



# **Forcepoint Dynamic User Protection**

**21.11**

**Neo macOS Installation Guide: Jamf  
Install**

## Contents

- [Install Neo using Jamf on page 2](#)
- [Troubleshooting Jamf installation on page 12](#)
- [Uninstall Neo using Jamf on page 17](#)
- [Appendix A: Manually creating the MDM profile on page 24](#)

# Install Neo using Jamf

Install Neo on macOS endpoints to get started analyzing your users with Dynamic User Protection or Cloud Security Gateway. Neo is a cloud-managed endpoint that runs on both Windows and macOS (as of version 21.02).

Use mobile device management (MDM) profiles via Jamf to install Neo on your macOS endpoints. This grants permissions and accessibility rules to Neo on the endpoint machines, allowing the installation to be completed without requiring administrator or user confirmation.

### Requirements for Neo installation:

- macOS Big Sur 11 or Monterey 12 with System Integrity Protection (SIP) enabled
- Preinstalled MDM profile
- At least one signed-in user

## Steps

- 1) Sign into the Dynamic User Protection management portal and download the macOS installation package, **fpneoinstaller\_mac.zip**.

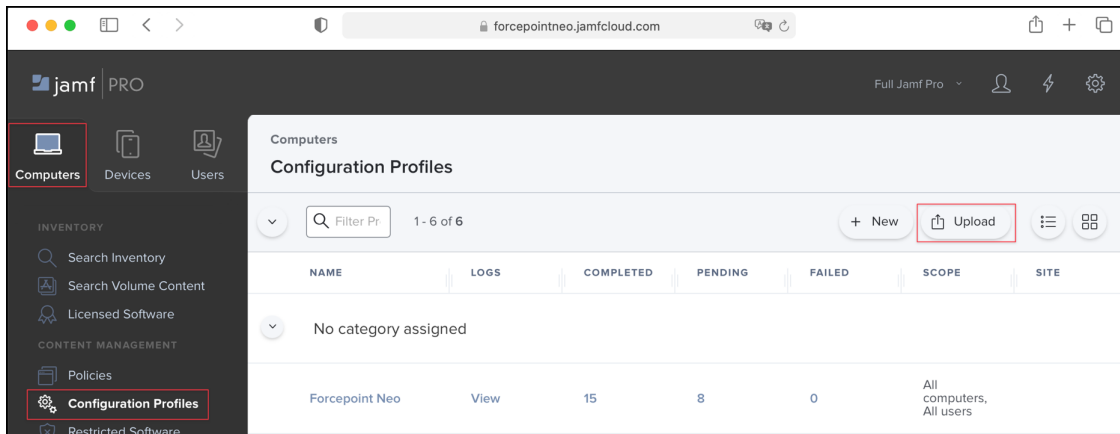
If you are a Forcepoint Cloud Security Gateway customer who wants to install Neo Web (proxy connect and direct connect modes), then download Neo from the Cloud Security Gateway Portal (**Web > Settings > Endpoint > General > Endpoint Client Download**).

The ZIP file contains the following files:

- The installation package
- The manifest JSON file
- Folder for installing Neo with Jamf
  - Instructions for installing Neo with Jamf
  - Forcepoint Neo profile file
  - Forcepoint Neo NC Root CA profile file
  - Forcepoint Cloud CA certificate file
  - Forcepoint Neo NC Root CA certificate file
- Folder for installing Neo manually
  - Instructions for installing Neo manually

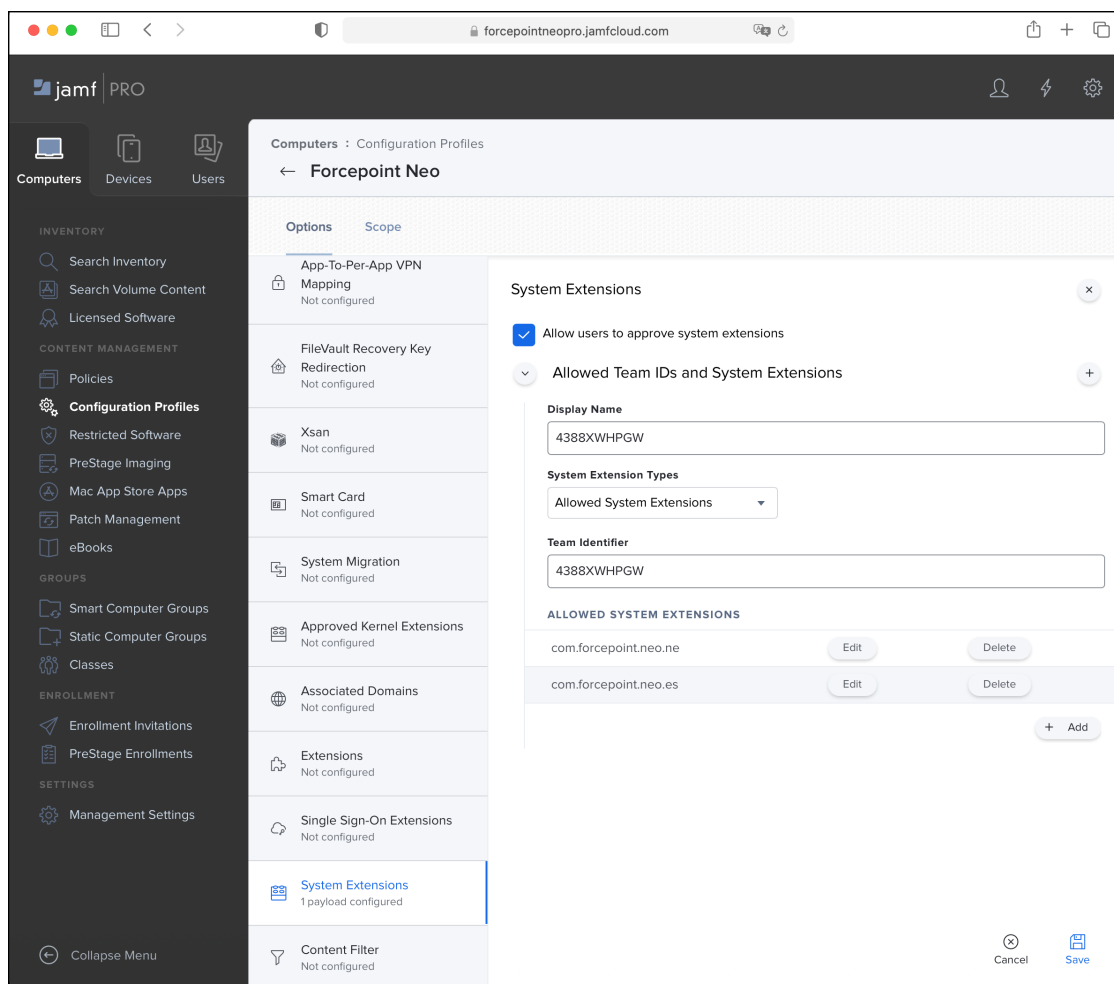
- 2) Unzip the installation package.

- 3) On an admin machine, use Safari to navigate to Jamf Pro.
- 4) Enter the administrator name and password, then click **Log in**.
- 5) Import the Forcepoint Neo profile file in Jamf Pro.
  - a) On the **Computers** tab, select **Configuration Profiles**, then click **Upload**.



- b) Select the **Forcepoint Neo.mobileconfig** configuration file.
- c) After the configuration file is uploaded, click **Remove Signature**. If the **Remove Signature** button does not appear, click **Edit** first.
- d) Click **Save**.

- e) On the **System Extensions** tab, enter the following information if it is not already populated:
  - i) Select the check box **Allow users to approve system extensions**
  - ii) **Display Name:** 4388XWHPGW
  - iii) From **System Extension Types**, select **Allowed System Extensions**
  - iv) **Team Identifier:** 4388XWHPGW
  - v) **Allowed System Extensions:** com.forcepoint.neo.ne, com.forcepoint.neo.es



- f) Click **Save**.

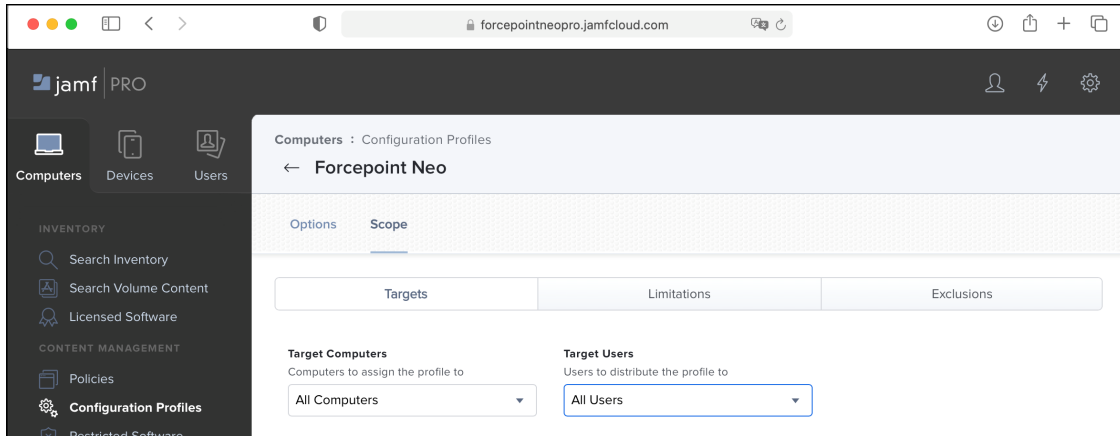


#### Note

If the profile was not imported correctly, you can manually create the MDM profile. See the procedure in Appendix A.

- 6) Deploy the Forcepoint Neo configuration profile to your endpoint machines.
  - a) On the **Computers** tab, select **Configuration Profiles**, then select the **Forcepoint Neo** profile.

- b) On the **Scope** tab, select **All Computers** and **All Users**.

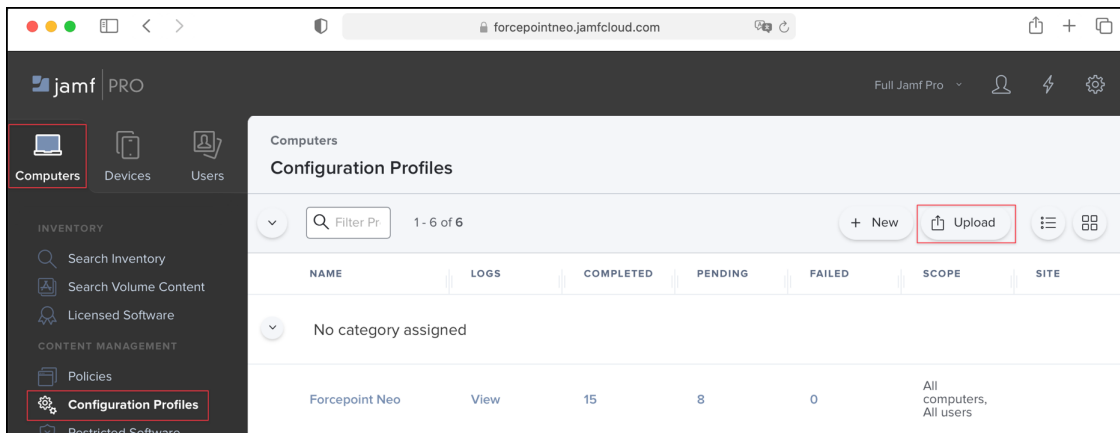


Alternatively, you can use this tab to specify certain individuals or groups on which to install Neo.

- c) Click **Save**.

- 7) Import the Forcepoint Neo NC Root CA profile file in Jamf Pro.

