Cybersecurity
Progress. Protected.

[Kennisbank](#) > [Endpoint Solutions](#) > [ESET Endpoint Security](#) > [Deploy ESET Endpoint products for macOS using Jamf Pro](#)

Deploy ESET Endpoint products for macOS using Jamf Pro

Steef | ESET Nederland - 2021-02-23 - [Reacties (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

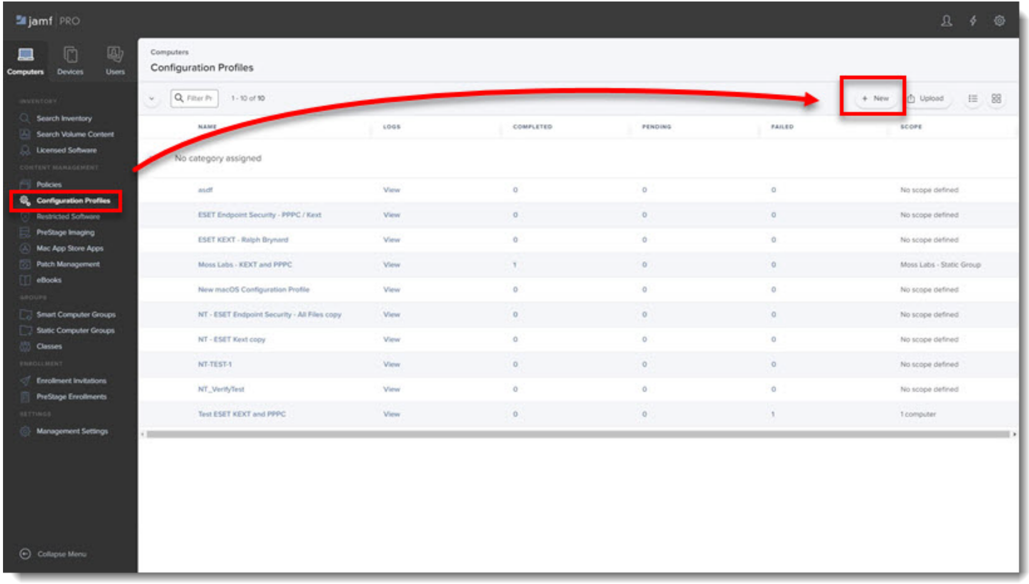
Follow the instructions below to deploy ESET Endpoint for macOS Big Sur using Jamf Pro to manage using ESET Security Management Center/ESET PROTECT.

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).



