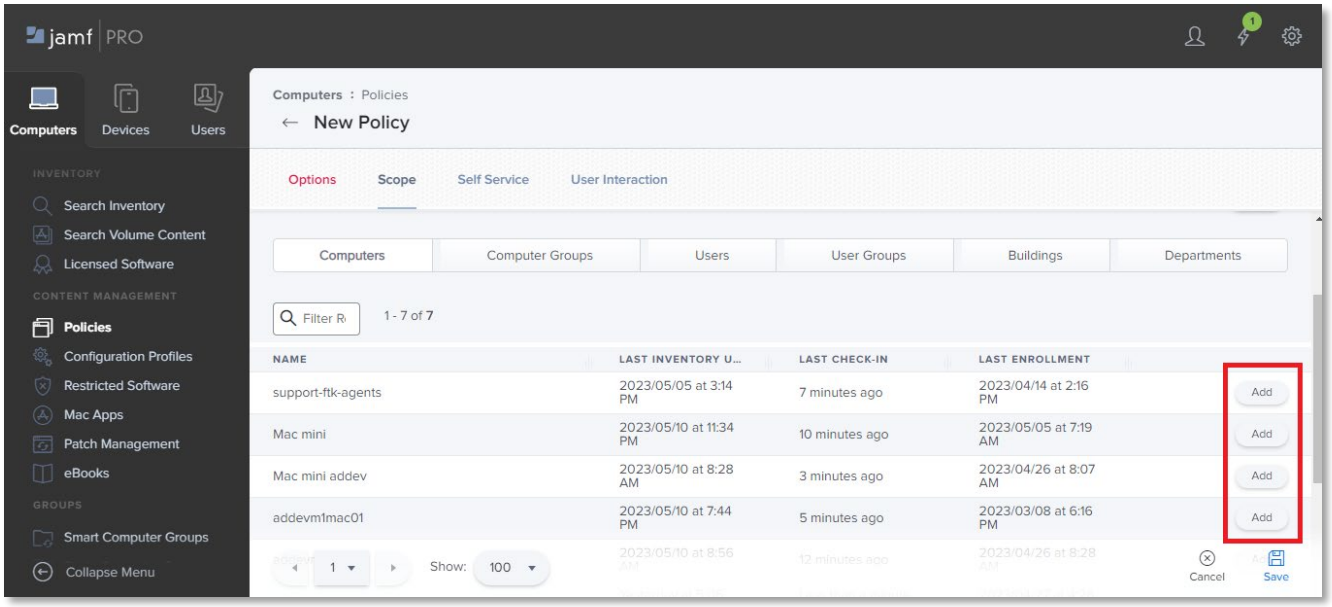


17. No **Parameters** should be added.

18. Select the **Scope** tab and click on **Add**.



19. Click on **Add** against the required target.



20. Click **Save**.

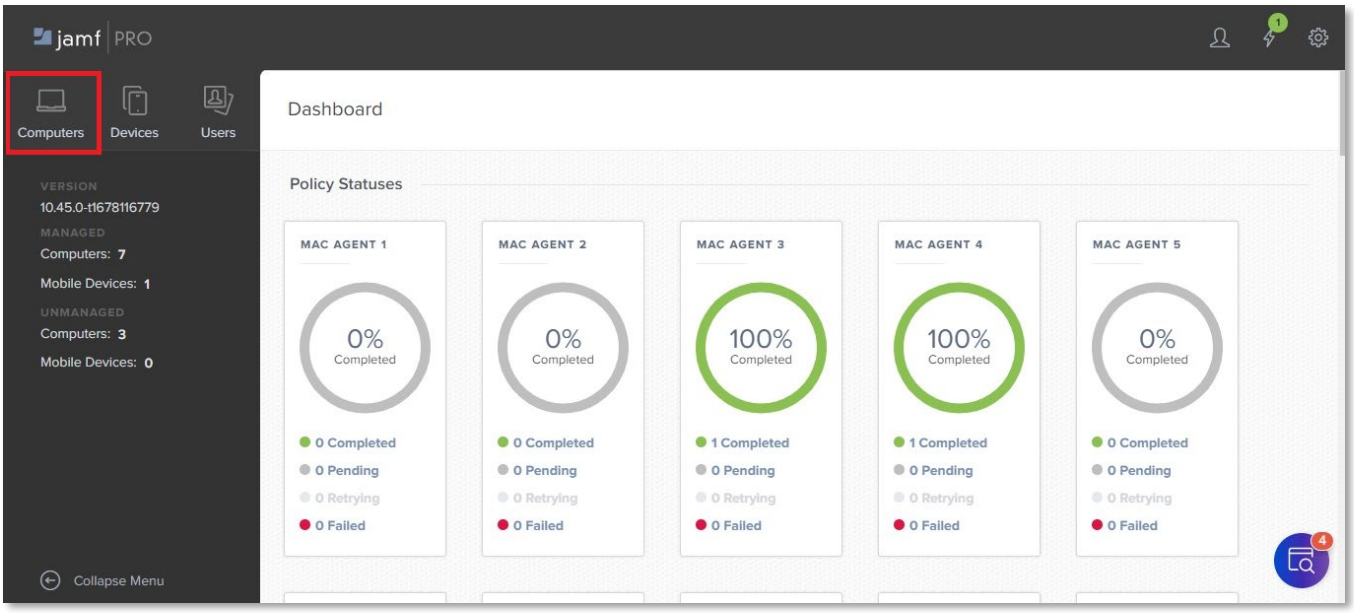
If the **Recurring Check-in** event was selected for **Trigger**, the new Policy will be run on targets the next time a user checks in to the JAMF application.

