Deploy ESET Endpoint products for macOS using Jamf Pro

Steef | ESET Nederland - 2021-02-23 - Comments (0) - ESET Endpoint Security

Issue

- Jamf Pro deployment for ESET Endpoint for macOS Big Sur
- Configure System Extensions and Privacy Preference Policy Control (PPPC)
- Create Policies
- Additional Options
- Jamf Pro deployment for ESET Endpoint for macOS (earlier versions)

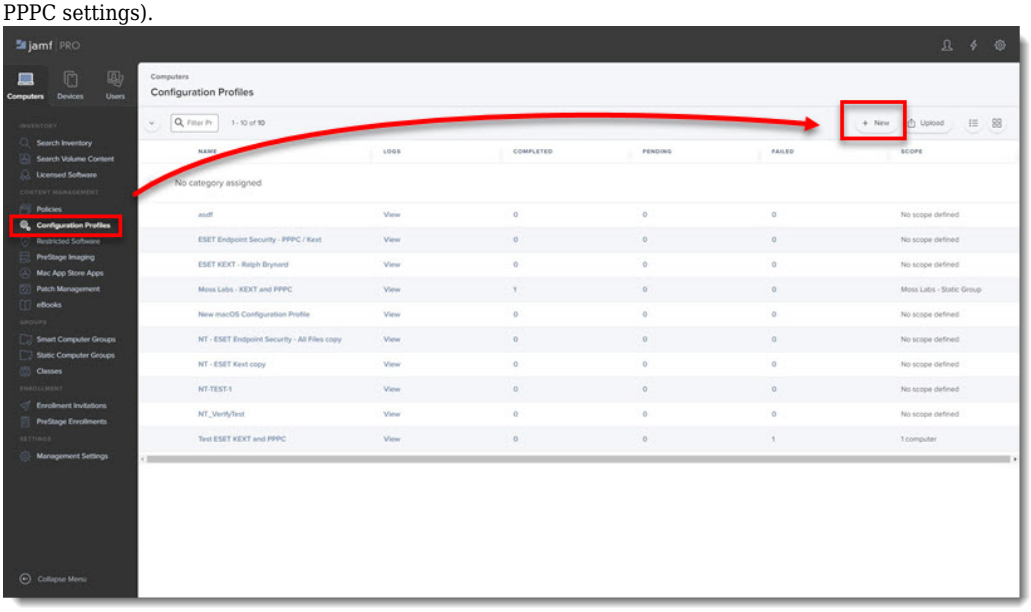
Solution

Follow the instructions below to deploy ESET Endpoint for macOS Big Sur using Jamf Pro to manage using ESET Security Management Center/ESET PROTECT.

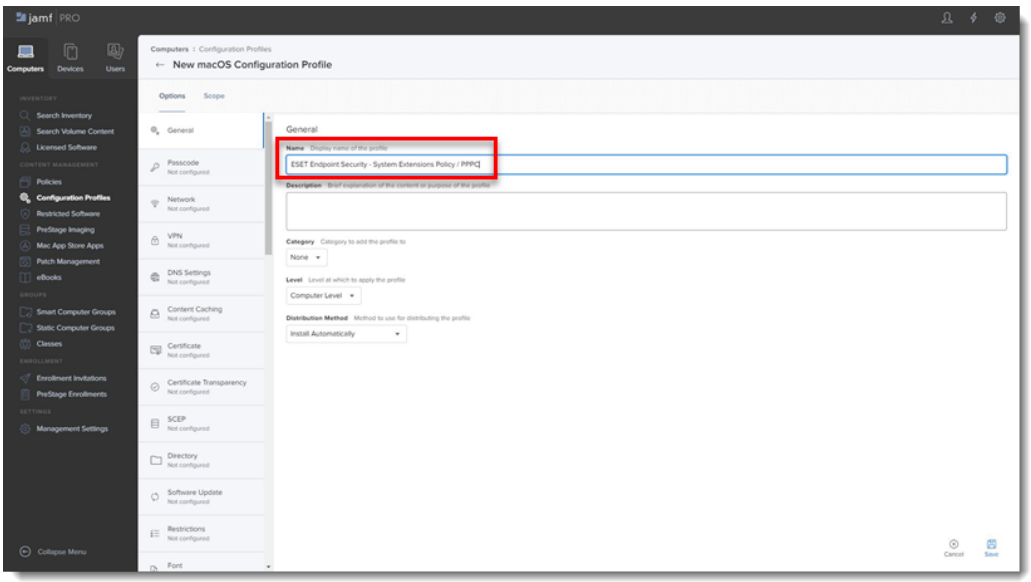
I. Configure System Extensions and Privacy Preference Policy Control (PPPC) profile

> **One configuration profile can use both settings**
> System Extensions and PPPC (Big Sur) are required to deploy to ESET Endpoint products, but if all machines are Big Sur, one configuration profile can be used for both System Extensions and PPPC settings.

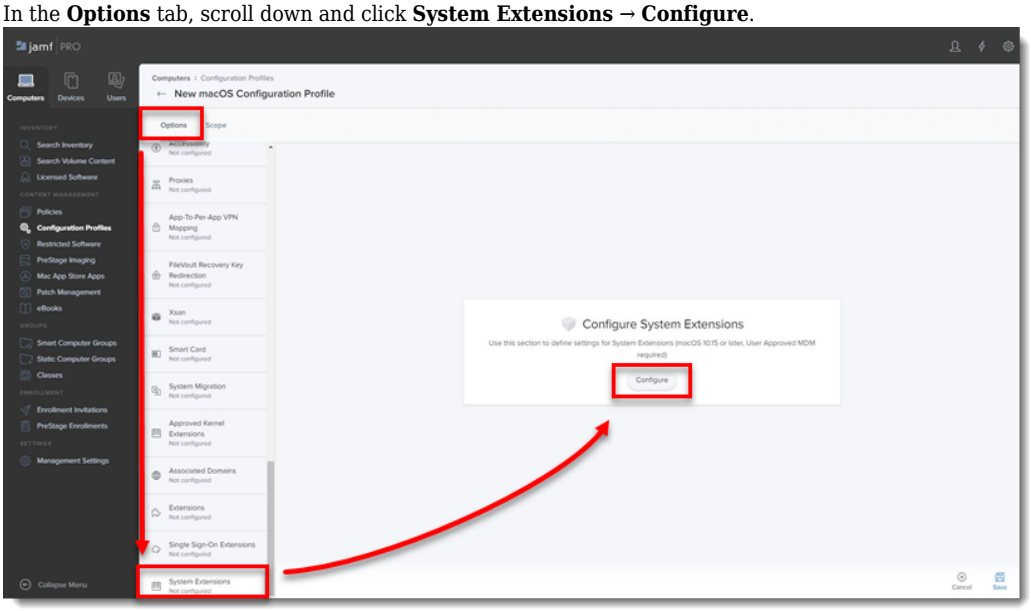
1. Click **Configuration Profiles** to set the approval for System Extensions and PPPC and then click **New** to add a new configuration profile (one configuration profile can contain both System Extension and PPPC settings).