- a) On the **Computers** tab, select **Configuration Profiles**, then click **Upload**.



- b) Select the **Forcepoint Neo NC Root CA.mobileconfig** configuration file.

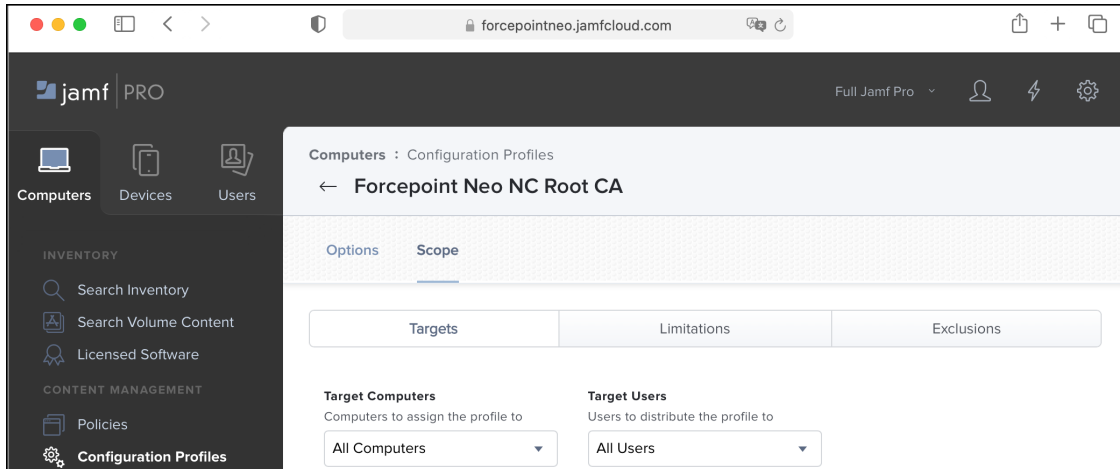
- c) After the configuration file is uploaded, click **Remove Signature**. If the **Remove Signature** button is not available, click **Edit**.

- d) Click **Save**.

- 8) Deploy the Forcepoint Neo NC Root CA configuration profile to your endpoint machines.

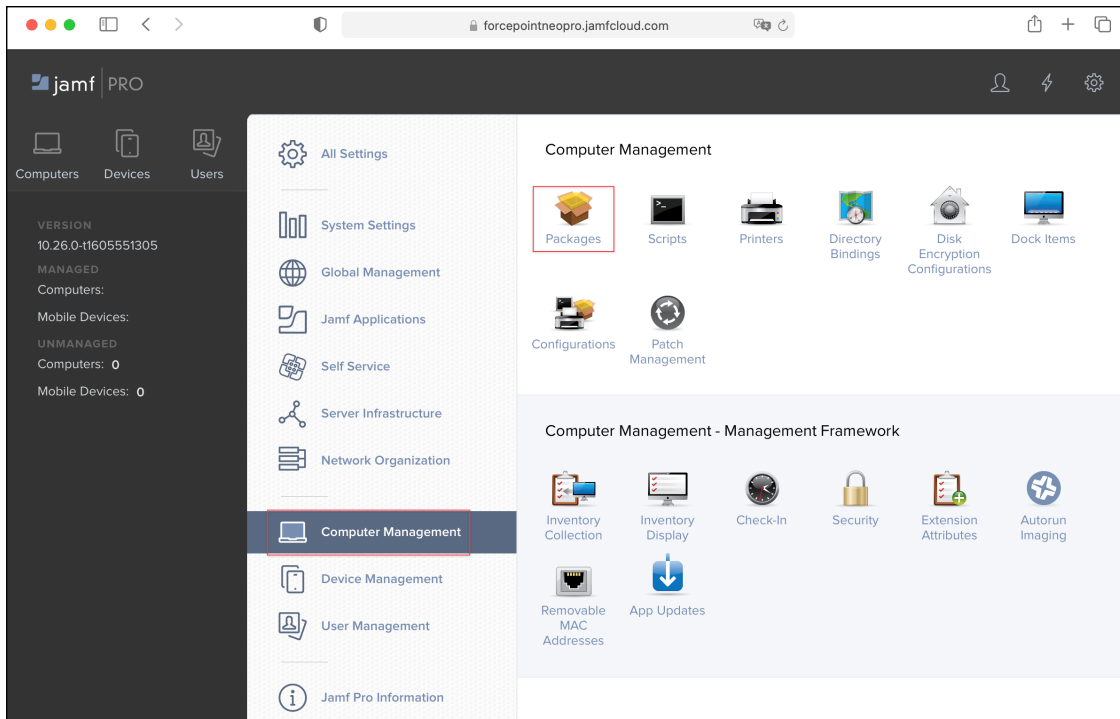
- a) On the **Computers** tab, select **Configuration Profiles**, then select the **Forcepoint Neo NC Root CA** profile.

- b) On the **Scope** tab, select **All Computers** and **All Users**.



Alternatively, you can use this tab to specify certain individuals or groups on which to install Neo.

- c) Click **Save**.
- 9) Create a policy to automatically deploy Neo on endpoint machines.
- a) Go to the **Computers** tab, then select **Management Settings**.
- b) Open the **Computer Management** menu, click **Packages**, then click **+ New**.



- c) Under **Filename**, click **Choose File**. Go to the location where you downloaded the Neo installation files. Select **fpneoinstaller\_mac.zip**, then click **Open**.

**Note**

You must select the **fpneoinstaller\_mac.zip** file and not the individual files within the zip file.

The screenshot displays the Jamf Pro web interface for creating a new package. The breadcrumb trail is 'Settings : Computer Management > Packages'. The page title is 'New Package'. There are three tabs: 'General' (selected), 'Options', and 'Limitations'. The 'Display Name' field contains 'fpneoinstaller\_mac'. The 'Category' dropdown is set to 'None'. The 'Filename' field contains 'fpneoinstaller\_mac.zip' and is highlighted with a red box; a 'Change File' button is next to it. Below this is the 'Manifest File' section with an 'Upload Manifest File' button. The 'Info' section has a text area for 'Information to display to the administrator when the package is deployed or uninstalled'. The 'Notes' section has a text area for 'Notes to display about the package (e.g. who built it and when it was built)'. At the bottom right are 'Cancel' and 'Save' buttons. The left sidebar shows the 'jamf PRO' logo, navigation icons for Computers, Devices, and Users, and system status: VERSION 10.26.0-11605551305, MANAGED Computers: 33, Mobile Devices: 0, UNMANAGED Computers: 2, Mobile Devices: 0. A 'Collapse Menu' button is at the bottom left of the sidebar.

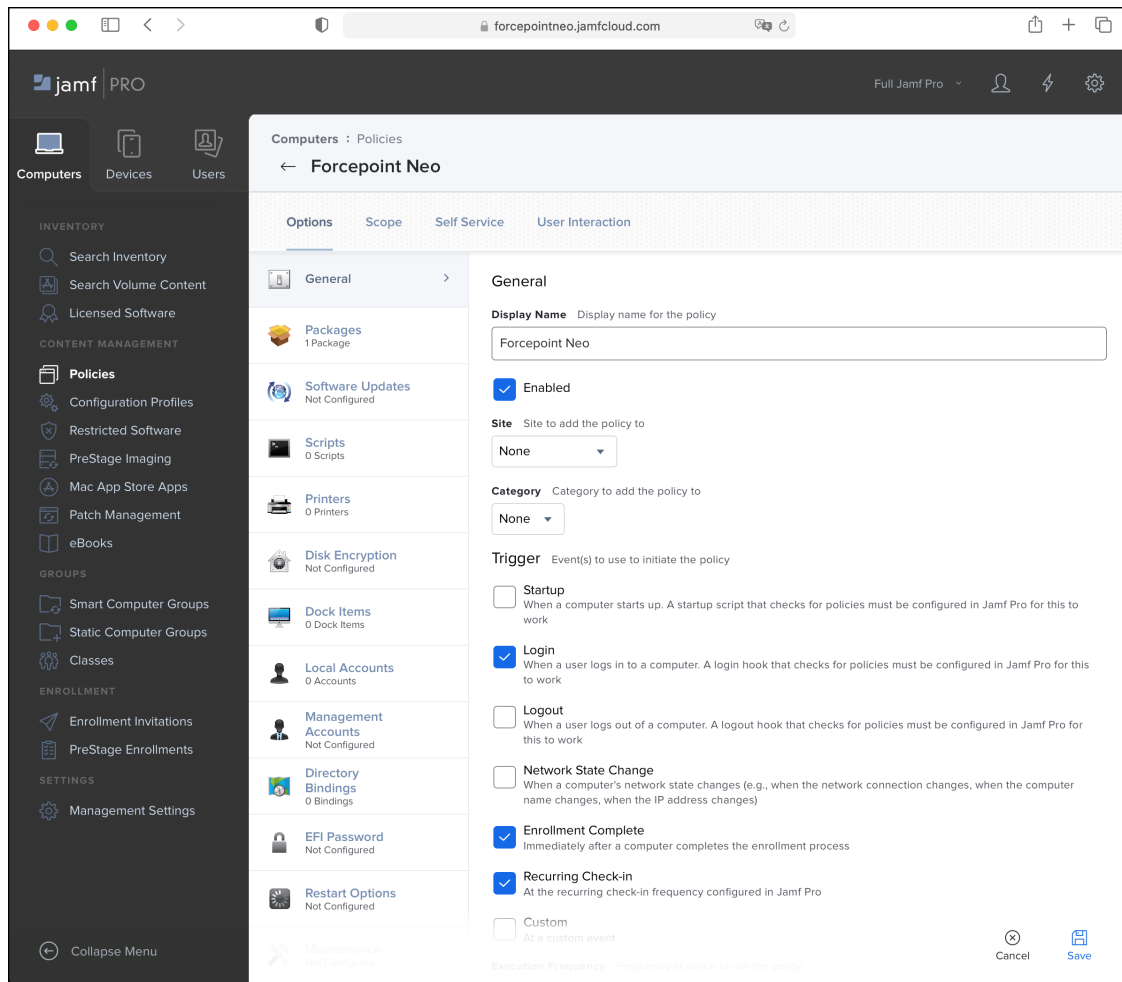
- d) On the **Computers** tab, select **Policies**, then click **+ New**.