2.4 Creating a Configuration Profile

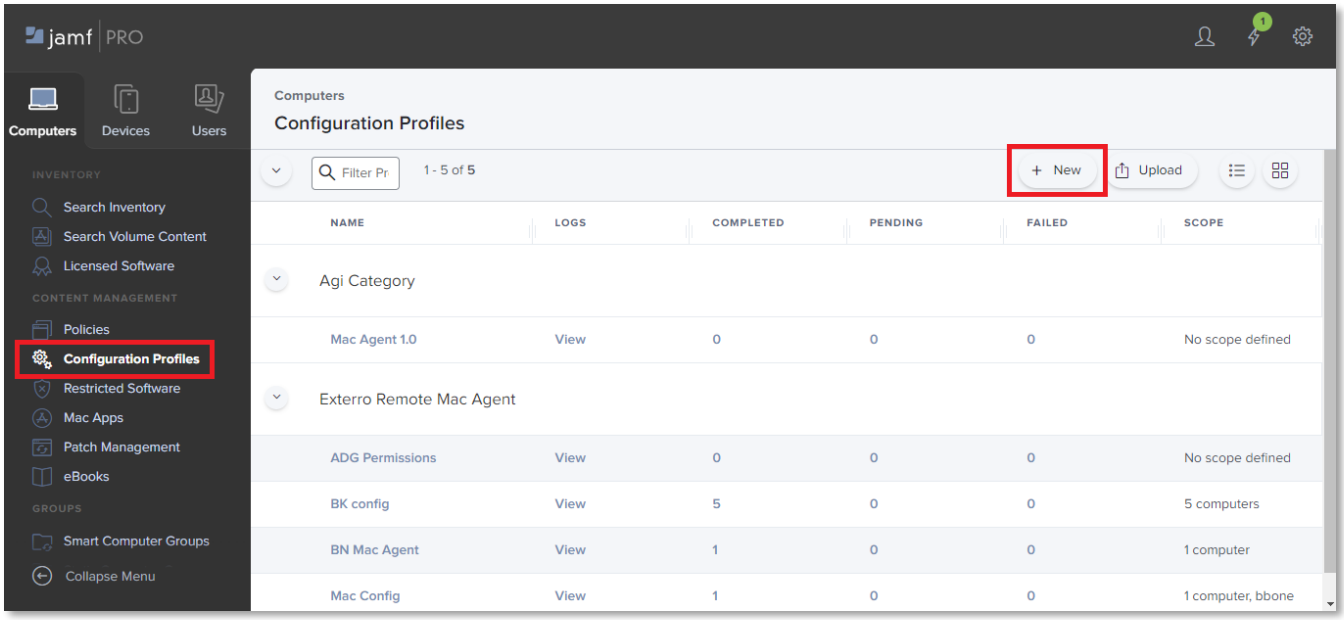
A Configuration Profile will be used to grant the Full Disk permissions necessary for the Agent to function correctly. Any permission overrides deployed by JAMF are not visible to users in **System Preferences > Security & Privacy > Full Disk Access** on the target machine(s). However, the pushed profile can be seen in **system Preferences > Profiles**.