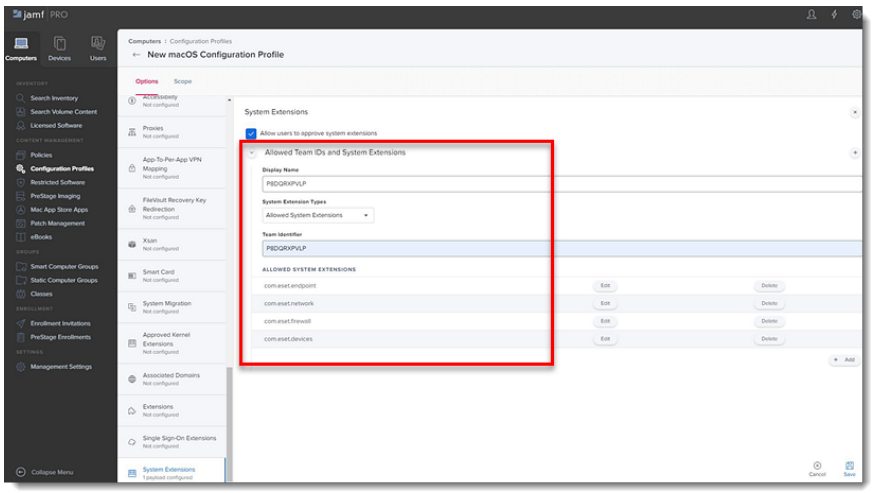
2. Type a **Name** for the profile.



3. In the **Options** tab, scroll down and click **System Extensions → Configure**.



4. In the **Allowed TEAM IDs and System Extensions** section, enter the following information:
    - **Display Name**: ESET SE [you can choose any name you want]
    - **System Extension Types**: Allowed System Extensions
    - **Team Identifier**: P8DQRXPVLP
    - **Allowed System Extensions**:
        - com.eset.endpoint
        - com.eset.network
        - com.eset.firewall
        - com.eset.devices



5. In the Options tab, scroll down and click **Privacy Preferences Policy Control → Configure**.



6. Add in the following information for your applicable ESET product:

> **Add both ESET Endpoint Antivirus and ESET Endpoint Security in the same PPPC setting**
> If you are deploying both ESET Endpoint Antivirus and ESET Endpoint Security, you can add them in the same PPPC setting by clicking the + sign (plus) at the top right and then adding the information for the additional product.

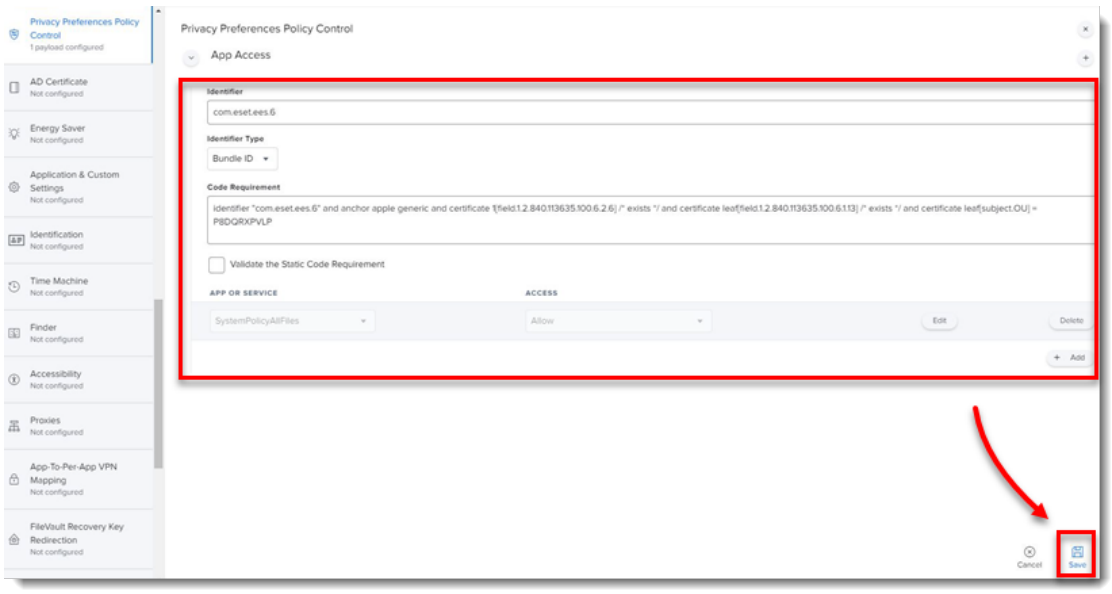
ESET Endpoint Antivirus:

- Identifier: com.eset.eea.6
- Identifier Type: Bundle ID
- Code Requirement: identifier "com.eset.eea.6" 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] = P8DQRXPVLP
- App or Service: SystemPolicyAllFiles
- Access: Allow

ESET Endpoint Security:

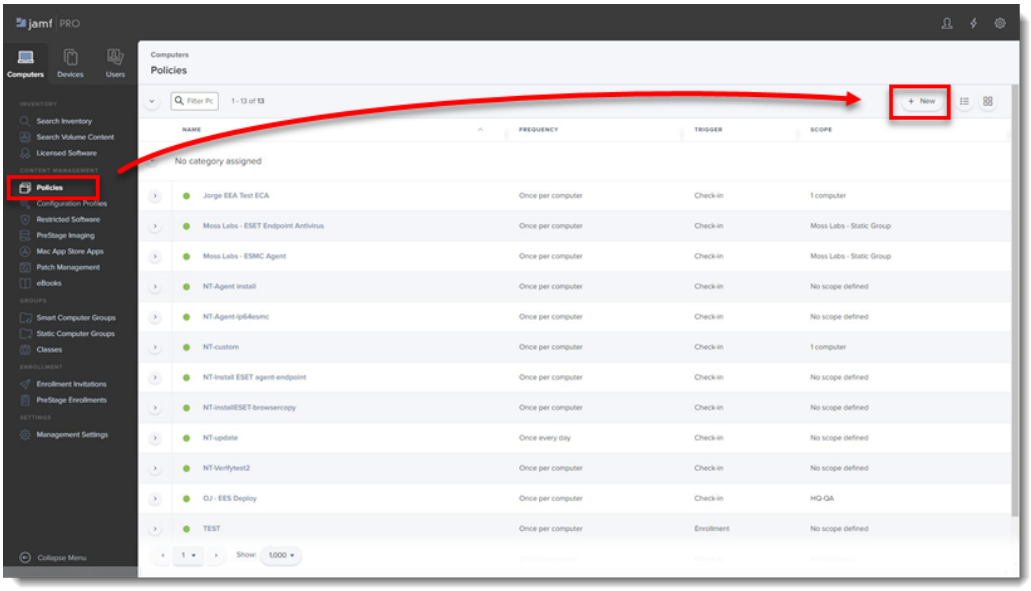
- Identifier: com.eset.ees.6
- Identifier Type: Bundle ID
- Code Requirement: identifier "com.eset.ees.6" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = P8DQRXPVLP
- App or Service: SystemPolicyAllFiles
- Access: Allow