e) Enter the following details:

i) **Display Name:** Forcepoint Neo

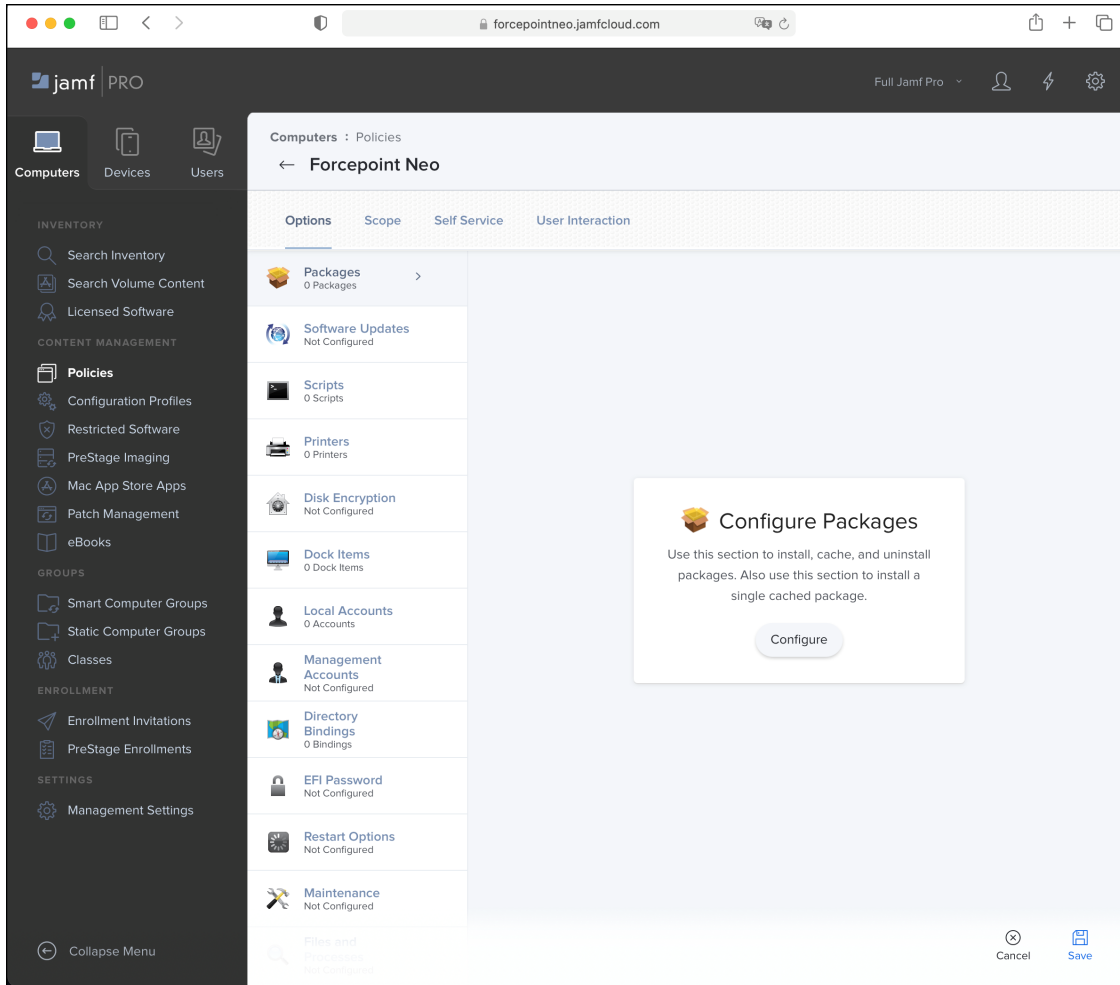
ii) Select the **Enabled** check box

iii) Under **Trigger**, select the trigger options to match your organization's routine. At least one user must be logged in when deployment starts. For example, if your organization enforces log out every night, then select **Login**. If your users rarely log out, then select **Recurring Check-in**. For freshly enrolled endpoints, select **Enrollment Complete**.



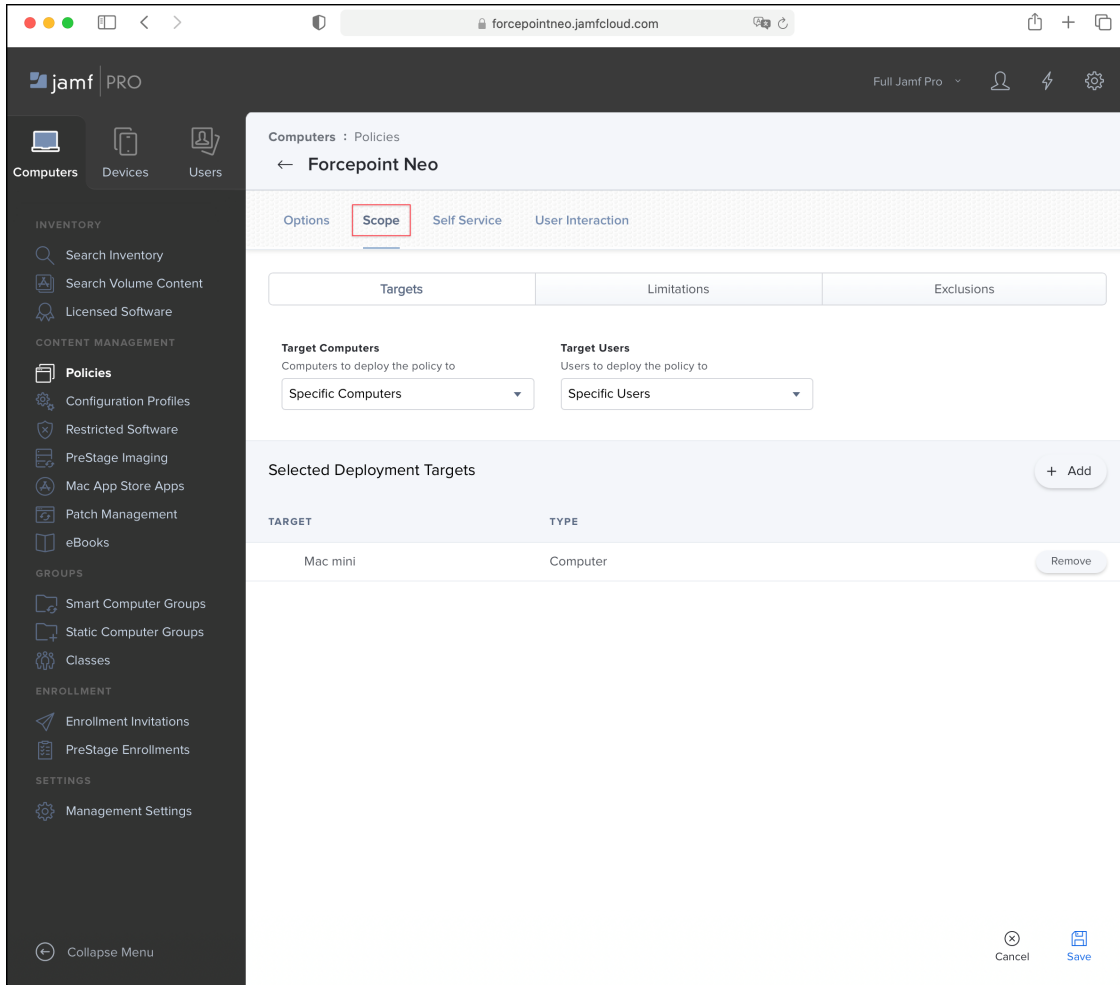


f) On the **Packages** tab, click **Configure Packages**.



g) Select the Neo package, then click **Add**.

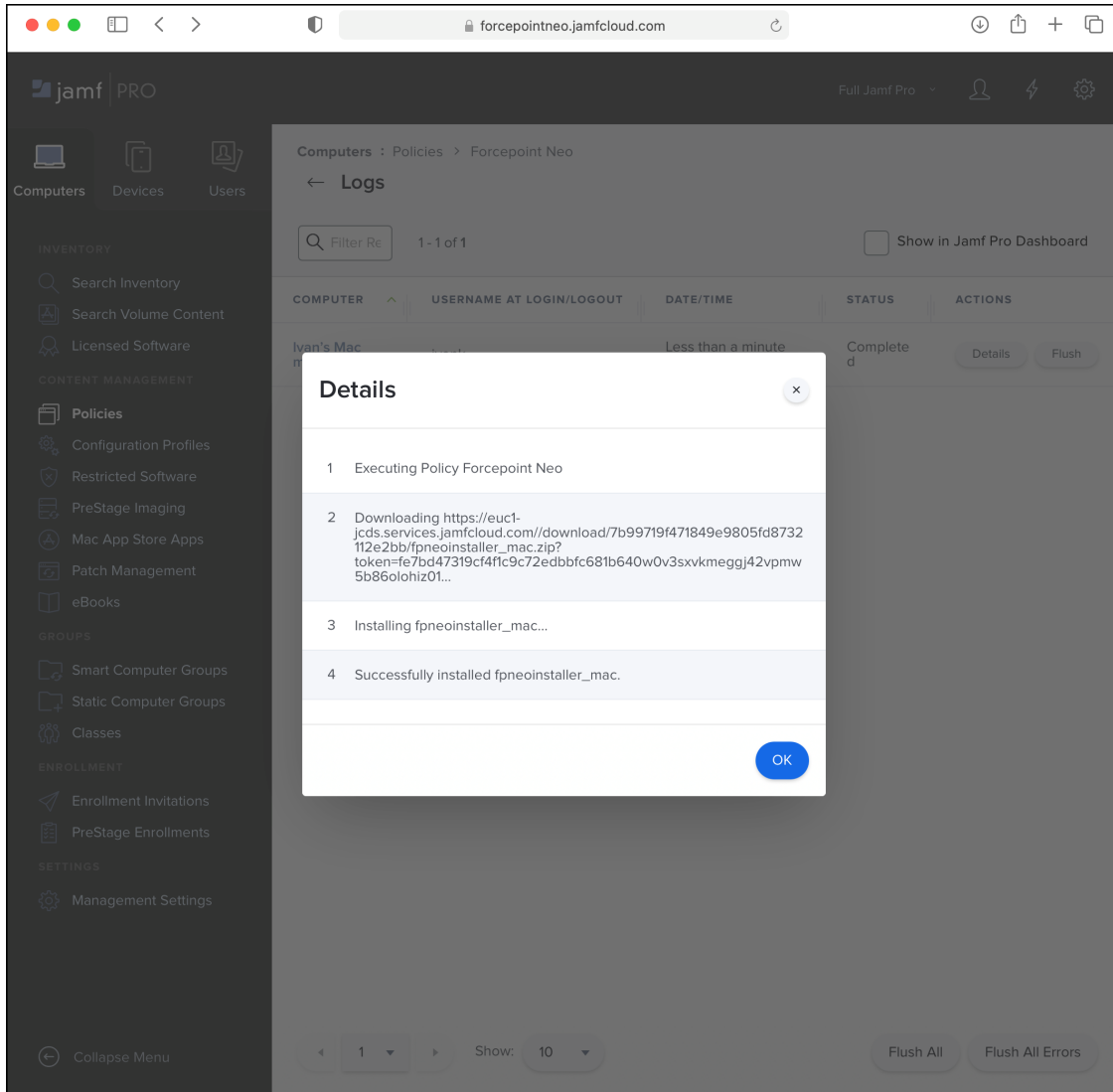
h) On the **Scope** tab, select **All Computers** and **All Users**.



Alternatively, use this tab to specify certain individuals or groups on which to install Neo.

i) Click **Save**.

j) Click **Logs** to verify the installation.