To create a Configuration Profile:

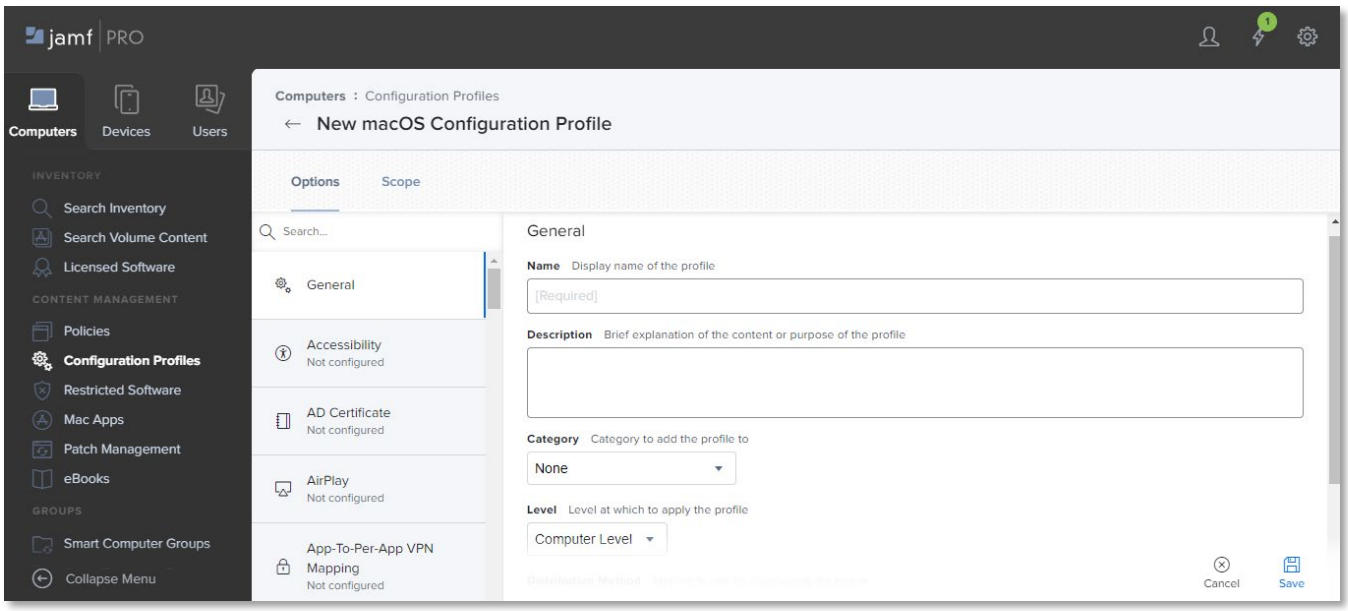
1. Log in to JAMF Pro application.
2. Click on **Computers**.