7. Click **Save** to apply your changes.

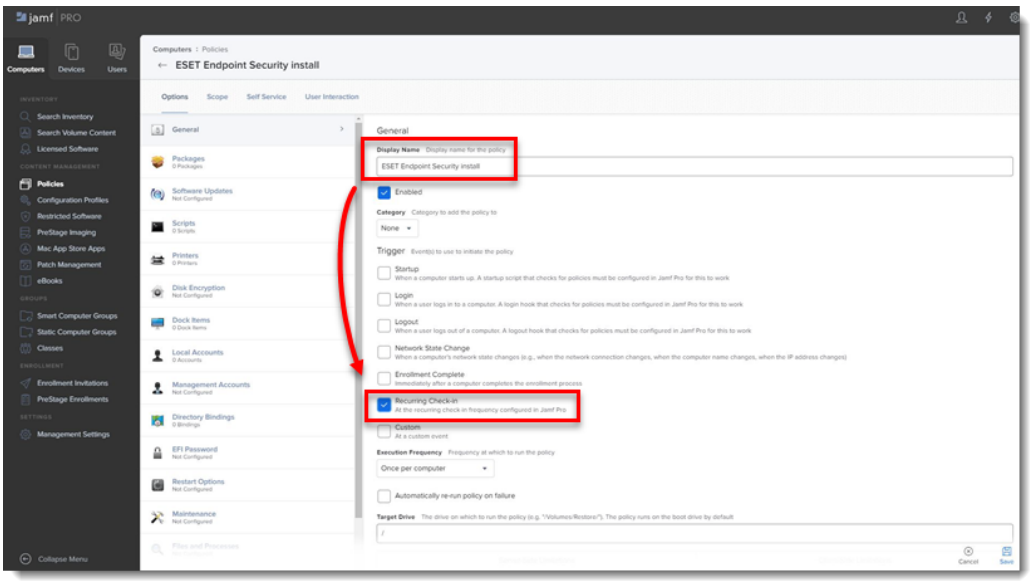


II. Create policies

1. Click **Policies** in the left menu and click **New**.



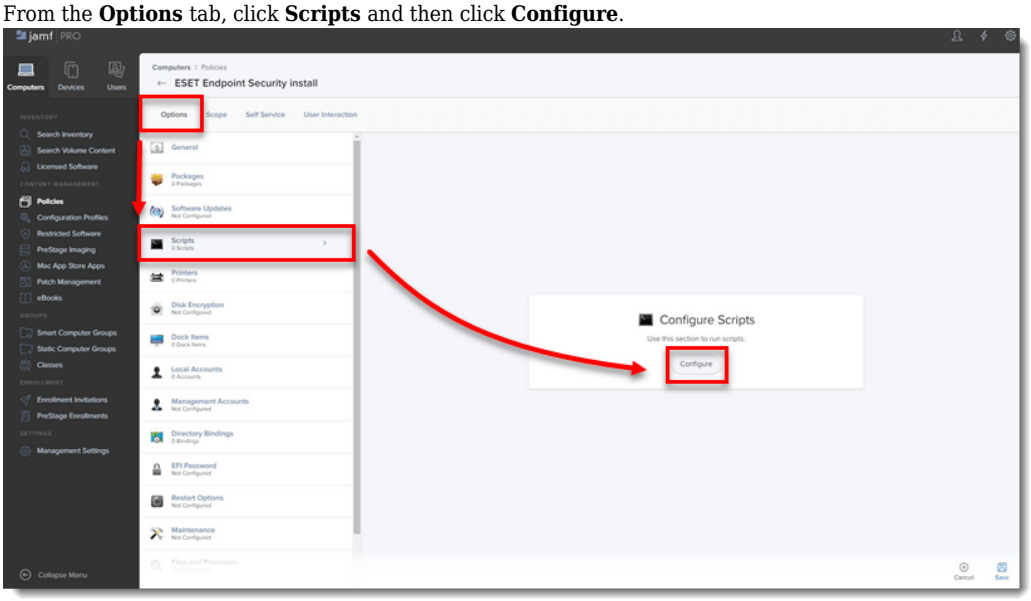
2. Type a **Display Name** for the policy, and in the **Trigger** section, select the **Recurring Check-in** check box.



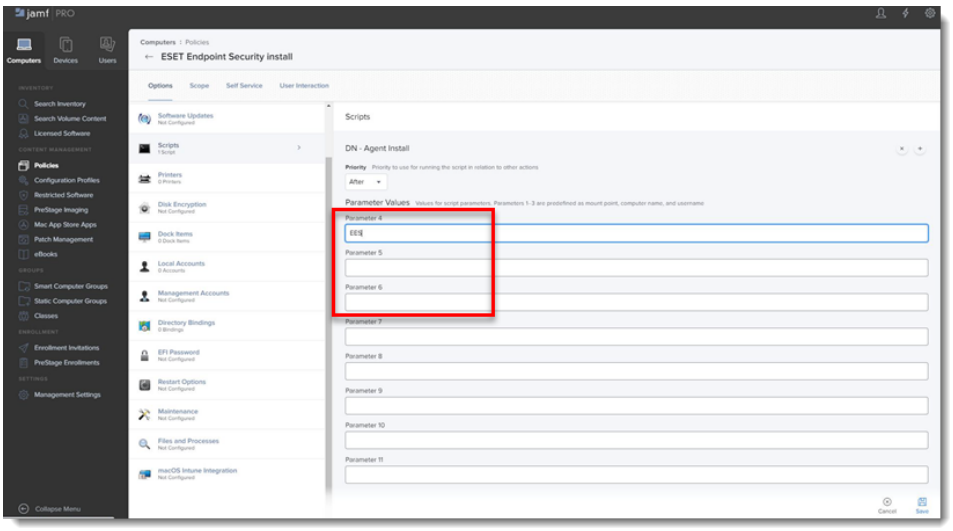
3. Download the following ESET Security product and ESET Management Agent installation scripts:
    - ESET Security product installation script: ESETavJamf.sh (right-click and select "Save link as")
    - ESET Management Agent installation script: Download the ESMCAgentInstaller.sh file from your ESET Security Management server, follow the instructions to Create Agent Live Installer.