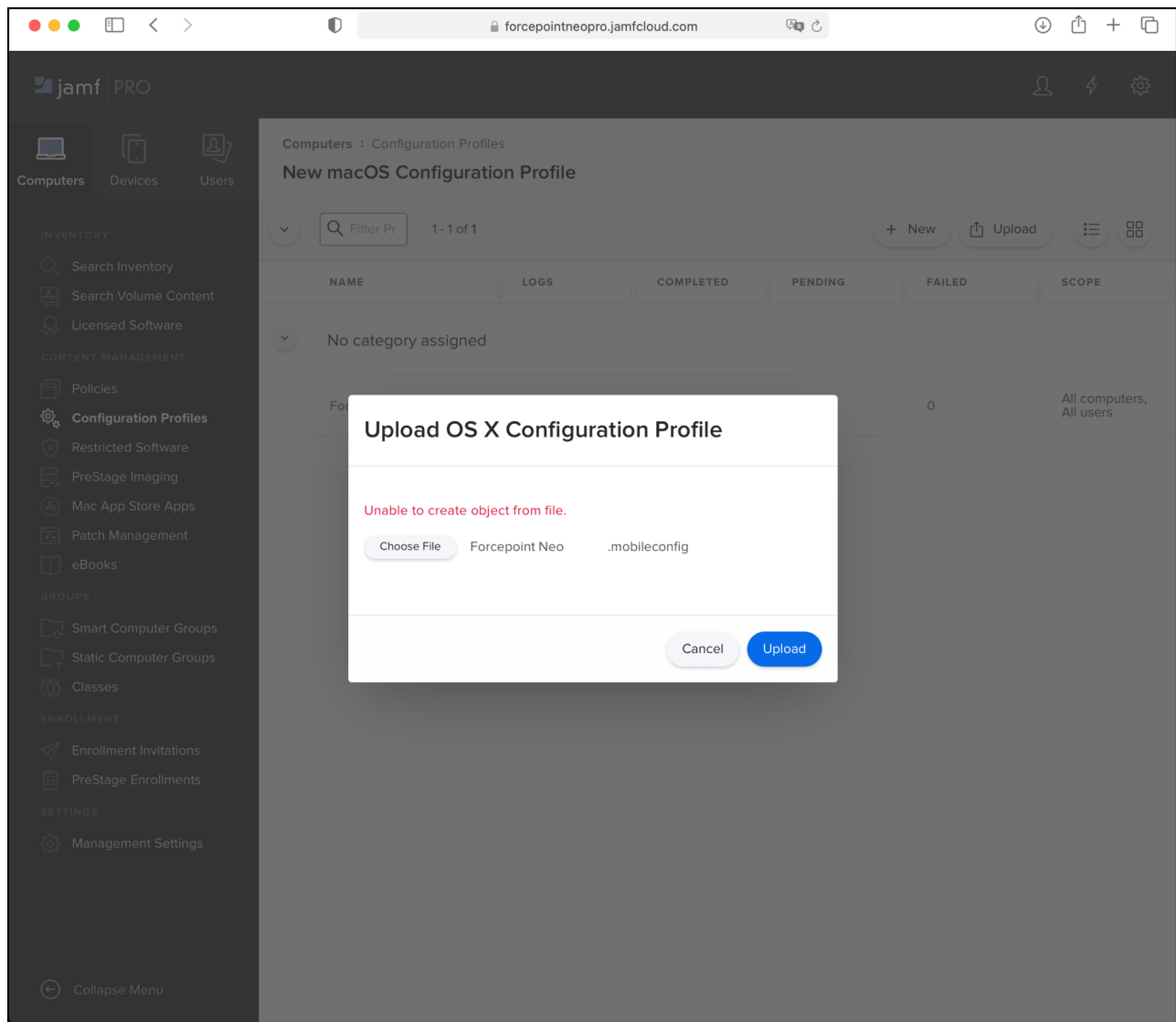
### Related tasks

Appendix A: Manually creating the MDM profile on page 24

# Troubleshooting Jamf installation

Troubleshooting helps you resolve common problems that you may encounter when installing Neo on macOS endpoints using Jamf.

## Error uploading a configuration profile



This error may occur when another configuration profile exists with the same `PayloadUUID` or `PayloadIdentifier`.

**Solution:** Remove the existing configuration profile before uploading a new one. Alternatively, open the configuration profile in a text editor and change all `PayloadUUID` or `PayloadIdentifier` values to unique values.

If the configuration profile is in a signed format, convert it to XML using the following command:

```
/usr/bin/security cmd -D -i signed_profile_path -o unsigned_profile_path
```

# The "Choose file" button is missing from the "New Package" section in Jamf

The screenshot shows the Jamf Pro web interface. The left sidebar contains navigation links for Computers, Devices, and Users, along with version and management statistics. The main content area is titled 'Settings : Computer Management > Packages' and 'New Package'. It has tabs for General, Options, and Limitations. The 'General' tab is active, showing fields for Display Name, Category, Filename, Manifest File, Info, and Notes. The 'Manifest File' section has an 'Upload Manifest File' button, but the 'Choose file' button is missing. The bottom right corner has 'Cancel' and 'Save' buttons.

jamf PRO

Computers Devices Users

VERSION  
10.26.0-t1605551305

MANAGED  
Computers: 5  
Mobile Devices: 0

UNMANAGED  
Computers: 0  
Mobile Devices: 0

Settings : Computer Management > Packages

← New Package

General Options Limitations

**Display Name** Display name for the package  
[Required]

**Category** Category to add the package to  
None

**Filename** Filename of the package on the distribution point (e.g. "MyPackage.dmg")  
[Required]

**Manifest File**  
Upload Manifest File

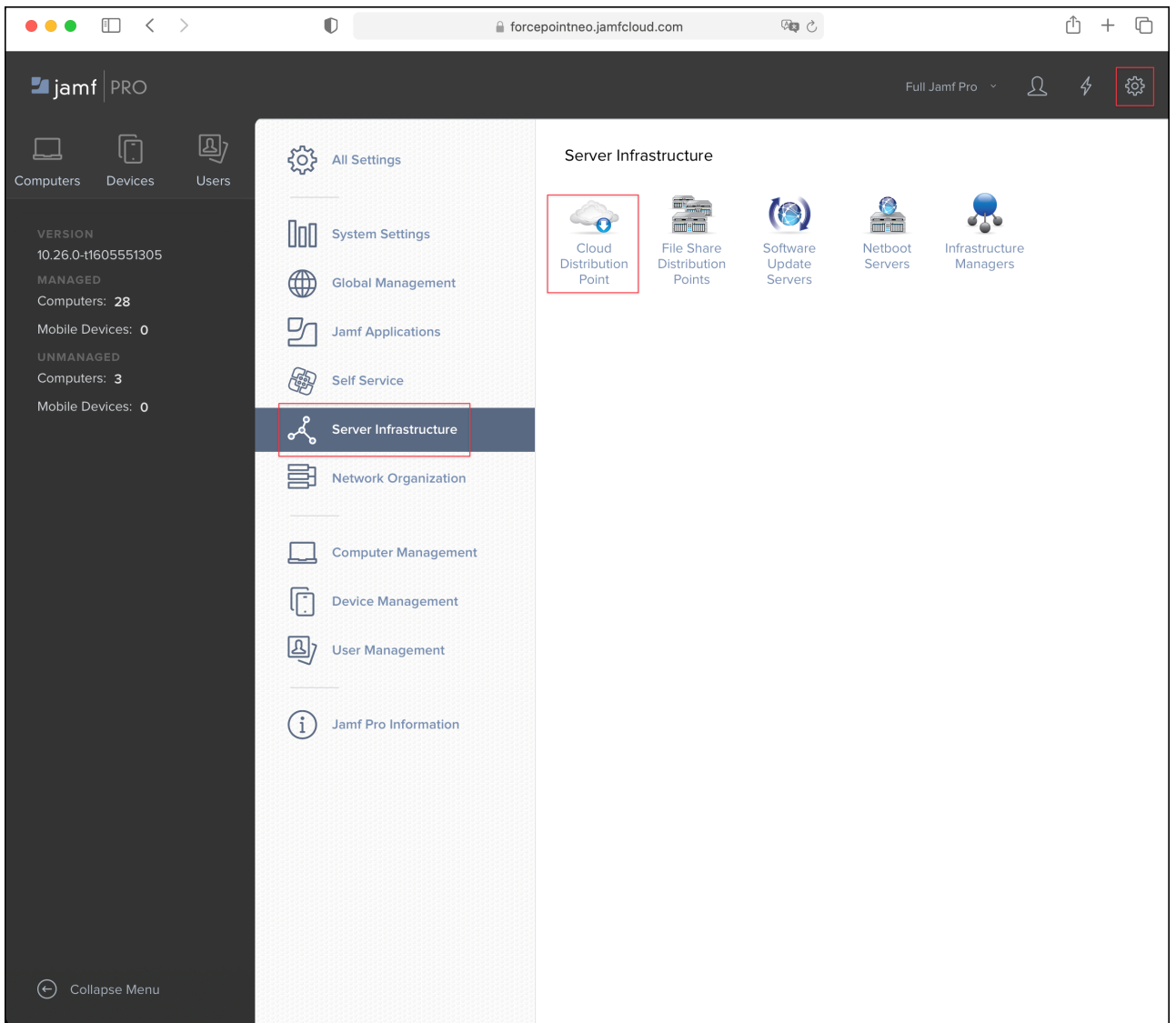
**Info** Information to display to the administrator when the package is deployed or uninstalled

**Notes** Notes to display about the package (e.g. who built it and when it was built)

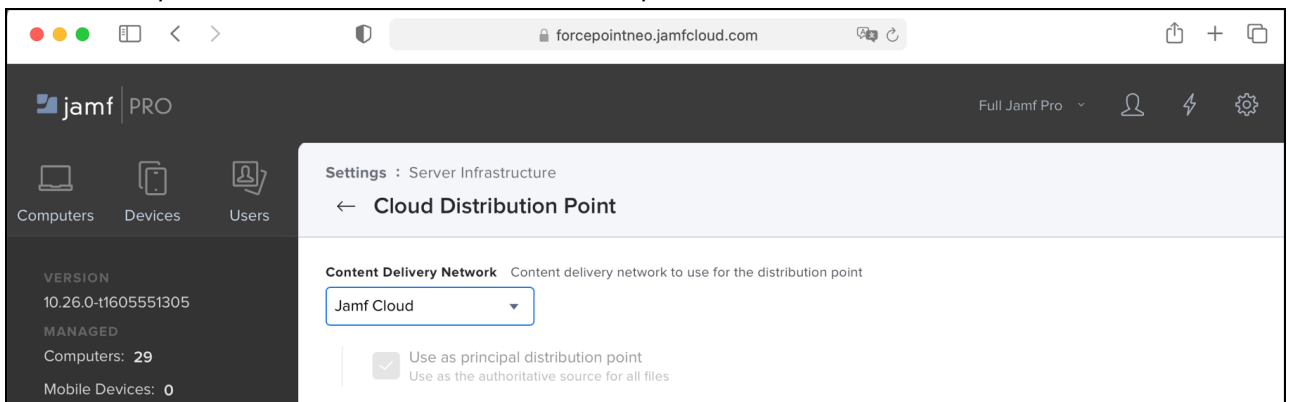
Cancel Save

## Solution:

- 1) Go to **Settings > Server Infrastructure > Cloud Distribution Point**.



2) From the drop-down menu, select a cloud distribution point, such as **Jamf Pro**.



3) Click **Save**.

# Failure deploying Neo endpoints

The screenshot shows the Jamf Pro web interface. The breadcrumb navigation is "Computers : Policies > Forcepoint Neo Production". The page title is "Logs". There is a search bar with "Filter Re" and "1 - 1 of 1" results. A checkbox "Show in Jamf Pro Dashboard" is present. The table has columns: COMPUTER, USERNAME AT LOGIN/LOGOUT, DATE/TIME, STATUS, and ACTIONS. One row is visible for "MacBookPro" with status "Failed". The "Details" button in the ACTIONS column is highlighted with a red box. The left sidebar contains various navigation options under categories like INVENTORY, CONTENT MANAGEMENT, GROUPS, ENROLLMENT, and SETTINGS. At the bottom, there are pagination controls showing "1" of 1 and "Show: 10", along with "Flush All" and "Flush All Errors" buttons.