3. Click on **Configuration Profiles** from the left pane and click on **New**.



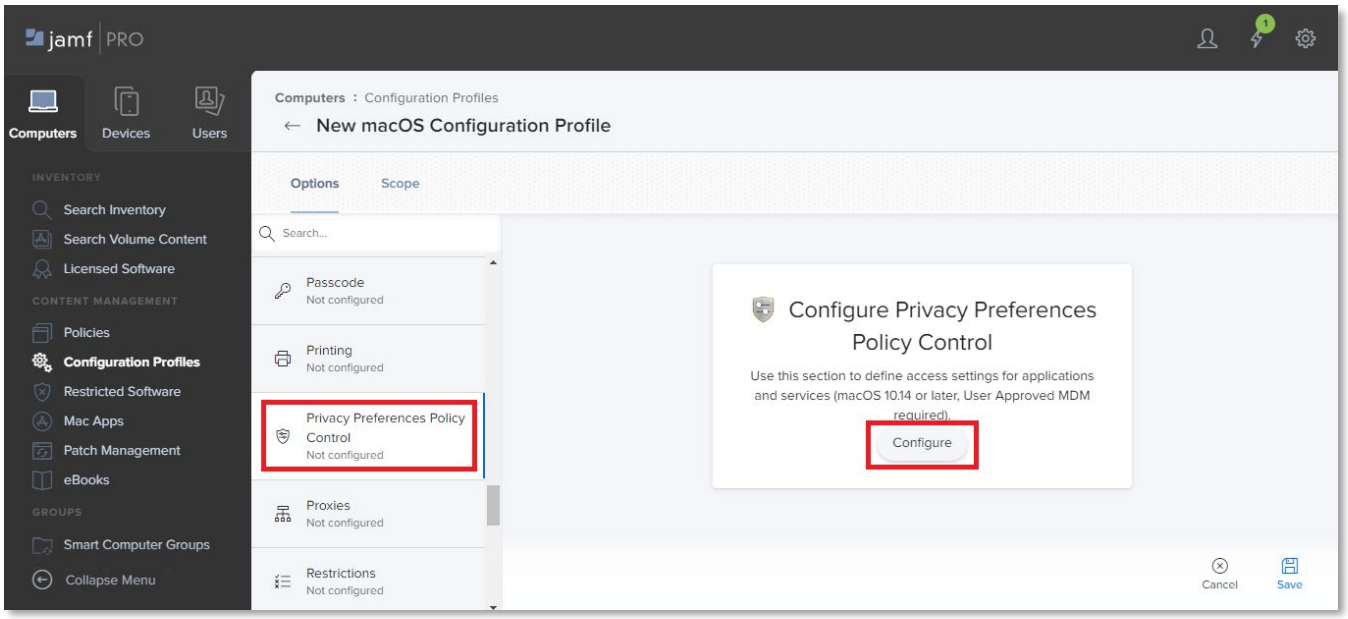
- The **New macOS Configuration Profile** page is displayed.



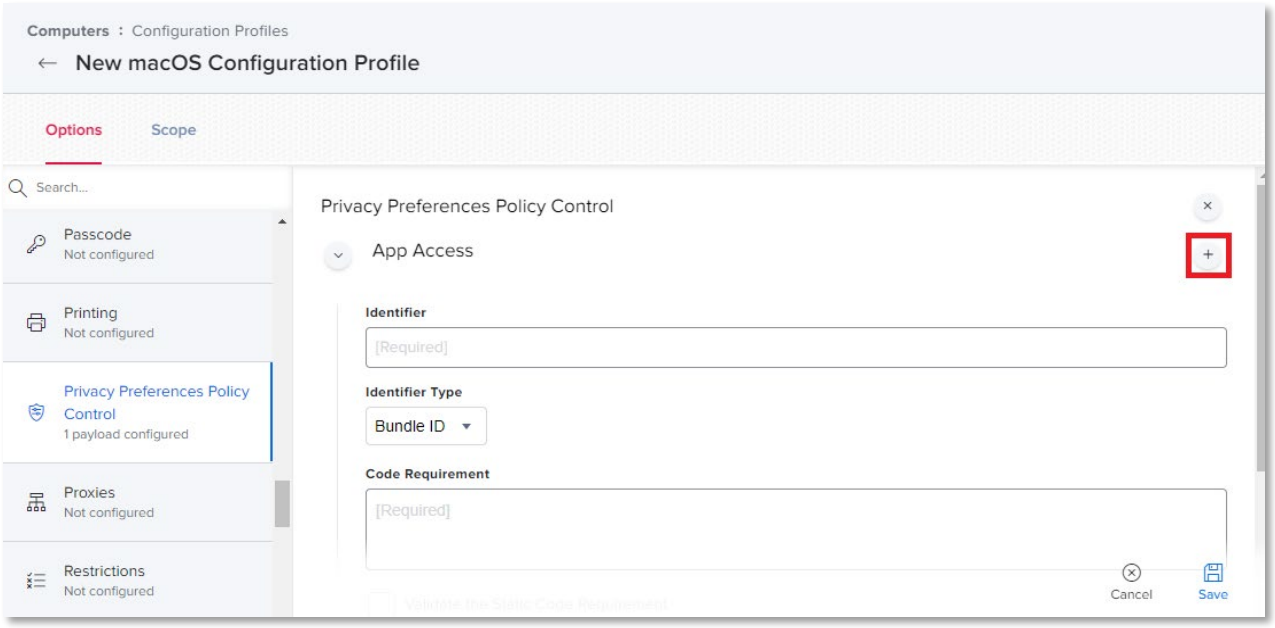
4. Provide the profile's **Name**.
5. Provide the **Description** of the profile.
6. Select the profile's **Category**.
7. Select the **Computer Level** option from the **Level** drop-down.
8. Select the required option for **Distribution Method**.