4. After downloading the scripts, add the scripts to Jamf (this link takes you to the Jamf Pro Administrator's Guide).

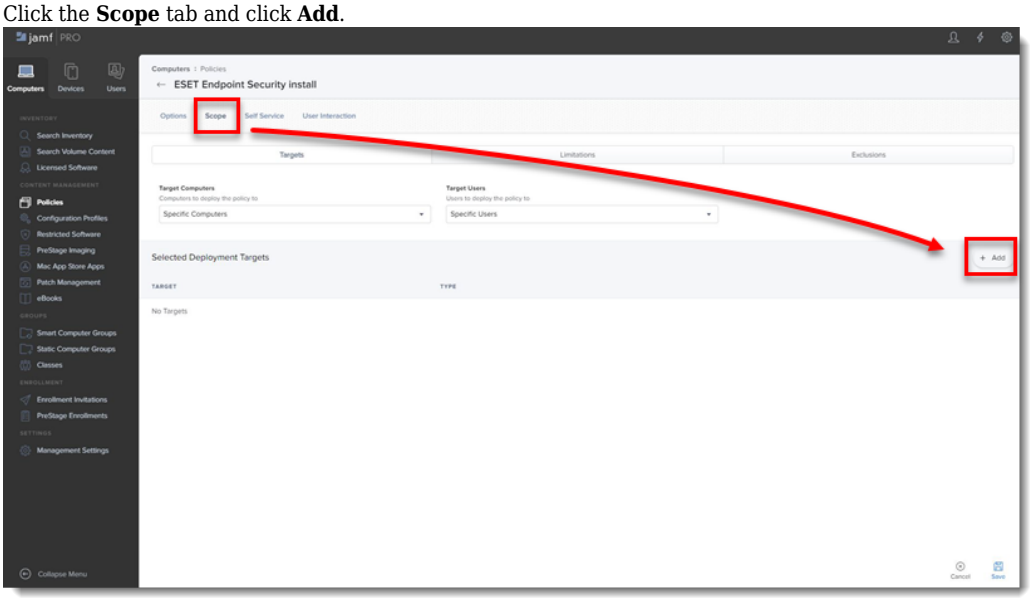
5. From the **Options** tab, click **Scripts** and then click **Configure**.



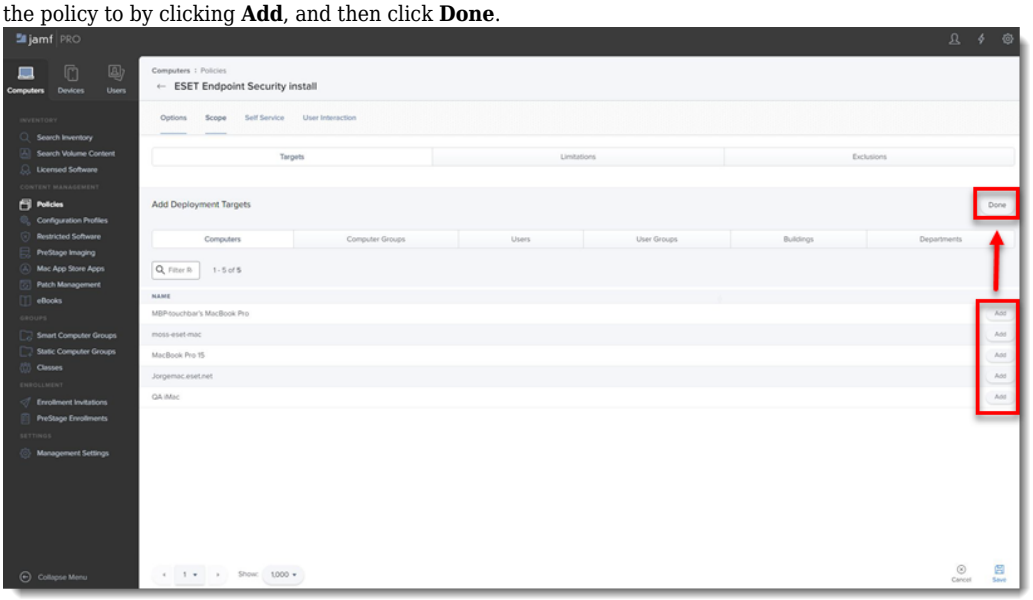
6. Click **Add** to select the scripts to add to the policy.
7. Add the following Parameter Values for the Endpoint script:
    1. Parameter 4 (Required): Type 'EES' (if you use ESET Endpoint Security) or 'EEA' (if you use ESET Endpoint Antivirus)
    2. Parameter 5 (Optional): License Key or Security Admin in the format PID:SecurityAdmin:Password, for example — 123-ABC-456:user=security.admin@email.com:pass=SecurityAdminPass
    3. Parameter 6 (Optional): Specify HTTP Proxy in the format http://10.0.0.100:3128



8. Click the **Scope** tab and click **Add**.



9. In the **Add Deployment Targets** section, select the computers (or Computer Groups) you want to apply the policy to by clicking **Add**, and then click **Done**.



10. Click **Save** to apply your changes.

Add Proxy Configurations notification

Users may receive the following notification: '**"ESET Endpoint Security"** or **"ESET Endpoint Antivirus" Would Like to Add Proxy Configurations**'. If you receive this notification, click **Allow**.