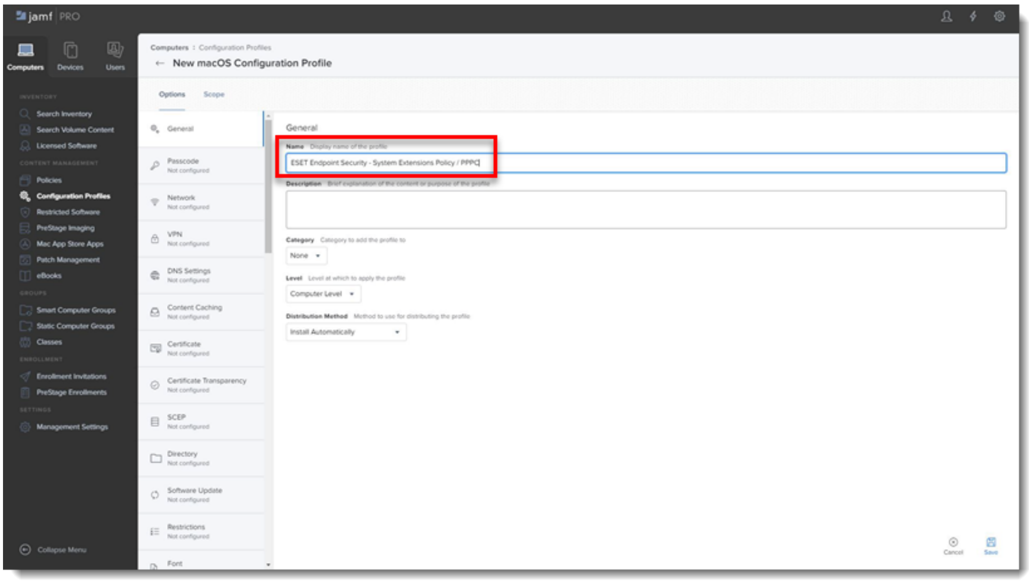
Computers

Configuration Profiles

No category assigned

NAME	LOGS	COMPLETED	PENDING	FAILED	SCOPE
asdf	View	0	0	0	No scope defined
ESET Endpoint Security - PPPC / Kext	View	0	0	0	No scope defined
ESET KEXT - Ralph Brynard	View	0	0	0	No scope defined
Moss Labs - KEXT and PPPC	View	1	0	0	Moss Labs - Static Group
New macOS Configuration Profile	View	0	0	0	No scope defined
NT - ESET Endpoint Security - All Files copy	View	0	0	0	No scope defined
NT - ESET Kext copy	View	0	0	0	No scope defined
NT-TEST-1	View	0	0	0	No scope defined
NT_VerifyTest	View	0	0	0	No scope defined
Test ESET KEXT and PPPC	View	0	0	1	1 computer

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



General

Name Display name of the profile

ESET Endpoint Security - System Extensions Policy / PPPC

Description Brief explanation of the content or purpose of the profile

Category Category to add the profile to

None

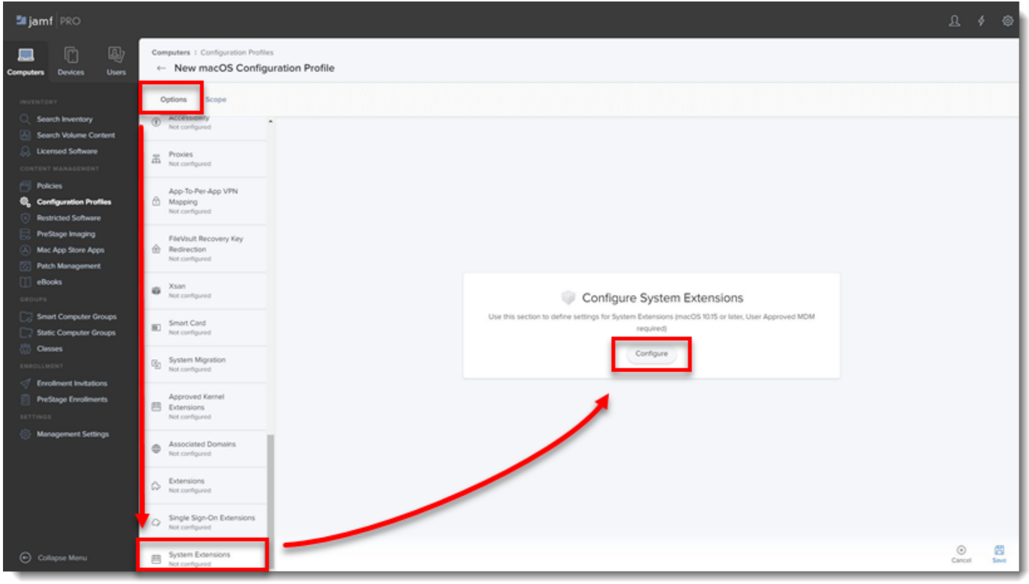
Level Level at which to apply the profile

Computer Level

Distribution Method Method to use for distributing the profile

Install Automatically

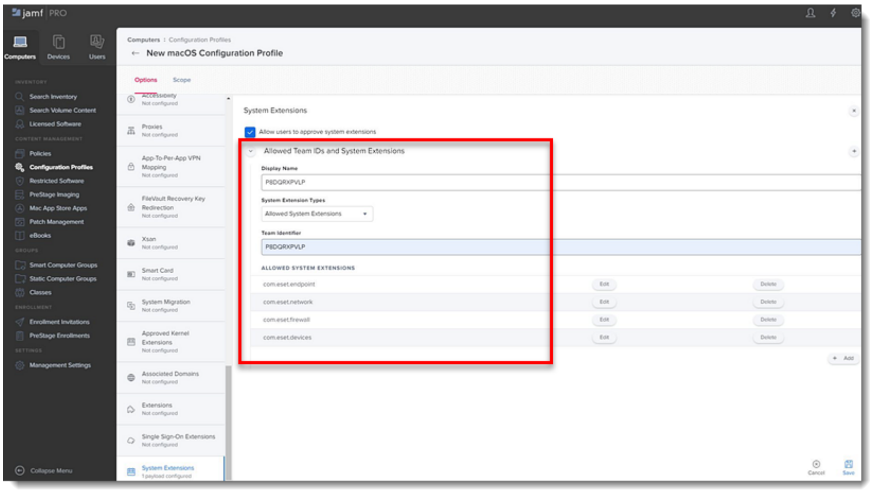
3. In the **Options** tab, scroll down and click **System Extensions** → **Configure**.