COMPUTER	USERNAME AT LOGIN/LOGOUT	DATE/TIME	STATUS	ACTIONS
MacBookPro	i	Less than a minute ago	Failed	<a href="#">Details</a> <a href="#">Flush</a>

The screenshot displays the Jamf Pro web interface. The left sidebar contains navigation menus for 'Computers', 'Devices', 'Users', 'Inventory', 'Content Management', 'Groups', 'Enrollment', and 'Settings'. The main content area is titled 'Computers : Policies > Forcepoint Neo Production' and shows a 'Logs' section with a search filter and a table of logs. A 'Details' modal is open, showing a list of 6 steps in the installation process. The final step (6) indicates a failure: 'Installation failed. The installer reported: installer: Package name is Forcepoint Neo installer: Installing at base path / installer: The install failed. (The Installer encountered an error that caused the installation to fail. Contact the software manufacturer for assistance. An error occurred while running scripts from the package "neo\_installer-production.pkg")'. The modal has an 'OK' button at the bottom right. The background interface includes a 'Show in Jamf Pro Dashboard' checkbox and a table with columns for 'STATUS' and 'ACTIONS'.

forcepointneo.jamfcloud.com

jamf | PRO

Full Jamf Pro

Computers : Policies > Forcepoint Neo Production

← Logs

Filter Re 1 - 1 of 1

Show in Jamf Pro Dashboard

COMPUTER

MacBo

**Details**

- 1 Executing Policy Forcepoint Neo Production
- 2 Downloading neo\_installer-production.pkg...
- 3 Downloading [https://euc1-jcds.services.jamfcloud.com/download/7b99719f471849e9805fd8732112e2bb/neo\\_installer-production.pkg?token=20f2ea7311fb4c39b3f2702bff738062k3griqwbkpe1l12upx4goh7dr7k9hy3...](https://euc1-jcds.services.jamfcloud.com/download/7b99719f471849e9805fd8732112e2bb/neo_installer-production.pkg?token=20f2ea7311fb4c39b3f2702bff738062k3griqwbkpe1l12upx4goh7dr7k9hy3...)
- 4 Verifying package integrity...
- 5 Installing neo\_installer-production...
- 6 Installation failed. The installer reported: installer: Package name is Forcepoint Neo installer: Installing at base path / installer: The install failed. (The Installer encountered an error that caused the installation to fail. Contact the software manufacturer for assistance. An error occurred while running scripts from the package "neo\_installer-production.pkg")

OK

STATUS ACTIONS

Failed Details Flush

1 Show: 10

Flush All Flush All Errors



The most likely reason for installation failure is a missing MDM profile for Neo on the endpoint machine. Verify installation errors by examining the file `/private/var/log/install.log` on the endpoint machine. The possible error messages are as follows:

```
preinstall: BundleID "com.forcepoint.neo.es" for TeamID "4388XWHPGW" incorrect or missing
preinstall: BundleID "com.forcepoint.neo.ne" for TeamID "4388XWHPGW" incorrect or not found
preinstall: Identifier "/Library/PrivilegedHelperTools/com.forcepoint.neo.privilege-helper" for
service "SystemPolicyAllFiles" incorrect or missing
preinstall: CodeRequirement for Identifier "/Library/PrivilegedHelperTools/
com.forcepoint.neo.privilege-helper" for service "SystemPolicyAllFiles" incorrect or missing
preinstall: Identifier "com.forcepoint.neo.es" for service "SystemPolicyAllFiles" incorrect or
missing
preinstall: CodeRequirement for Identifier "com.forcepoint.neo.es" for service
"SystemPolicyAllFiles" incorrect or missing
preinstall: Identifier "com.forcepoint.neo.agent" for service "SystemPolicyAllFiles" incorrect or
missing
preinstall: CodeRequirement for Identifier "com.forcepoint.neo.agent" for service
"SystemPolicyAllFiles" incorrect or missing
preinstall: Identifier "com.forcepoint.neo.protectiond" for service "SystemPolicyAllFiles"
incorrect or missing
preinstall: CodeRequirement for Identifier "com.forcepoint.neo.protectiond" for service
"SystemPolicyAllFiles" incorrect or missing
preinstall: Identifier "com.forcepoint.neo.agent" for service "AppleEvents" incorrect or missing
preinstall: IdentifierType for Identifier "com.forcepoint.neo.agent" for service "AppleEvents"
incorrect or missing
preinstall: CodeRequirement for Identifier "com.forcepoint.neo.agent" for service "AppleEvents"
incorrect or missing
preinstall: Identifier "com.forcepoint.neo.agent" for service "Accessibility" incorrect or missing
preinstall: IdentifierType for Identifier "com.forcepoint.neo.agent" for service "Accessibility"
incorrect or missing
preinstall: CodeRequirement for Identifier "com.forcepoint.neo.agent" for service "Accessibility"
incorrect or missing
```

**Solution:** Apply the proper MDM configuration profile.

## Uninstall Neo using Jamf

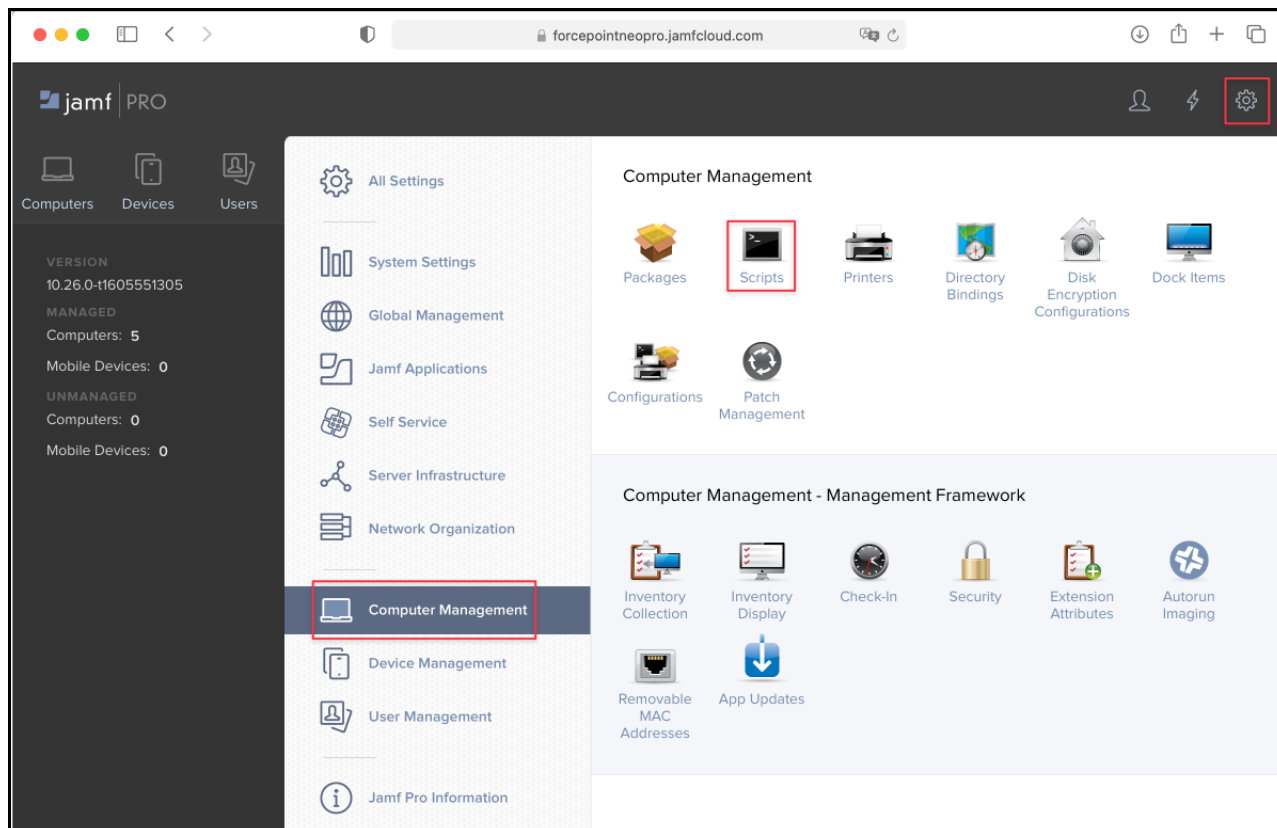
Uninstall Neo from macOS endpoints using Jamf Pro.

Create a Jamf policy to uninstall Neo from your endpoint machines.

### Steps

- 1) Sign in to Jamf Pro and go to **Computers > Settings**.

2) Open **Computer Management > Scripts**, then click **New**.



3) Under **Display Name**, enter the script name. For example, `uninstall_neo.sh`.

The screenshot shows the Jamf Pro web interface for configuring a script. The browser address bar shows `forcepointneo.jamfcloud.com`. The left sidebar displays the Jamf Pro logo and navigation icons for Computers, Devices, and Users. The main content area is titled 'Settings : Computer Management > Scripts' and shows the configuration for a script named 'run\_uninstall\_app.sh'. The 'General' tab is selected, showing the 'Display Name' field with the value 'run\_uninstall\_app.sh', the 'Category' dropdown set to 'None', and empty text boxes for 'Information' and 'Notes'. The bottom right corner has 'Cancel' and 'Save' buttons.