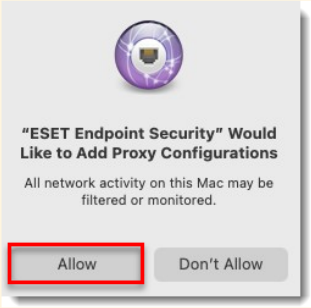


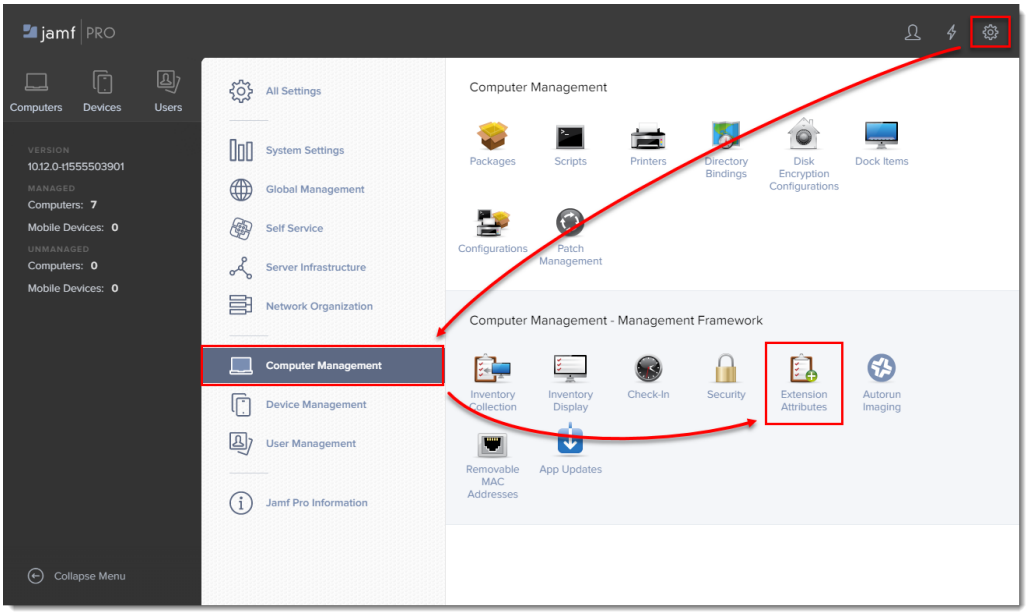
Figure 2-7

III. Additional options

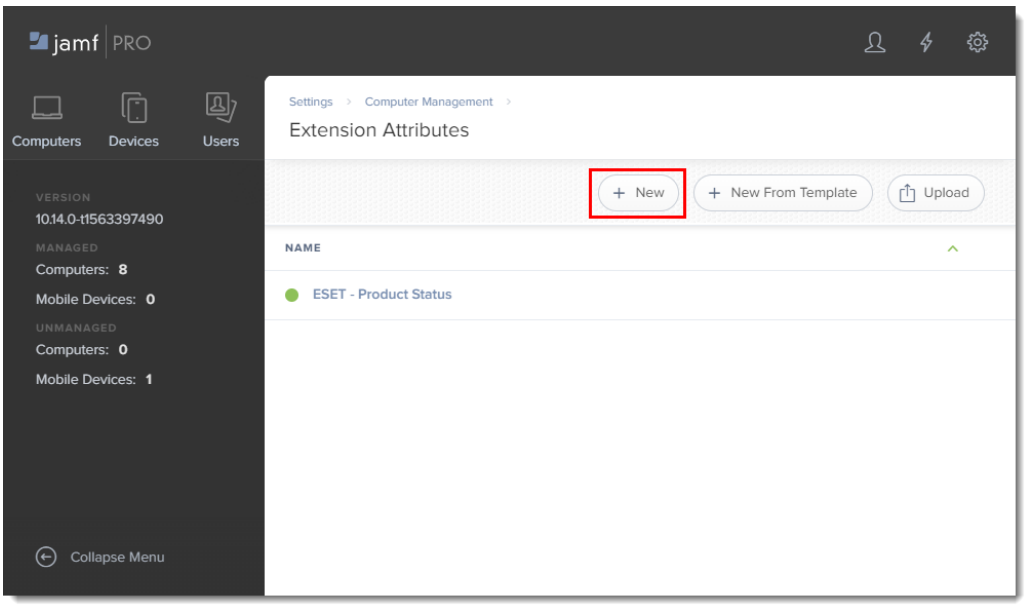
- Verify you can manage the ESET Endpoint using ESET Security Management Center: In the ESMC **Computers** section you will see the Jamf endpoint in the **All** Group.
- If you did not enter the License Key or Security Admin during the install scripts, you can activate using ESET Security Management Center.
- Extension Attributes: Extension Attributes show information regarding ESET products in the **Computer details → Search Inventory → General** section.

Follow the instructions below to add the Extension Attribute:

1. In the main window, click the **All Settings** gear icon → **Computer Management** → **Extension attributes**.



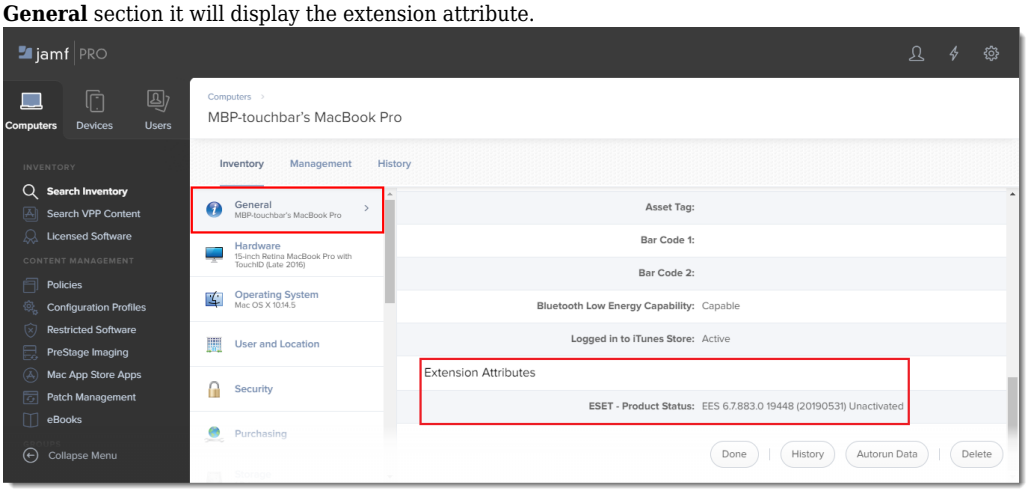
2. Click **New** to create a new extension attribute.



3. Type a name for the extension attribute, change the input type to **Script** and then paste the ESETstatusEA.sh (right-click and select "Save link as") script into the Shell field and click **Save**.



4. The extension attribute will be automatically set to all computer groups. Click a computer and in the **General** section it will display the extension attribute.

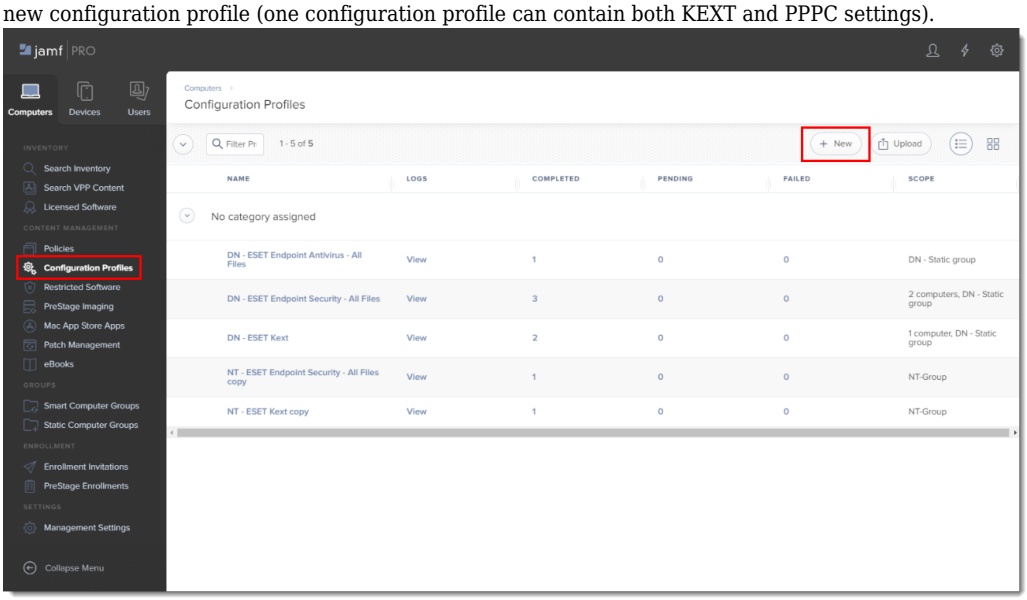


Jamf Pro deployment for ESET Endpoint for macOS (earlier versions).