Configure System Extensions

Use this section to define settings for System Extensions (macOS 10.15 or later, User Approved MDM required)

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



System Extensions

☑ Allow users to approve system extensions

Allowed Team IDs and System Extensions

Display Name: P8DQRXPVLP

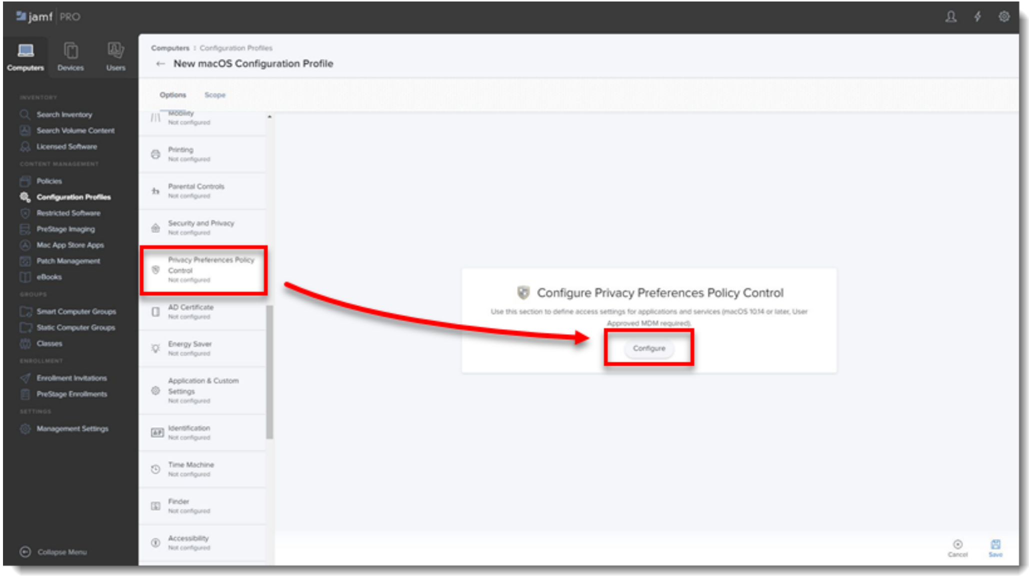
System Extension Types: Allowed System Extensions

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**.



Configure Privacy Preferences Policy Control

Use this section to define access settings for applications and services (macOS 10.14 or later, User Approved MDM required)

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.

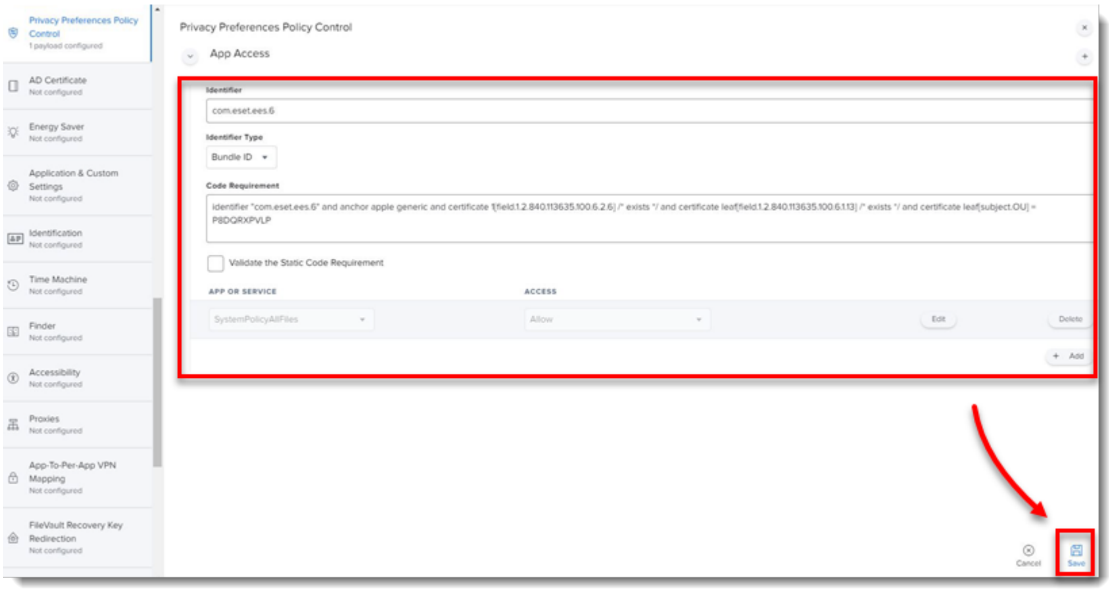
ESET Endpoint Antivirus:

- 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.



Privacy Preferences Policy Control

App Access

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
```

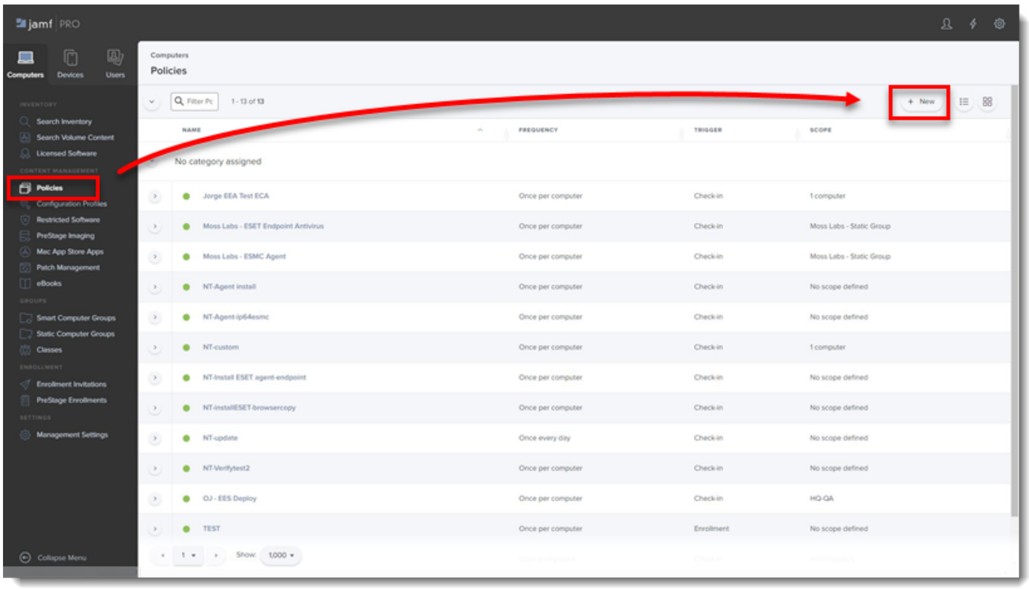
□ Validate the Static Code Requirement

APP OR SERVICE	ACCESS		
SystemPolicyAllFiles	Allow	Edit	Delete

+ Add

II. Create policies

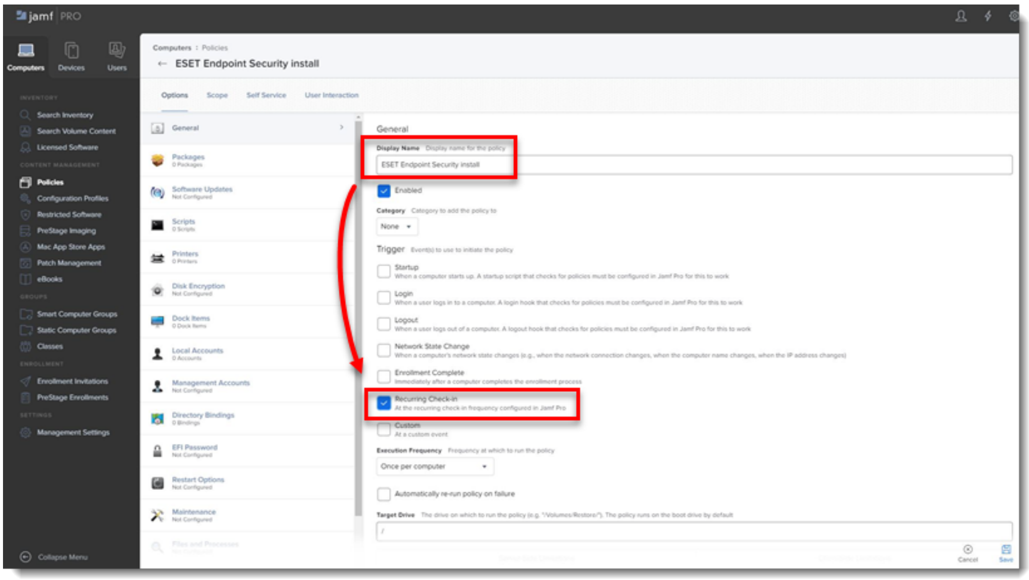
1. Click **Policies** in the left menu and click **New**.



No category assigned

NAME	FREQUENCY	TRIGGER	SCOPE
Jorge EEA Test ECA	Once per computer	Check-in	1 computer
Moss Labs - ESET Endpoint Antivirus	Once per computer	Check-in	Moss Labs - Static Group
Moss Labs - ESMC Agent	Once per computer	Check-in	Moss Labs - Static Group
NT-Agent install	Once per computer	Check-in	No scope defined
NT-Agent-ip64esmc	Once per computer	Check-in	No scope defined
NT-custom	Once per computer	Check-in	1 computer
NT-Install ESET agent-endpoint	Once per computer	Check-in	No scope defined