jamf | PRO

Full Jamf Pro

Computers Devices Users

VERSION  
10.26.0-t1605551305

MANAGED  
Computers: 28  
Mobile Devices: 0

UNMANAGED  
Computers: 3  
Mobile Devices: 0

Collapse Menu

Settings : Computer Management > Scripts

← run\_uninstall\_app.sh

General Script Options Limitations

**Display Name** Display name for the script

run\_uninstall\_app.sh

**Category** Category to add the script to

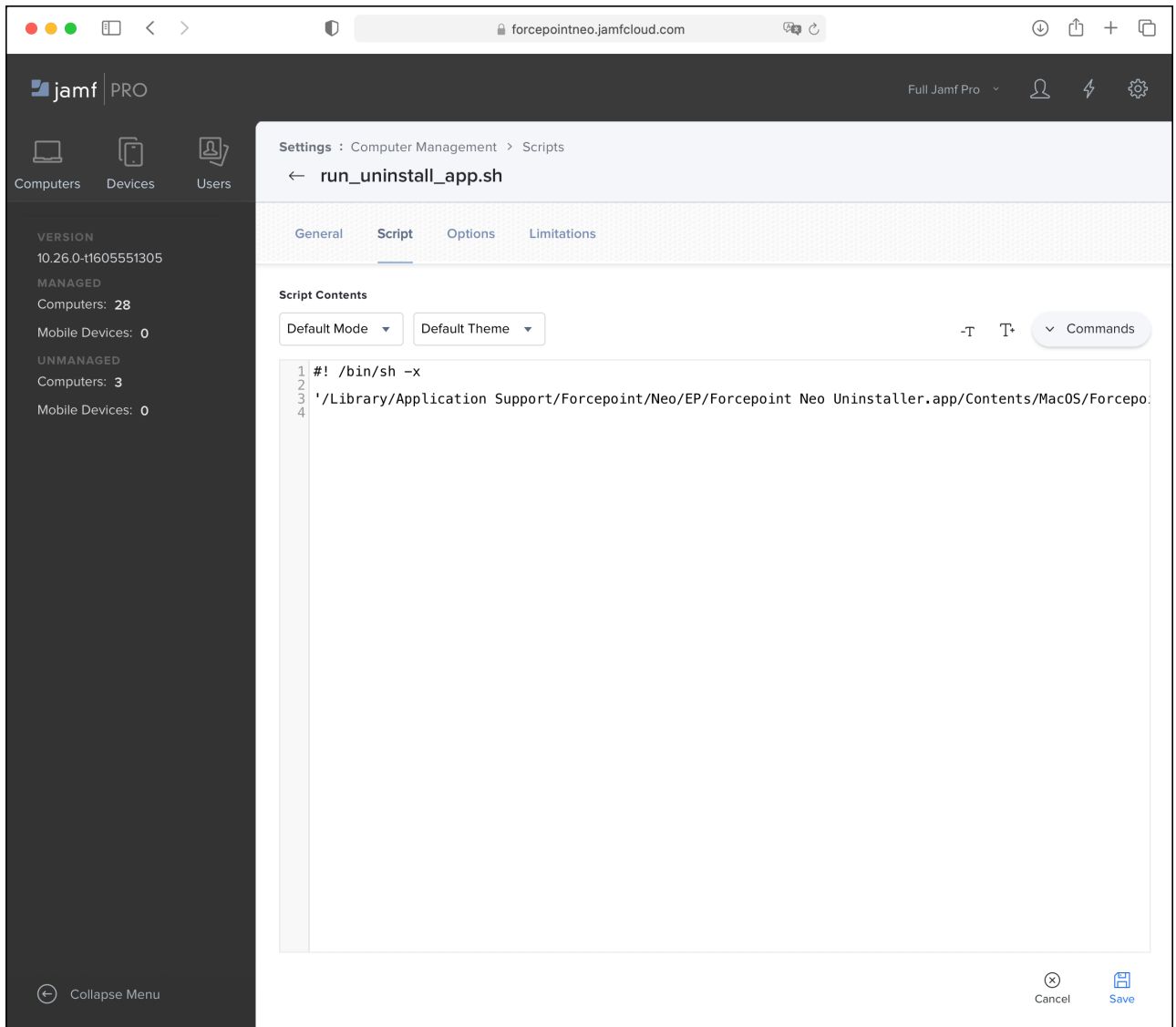
None

**Information** Information to display to the administrator when the script is run

**Notes** Notes to display about the script (e.g., who created it and when it was created)

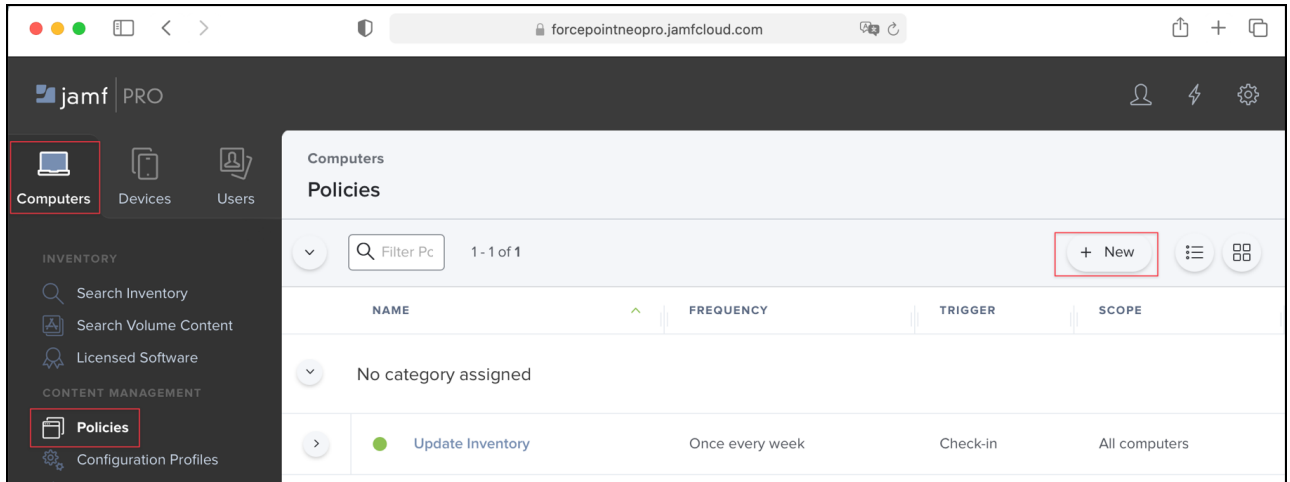
Cancel Save

- 4) On the **Script** tab, enter the following: `#!/bin/sh -x '/Library/Application Support/Forcepoint/Neo/EP/Forcepoint Neo Uninstaller.app/Contents/MacOS/Forcepoint Neo Uninstaller'`



- 5) Click **Save**.

6) Open **Computers > Policies**, then click **New**.



7) Enter the following details:

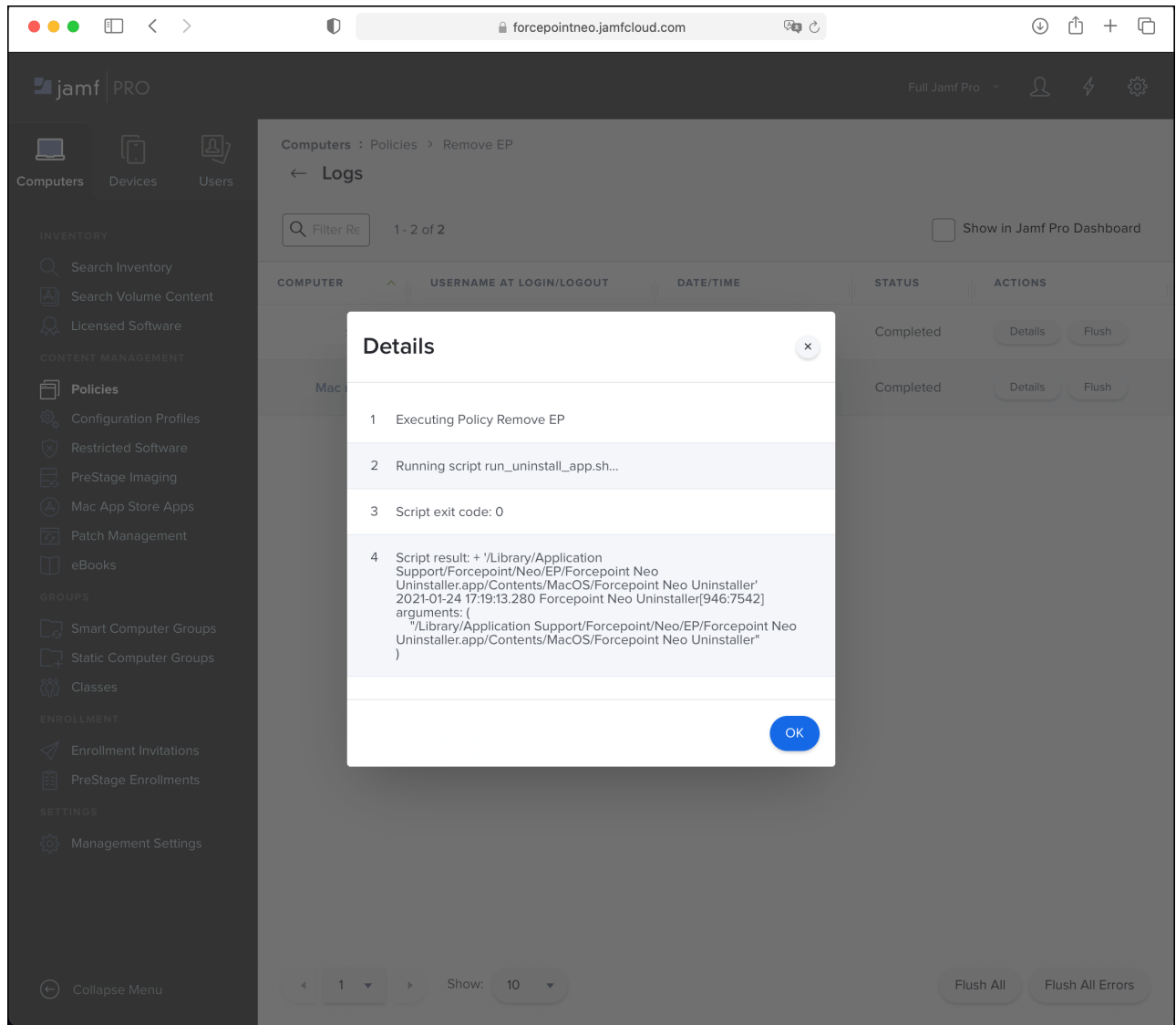
- a) **Display Name:** Remove Neo
- b) Select the **Enabled** check box

c) Under **Trigger**, select **Login**, **Enrollment Complete**, and **Recurring Check-in**.

The screenshot shows the Jamf Pro web interface for configuring a policy named "Remove Neo". The interface is divided into a left sidebar and a main content area. The sidebar contains navigation links for Computers, Devices, and Users, as well as a detailed inventory and management menu. The main content area is titled "Computers : Policies" and "Remove Neo". It features tabs for "Options", "Scope", "Self Service", and "User Interaction". The "Options" tab is selected, showing a "General" section with fields for "Display Name" (set to "Remove Neo"), "Enabled" (checked), "Site" (set to "None"), and "Category" (set to "None"). Below this is the "Trigger" section, which lists several events: "Startup", "Login", "Logout", "Network State Change", "Enrollment Complete", "Recurring Check-in", and "Custom". The "Login", "Enrollment Complete", and "Recurring Check-in" triggers are checked, indicating they are selected for the policy. The "Execution Frequency" field is at the bottom, with a note "Frequency at which to run the policy". At the bottom right, there are "Cancel" and "Save" buttons.

8) On the **Scripts** tab, click **Configure Scripts** and add the script created above.

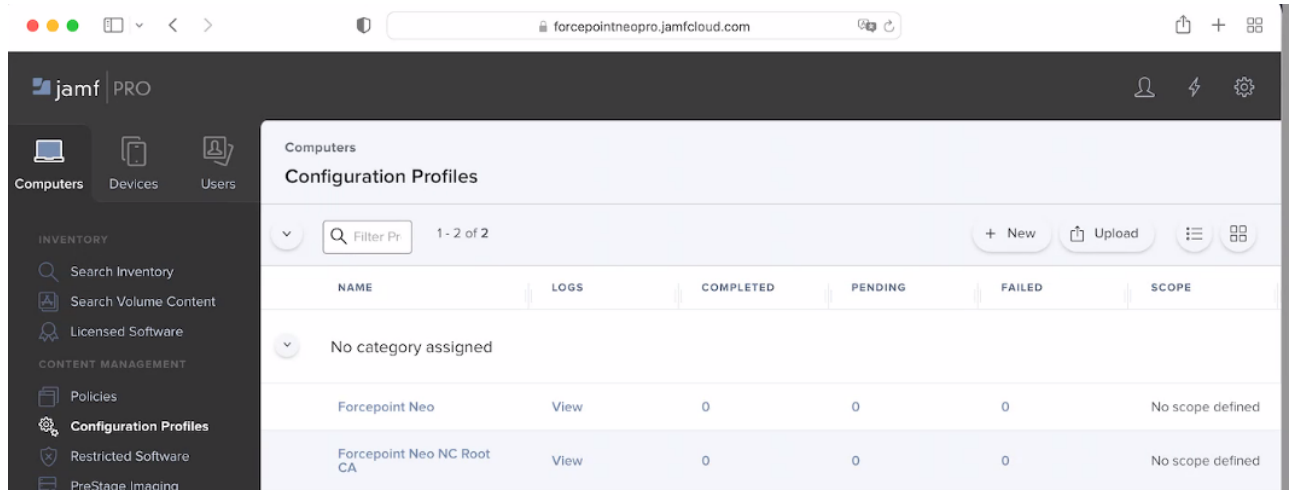
9) On the **Scope** tab, select **All Computers** and **All Users**.



#### Note

*Alternatively, use this tab to specify certain individuals or groups from which to uninstall Neo.*

- 10) Click **Save**.
- 11) Click **Logs** to verify the un-installation.

12) Open **Computers** tab > **Configuration Profiles**.