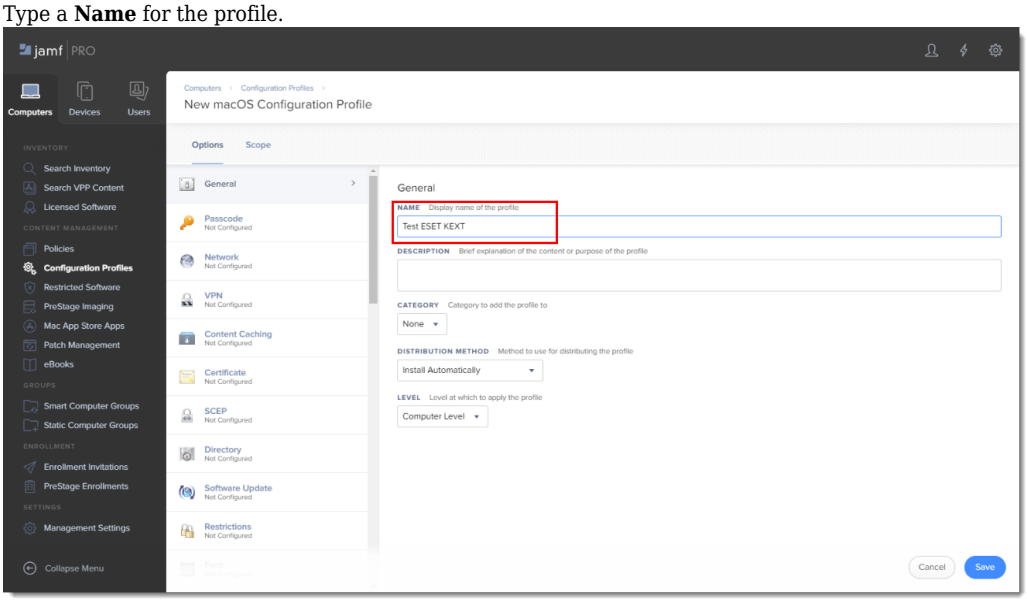
I. Configure KEXT and PPPC profile

> **One configuration profile can contain both settings**
> KEXT (High Sierra 10.13+) and PPPC (Mojave 10.14+) or one configuration profile can contain both KEXT and PPPC settings if all machines are Mojave.

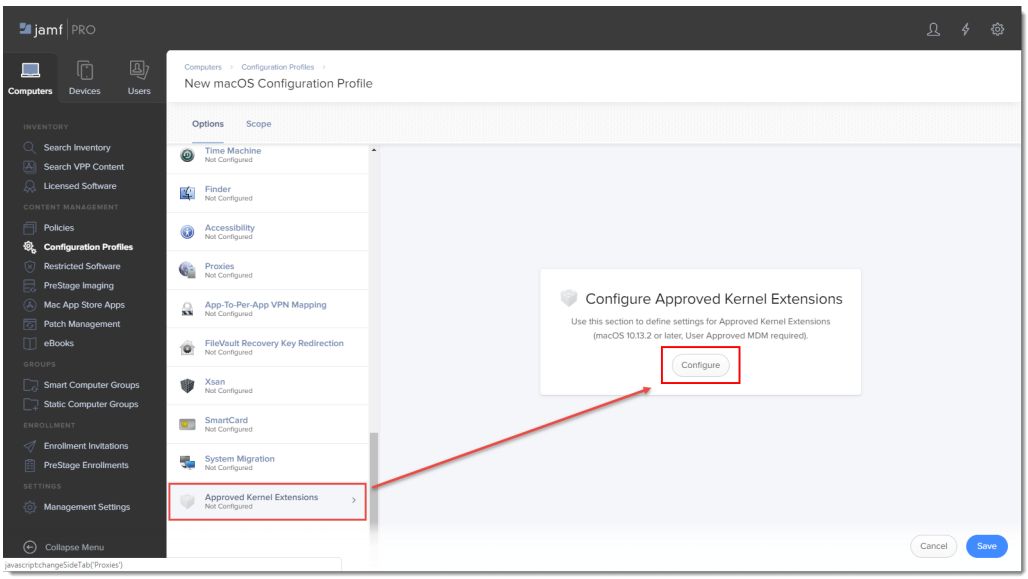
1. Click **Configuration Profiles** to set the approval for the KEXT and PPPC and then click **New** to add a new configuration profile (one configuration profile can contain both KEXT and PPPC settings).



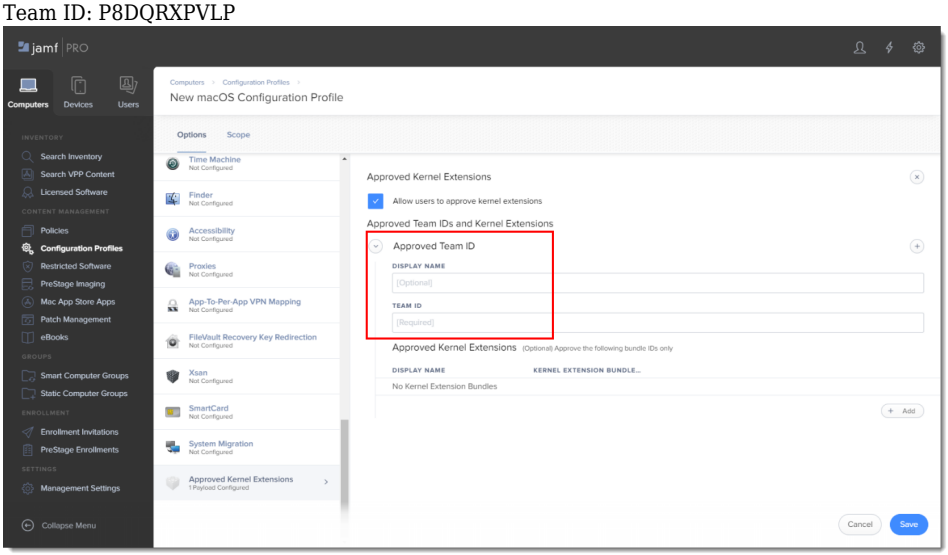
2. Type a **Name** for the profile.



3. In the **Options** tab, scroll down and click **Approved Kernel Extensions → Configure**.



4. In the **Approved TEAM ID** section, enter the following information:
    1. Display Name: ESET KEXT [you can choose any name you want]
    2. Team ID: P8DQRXPVLP



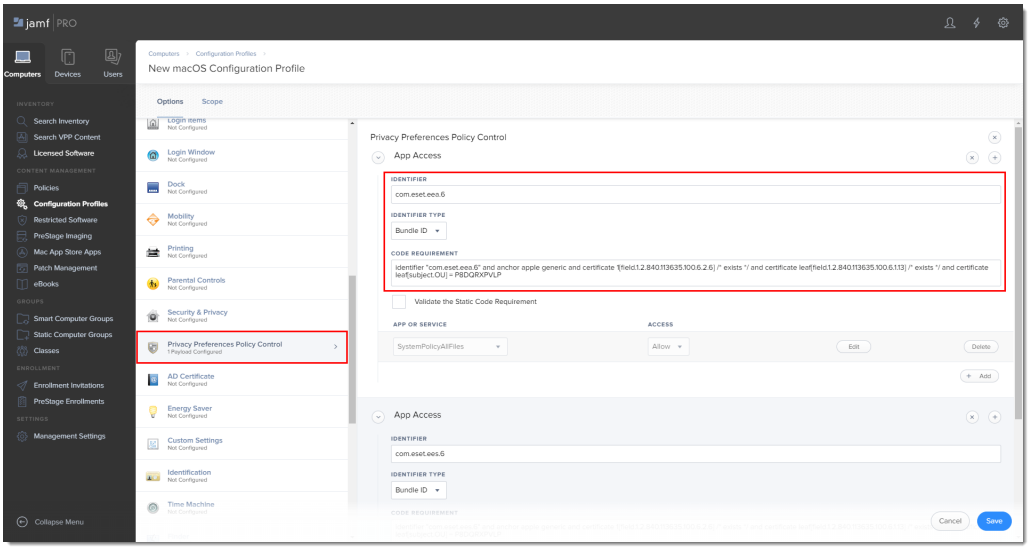
5. In the **Options** tab, scroll to **Privacy Preferences Policy Control** and add in the following information for your applicable ESET product:

> **Add both ESET Endpoint Antivirus and ESET Endpoint Security in the same PPPC setting**
> If you are deploying both ESET Endpoint Antivirus and ESET Endpoint Security, you can add them in the same PPPC setting by clicking the + sign (plus) at the top right and then adding the information for the additional product.