Note: *You are recommended to select* ***Install Automatically****.*

9. Scroll down and select the **Privacy Preferences Policy Control** tab from the middle pane.
10. Click **Configure**.



11. Create six **App Access** sections by clicking on the  button.



12. Provide following values for the corresponding fields in each **App Access** sections:

Identifier	Identifier Type
/Library/ExterroEnterpriseMacAgent/ADG.ManagedAgentSvc	Path

13. Provide following value for the **Code Requirement** field:

identifier ADG and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] / exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = Z5Y6K88KZA*

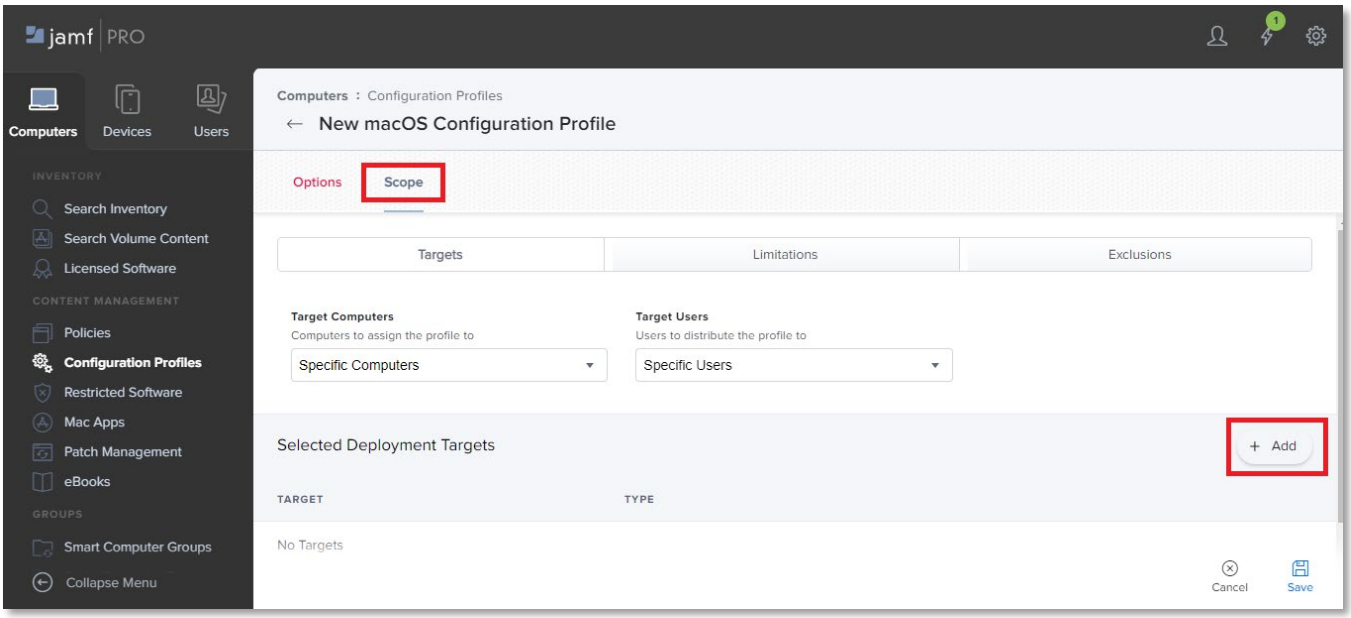
14. For each **App Access** section, follow the below steps:

    a. click **Add** and select the following values for the corresponding drop-down fields:

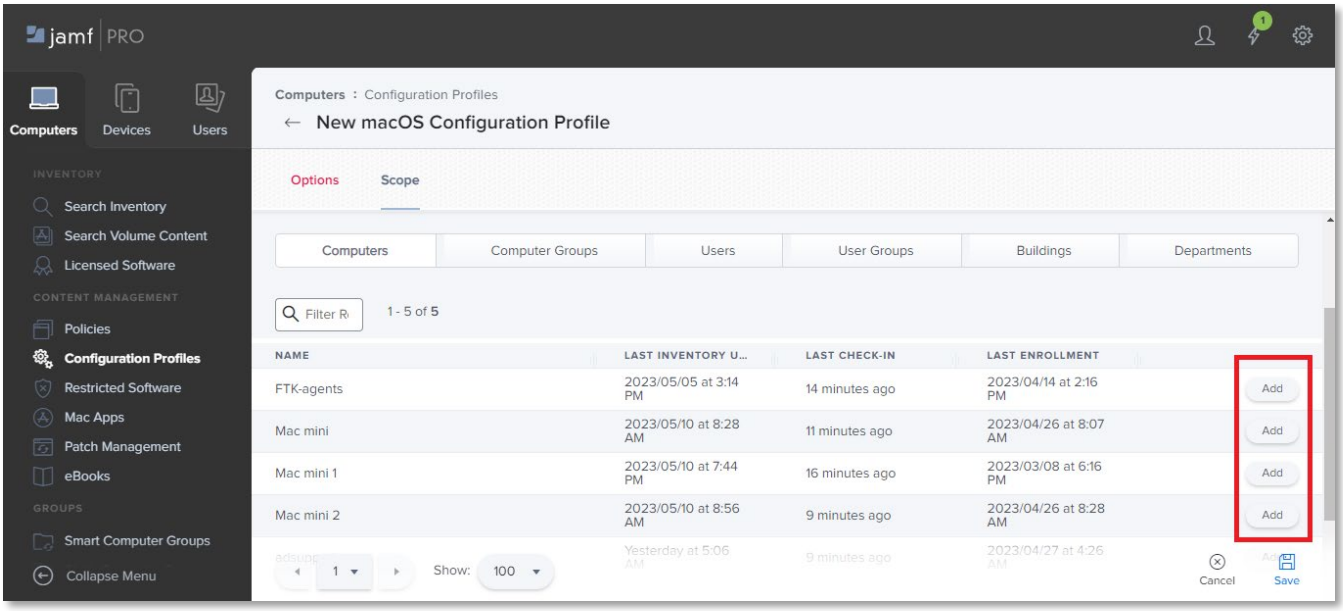
    - **App or Service** - SystemPolicySysAllFiles
    - **Access** – Allow

    b. Click **Save**.

15. Click on the **Scope** tab and click on **Add**.



16. Add the scope that includes the required target(s).



17. Click **Save**.

If the **Install Automatically** option was selected for **Distribution Method**, the new profile will start showing up on the targets the next time users check in to JAMF. (Refer **System Preferences** > **Profiles**).

Contact Exterro

If you have any questions, please refer to this document, or any other related materials provided to you by Exterro. For usage questions, please check with your organization's internal application administrator. Alternatively, you may contact your Exterro Training Manager or other Exterro account contact directly.

For technical difficulties, support is available through support@exterro.com.

Contact:

Exterro, Inc.

2175 NW Raleigh St., Suite 110

Portland, OR 97210.

Telephone: 503-501-5100

Toll Free: 1-877-EXTERRO (1-877-398-3776)

Fax: 1-866-408-7310

General E-mail:info@exterro.com

Website: www.exterro.com