## 13) Remove Forcepoint Neo and Forcepoint Neo NC Root CA profiles.

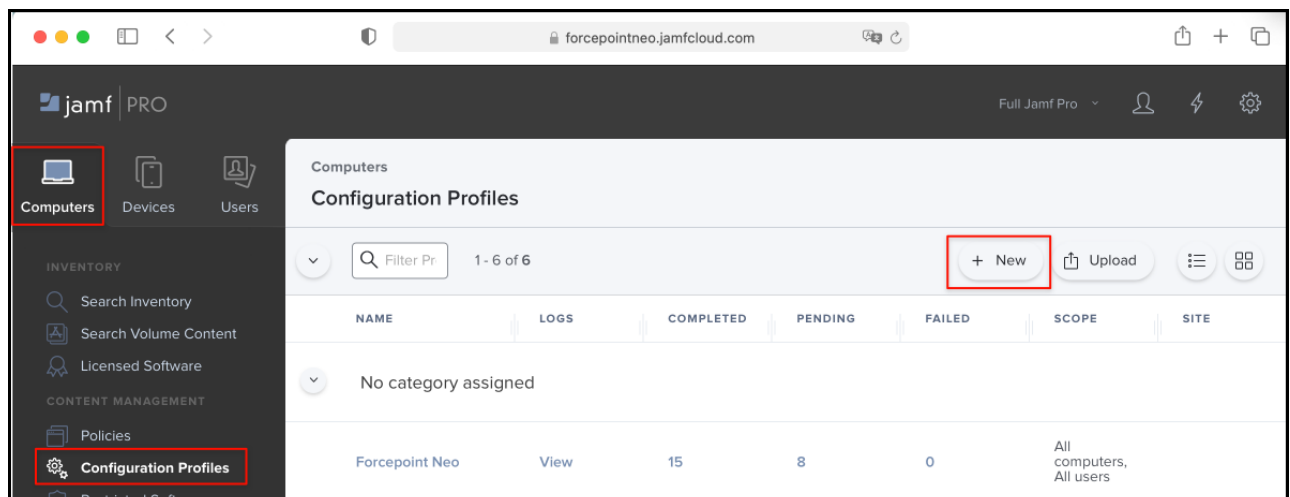
**Note**

*Alternatively, you can use the **Scope** tab inside each configuration profile to specify certain individuals or groups from which to uninstall Neo profiles.*

## Appendix A: Manually creating the MDM profile

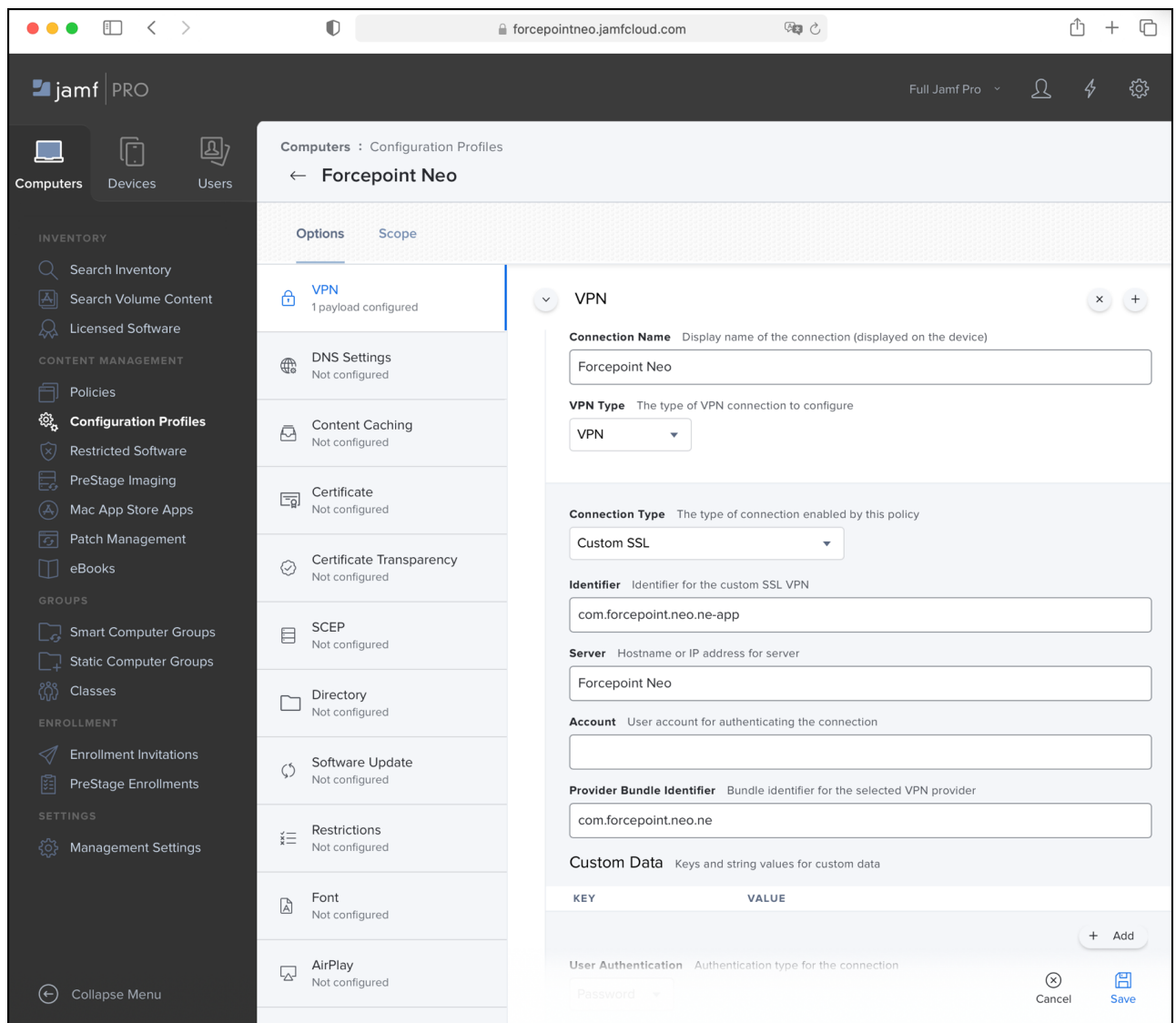
You can manually create the MDM profile if you have issues importing the MDM profile provided by Forcepoint.

### Steps

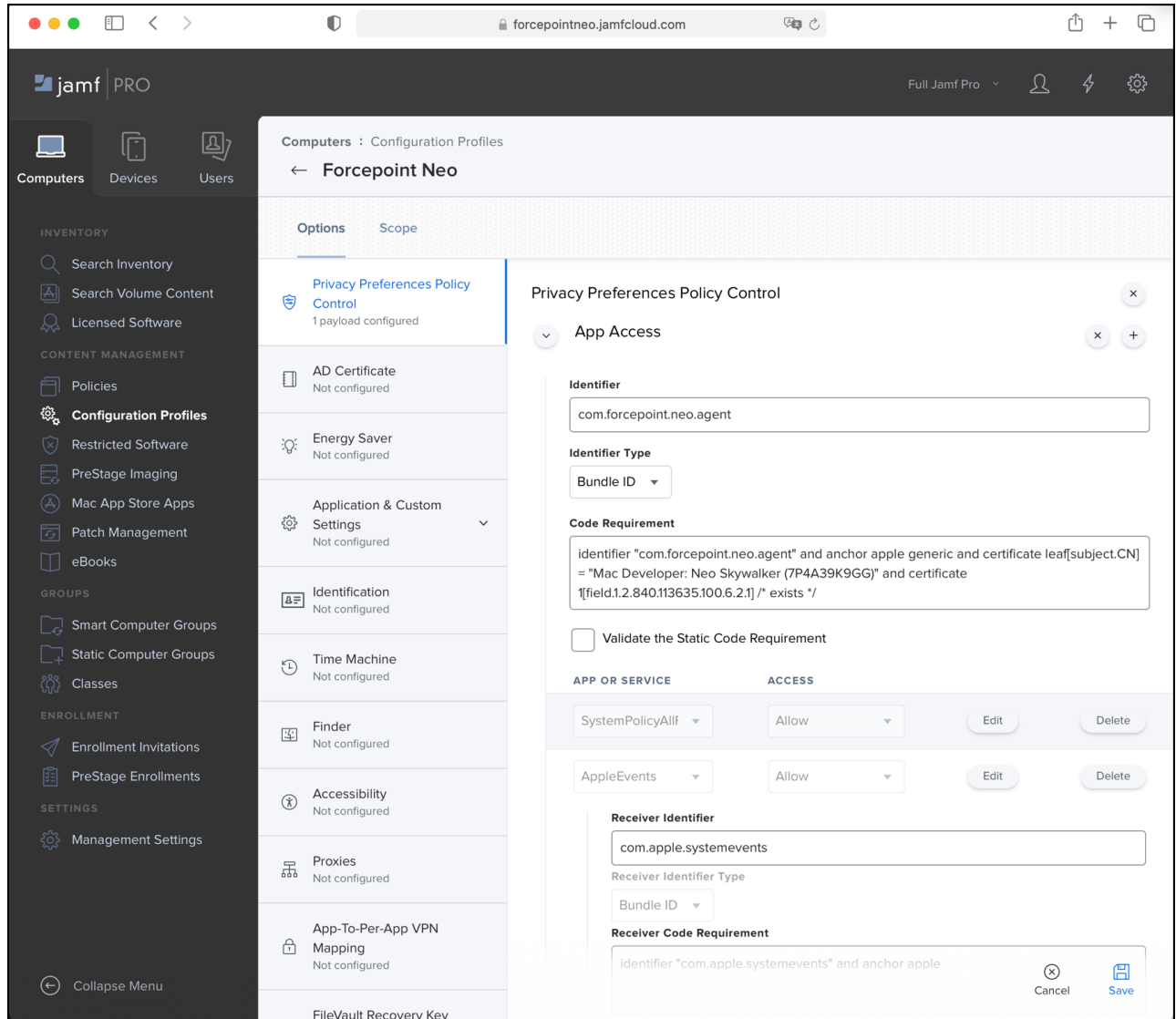
1) On the **Computers** tab, select **Configuration Profiles**, then click **New**.



- 2) On the **General** tab, enter `Forcepoint Neo` in the **Name** field.
- 3) On the **VPN** tab, enter the following:
  - a) **Connection Name:** `Forcepoint Neo`
  - b) **VPN Type:** `VPN`
  - c) **Identifier:** `com.forcepoint.neo.ne-app`
  - d) **Server:** `Forcepoint Neo`
  - e) **Provider Bundle Identifier:** `com.forcepoint.neo.ne`
  - f) Select the check box **Prohibit users from disabling on-demand VPN settings**



4) On the **Privacy Preferences Policy Control** tab, define the following components:



a) Enter the information for the first component.