ESET Endpoint Antivirus:
Identifier: com.eset.eea.6
Identifier type: Bundle ID
Code Requirement: identifier "com.eset.eea.6" 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] = P8DQRXPVLP
App or Service: SystemPolicyAllFiles
Access: Allow

ESET Endpoint Security:
Identifier: com.eset.ees.6
Identifier type: Bundle ID
Code Requirement: identifier "com.eset.ees.6" 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] = P8DQRXPVLP
App or Service: SystemPolicyAllFiles

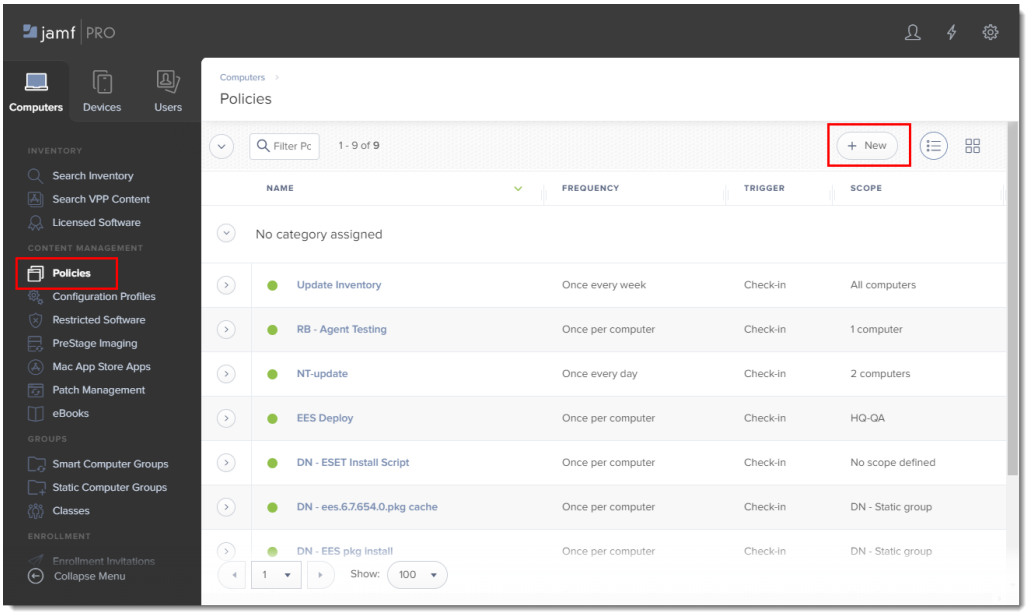
Access: Allow



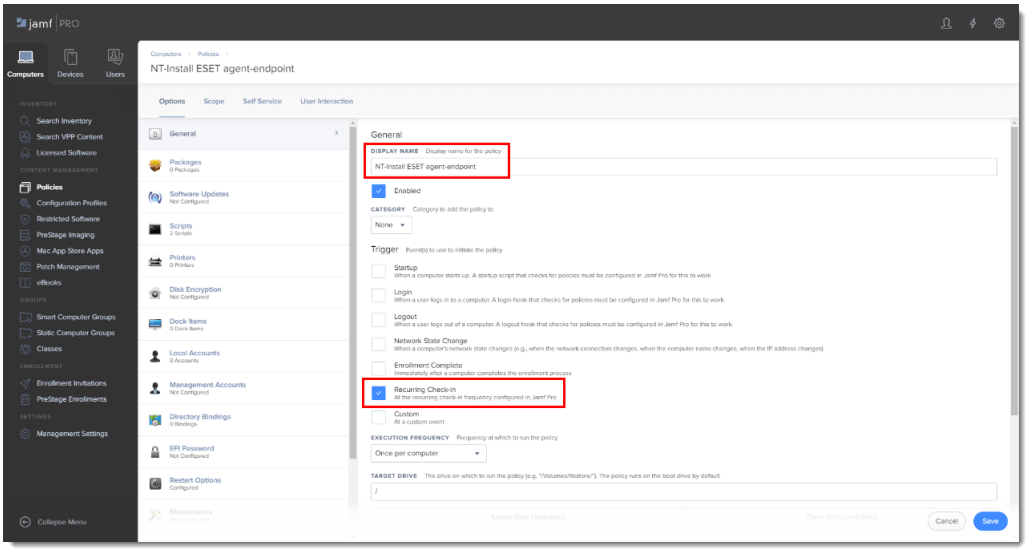
6. Click **Save** to apply your changes.

II. Create policies

1. Click **Policies** in the left menu and click **New**.



2. Type a name for the policy and in the **Trigger** section, select **Recurring Check-in**.

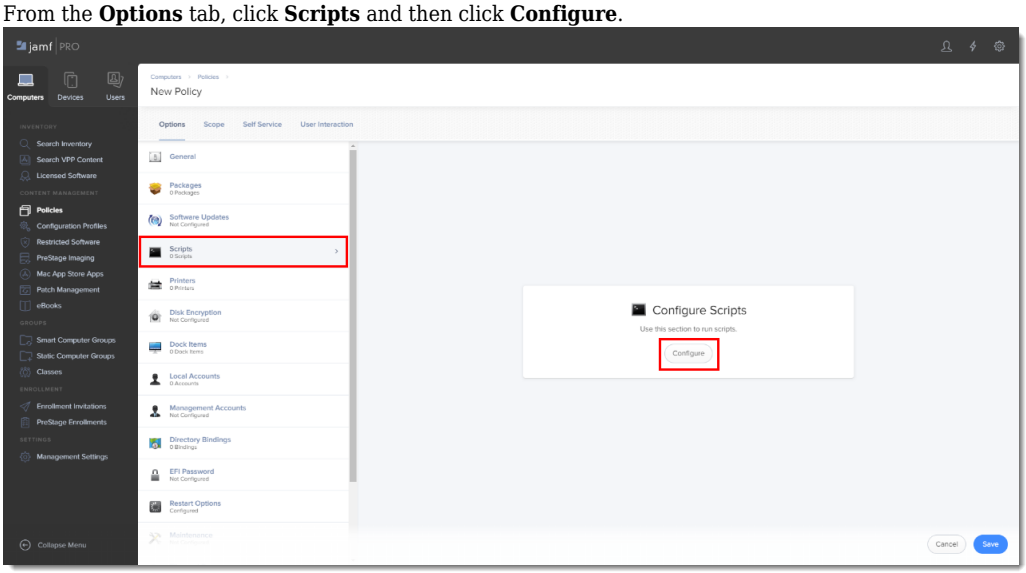


3. Download the following ESET Security product and ESET Management Agent installation scripts:

    - ESET Security product installation script: ESETavJamf.sh (right-click and select "Save link as")
    - ESET Management Agent installation script: Download the ESMCAgentInstaller.sh file from your ESET Security Management server, follow the instructions to Create Agent Live Installer.