- **Identifier:** com.forcepoint.neo.agent
- **Identifier Type:** Bundle ID
- **Code Requirement:** identifier "com.forcepoint.neo.agent" 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] = "4388XWHPGW"
- From **App or Service**, select **SystemPolicyAllFiles** and from **Access**, select **Allow**
- From **App or Service**, select **AppleEvents** and from **Access**, select **Allow**
- **Receiver Identifier:** com.apple.systemevents
- **Receiver Identifier Type:** Bundle ID
- **Receiver Code Requirement:** identifier "com.apple.systemevents" and anchor apple
- From **App or Service**, select **Accessibility**, and from **Access**, select **Allow**

b) Press the + button to add a new component, then enter the following information:

- **Identifier:** `com.forcepoint.neo.es`
- **Identifier Type:** **Bundle ID**
- **Code Requirement:** `identifier "com.forcepoint.neo.es" 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] = "4388XWHPGW"`
- From **App or Service**, select **SystemPolicyAllFiles**, and from **Access**, select **Allow**

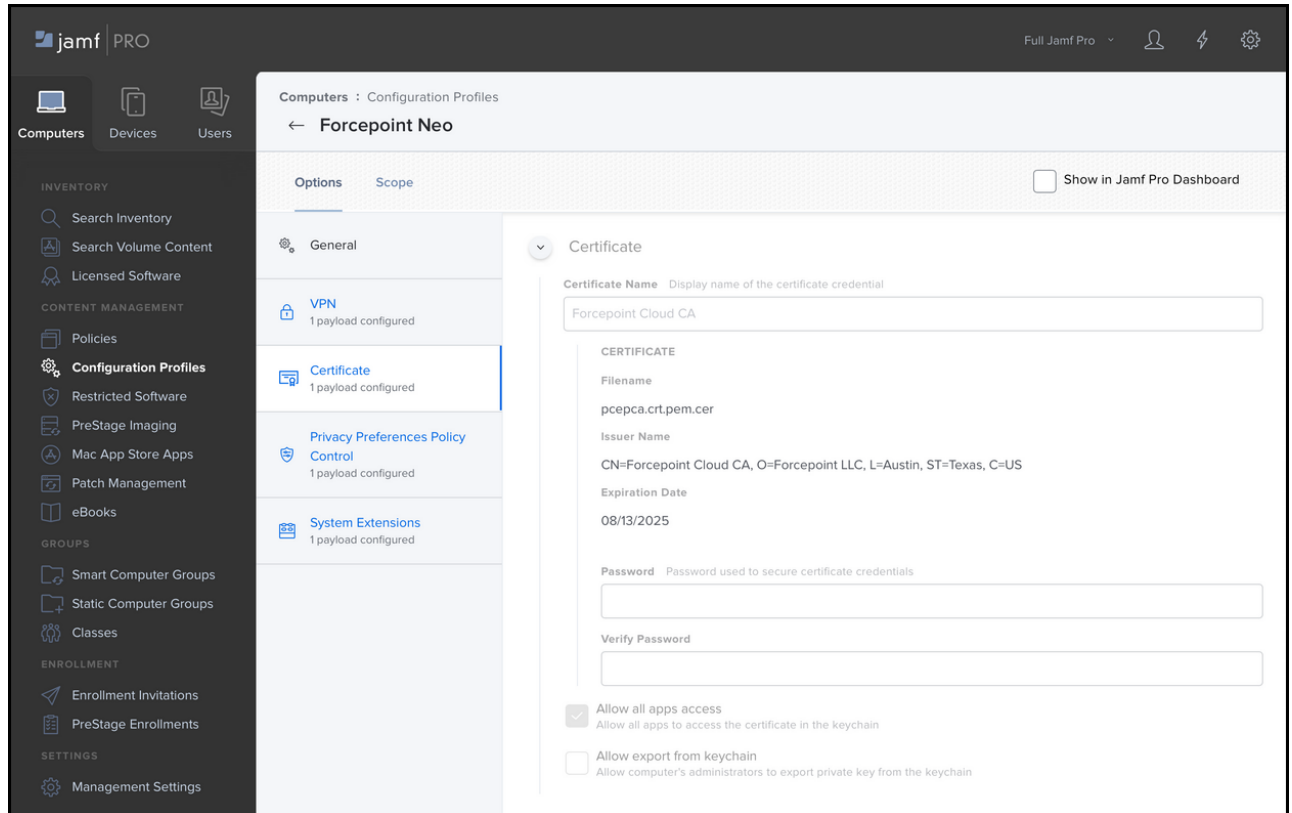
c) Press the + button to add a new component, then enter the following information:

- **Identifier:** `/Library/Application Support/Forcepoint/Neo/EP/bin/fpneoprotectiond`
- **Identifier Type:** **Path**
- **Code Requirement:** `identifier "com.forcepoint.neo.protectiond" 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] = "4388XWHPGW"`
- From **App or Service**, select **SystemPolicyAllFiles**, and from **Access**, select **Allow**

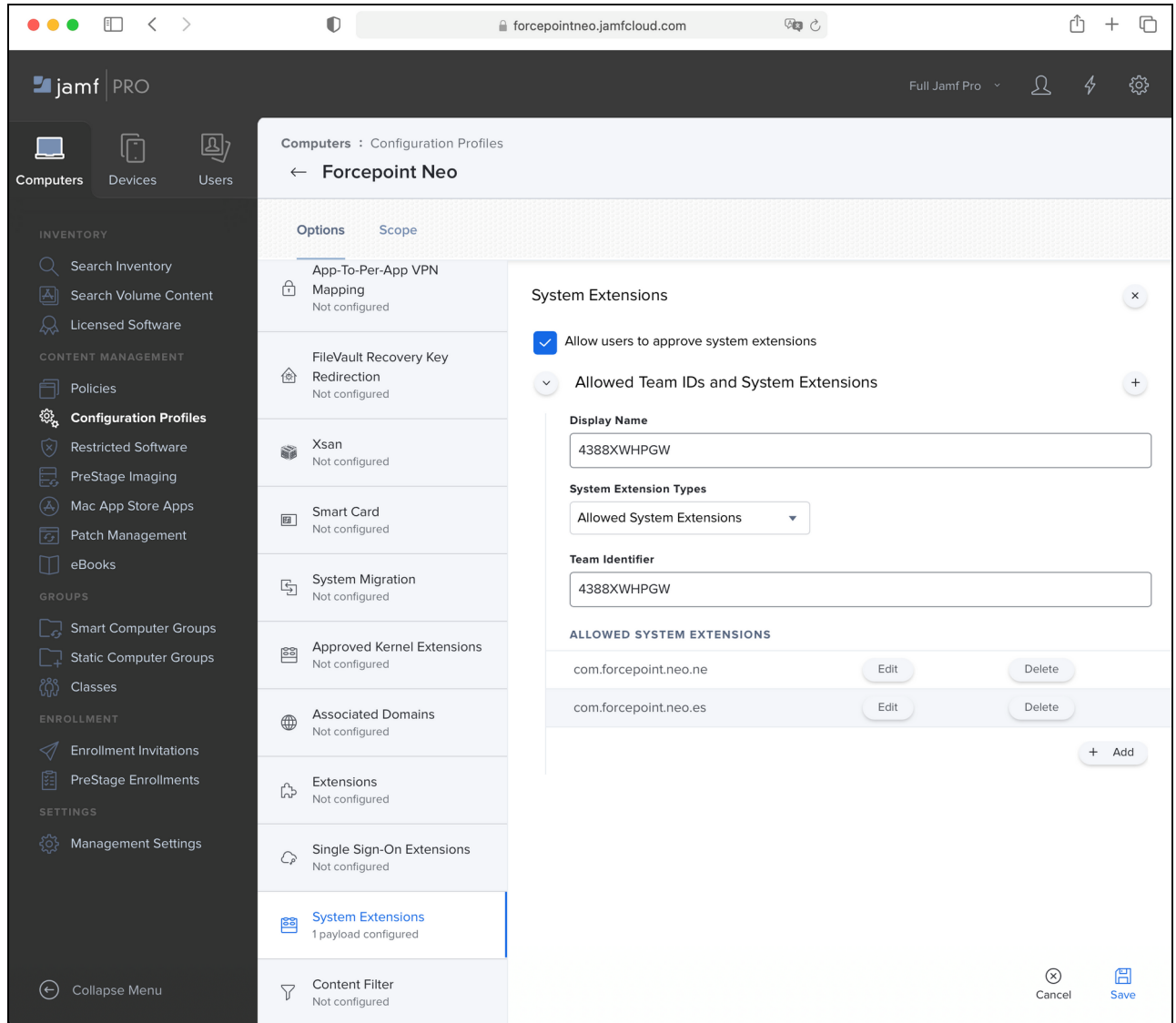
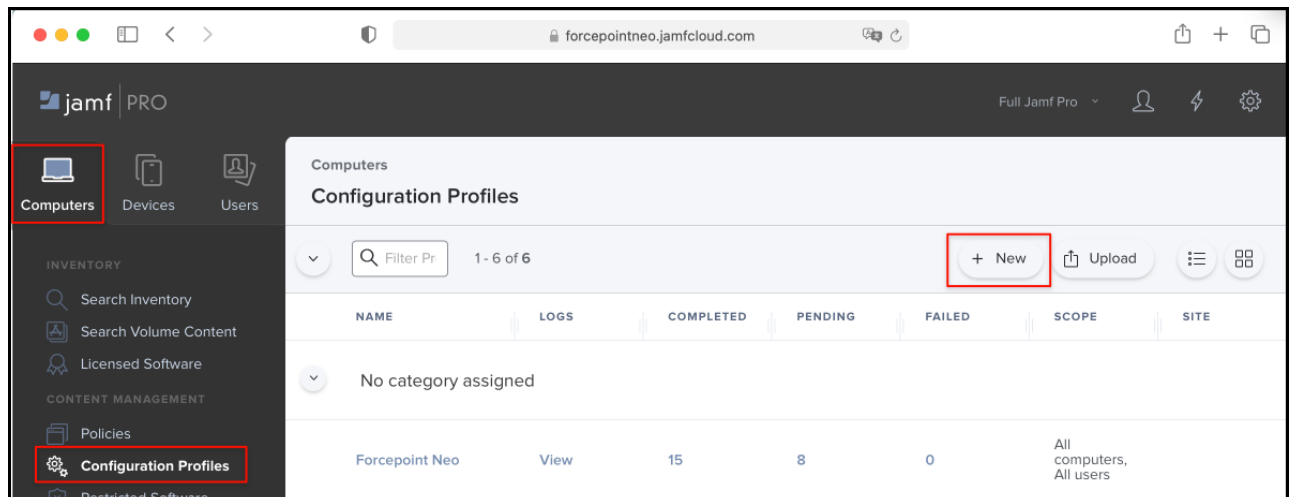
d) Press the + button to add a new component, then enter the following information:

- **Identifier:** `/Library/PrivilegedHelperTools/com.forcepoint.neo.privilege-helper`
- **Identifier Type:** **Path**
- **Code Requirement:** `identifier "com.forcepoint.neo.privilege-helper" 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] = "4388XWHPGW"`
- From **App or Service**, select **SystemPolicyAllFiles**, and from **Access**, select **Allow**

- 5) On the **Certificate** tab, define the following components:
- Under **Certificate Name**, enter **Forcepoint Cloud CA**.
  - Upload the **Forcepoint Cloud CA.cer** file.
  - Select **Allow all apps access**.
  - Make sure **Allow export from keychain** is not selected.



- 6) Click **Save**.
- 7) On the **System Extensions** tab, enter the following:
- a) Select the check box **Allow users to approve system extensions**
  - b) **Display Name:** 4388XWHPGW
  - c) From **System Extension Types**, select **Allowed System Extensions**
  - d) **Team Identifier:** 4388XWHPGW

**e) Allowed System Extensions:** `com.forcepoint.neo.ne`, `com.forcepoint.neo.es`**8) On the Computers tab, select Configuration Profiles, then click New.**

- 9) On the **General** tab, enter `Forcepoint Neo NC Root CA` in the **Name** field.
- 10) On the **Certificate** tab, define the following components:
  - Under **Certificate Name**, enter **Forcepoint Neo NC Root CA**.
  - Upload the **Forcepoint Neo NC Root CA.cer** file.
  - Select **Allow all apps access**.
  - Make sure **Allow export from keychain** is not selected.