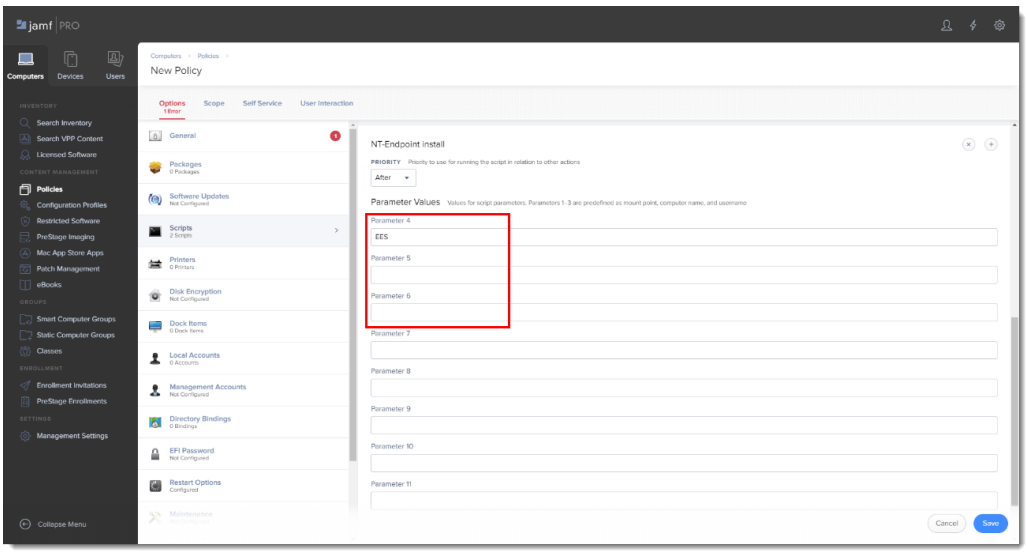
4. After downloading the scripts, add the scripts to Jamf (this link takes you to the Jamf Pro Administrator's Guide).

5. From the **Options** tab, click **Scripts** and then click **Configure**.

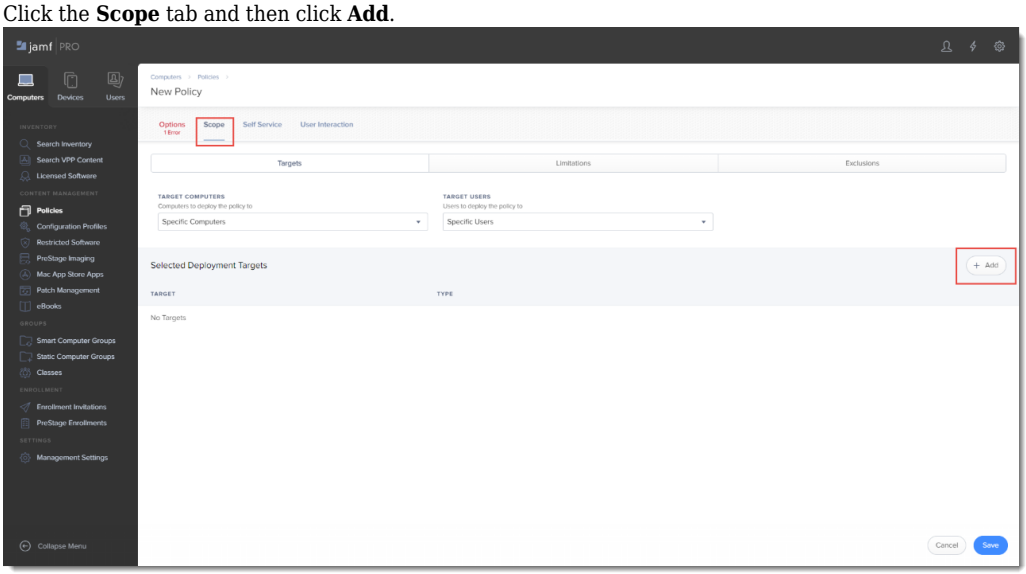


6. Click **Add** to select the scripts to add to the policy.
7. Add the following Parameter Values for the Endpoint script:

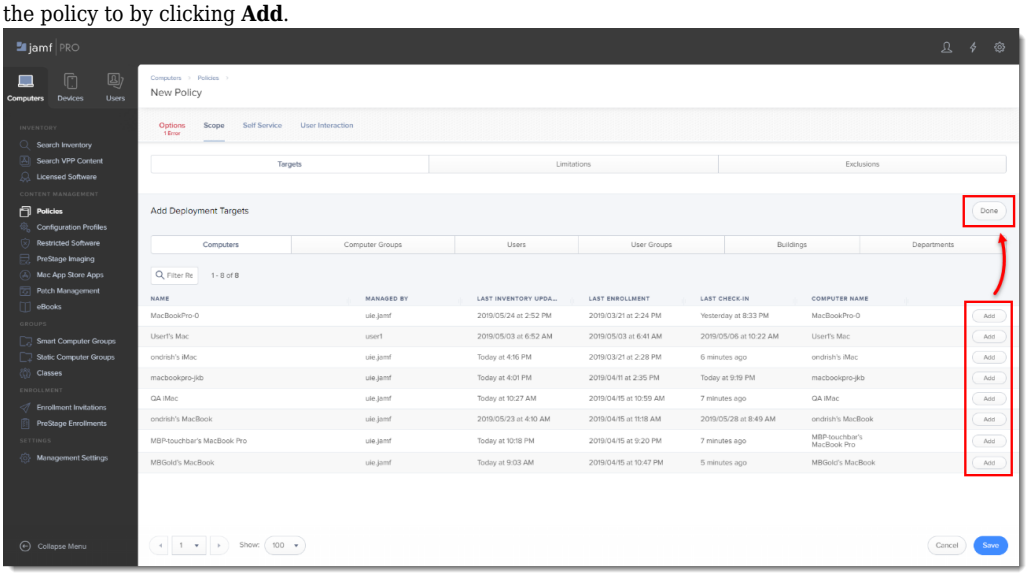
    Parameter 4 (Required): 'EES' (if you use ESET Endpoint Security) or 'EEA' (if you use ESET Endpoint Antivirus)Parameter 5 (Optional): License Key or Security Admin in the format PID:SecurityAdmin:Password, for example — 123-ABC-456:user=security.admin@email.com:pass=SecurityAdminPass
    Parameter 6 (Optional): Specify HTTP Proxy in the format http://10.0.0.100:3128



8. Click the **Scope** tab and then click **Add**.



9. In the **Add Deployment Targets** section, select the computers (or Computer Groups) you want to apply the policy to by clicking **Add**.



10. Click **Done** when finished and then click **Save** to apply your changes.

Related Content

- Security baseline policy voor | ESET Protect Cloud
- Multifactorauthenticatie toepassen en eerste client uitrollen in | ESET Protect Cloud
- Security voor de client nu in de cloud! | ESET Protect Cloud