NT-installESET-browsercopy	Once per computer	Check-in	No scope defined
NT-update	Once every day	Check-in	No scope defined
NT-Verifytest2	Once per computer	Check-in	No scope defined
OJ - EES Deploy	Once per computer	Check-in	HQ-QA
TEST	Once per computer	Enrollment	No scope defined

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



ESET Endpoint Security install

General

Display Name Display name for the policy

ESET Endpoint Security install

☑ Enabled

Category Category to add the policy to

None

Trigger Event(s) to use to initiate the policy

□ Startup
When a computer starts up. A startup script that checks for policies must be configured in Jamf Pro for this to work

□ Login
When a user logs in to a computer. A login hook that checks for policies must be configured in Jamf Pro for this to work

□ Logout
When a user logs out of a computer. A logout hook that checks for policies must be configured in Jamf Pro for this to work

□ Network State Change
When a computer's network state changes (e.g., when the network connection changes, when the computer name changes, when the IP address changes)

□ Enrollment Complete
Immediately after a computer completes the enrollment process

☑ Recurring Check-in
At the recurring check-in frequency configured in Jamf Pro

□ Custom
At a custom event

Execution Frequency Frequency at which to run the policy

Once per computer

□ Automatically re-run policy on failure

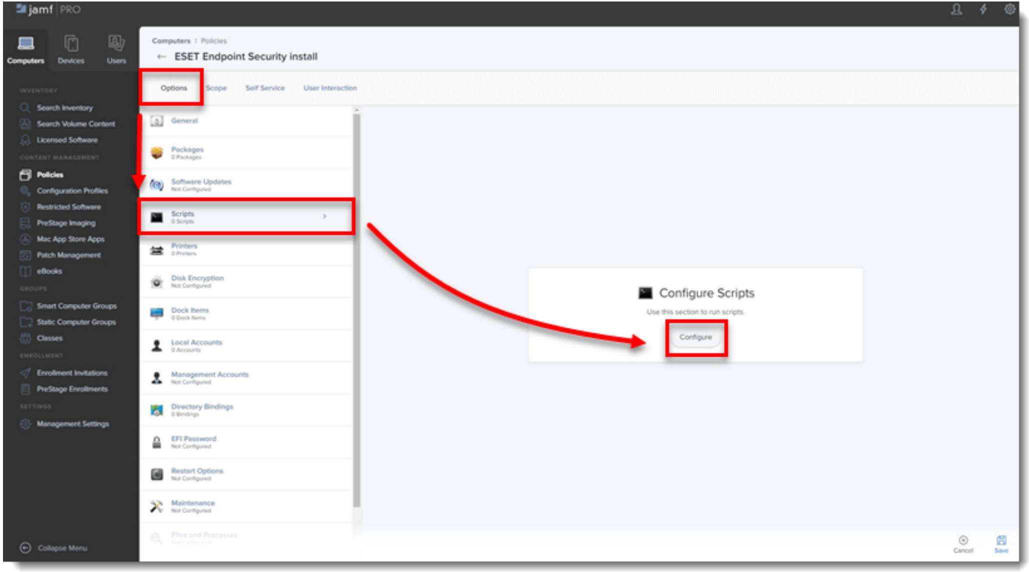
Target Drive The drive on which to run the policy (e.g. "/Volumes/Restore/"). The policy runs on the boot drive by default

/

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**.

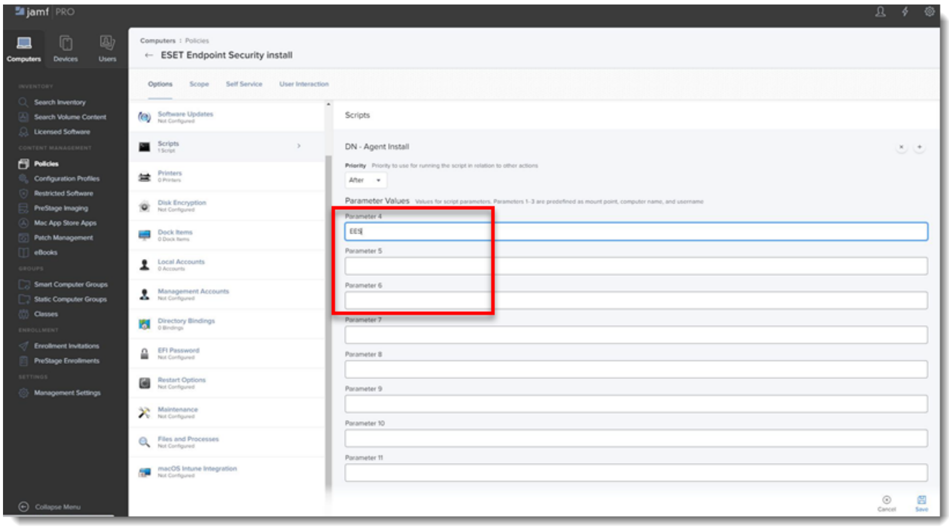


ESET Endpoint Security install

Configure Scripts

Use this section to run scripts.

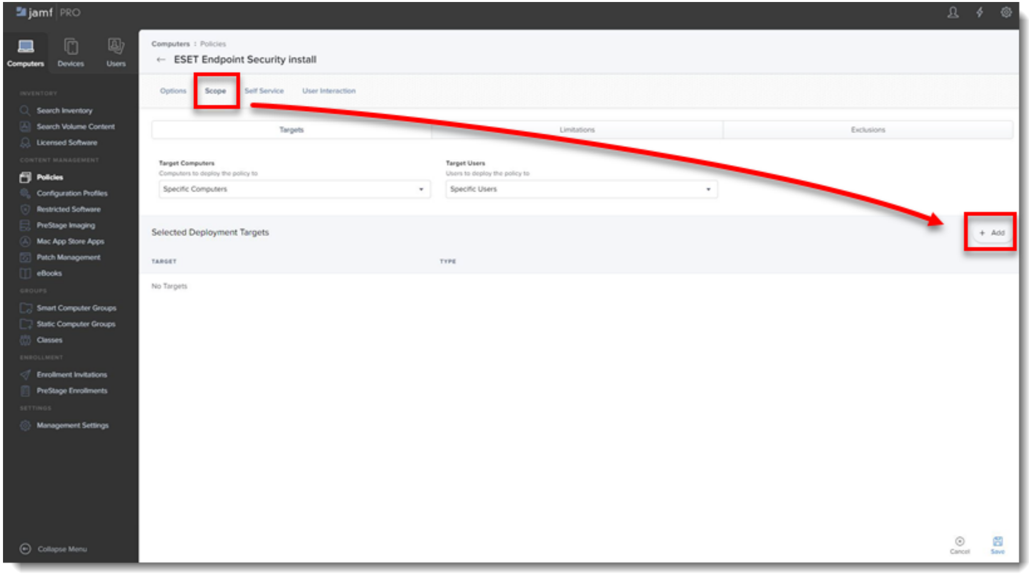
6. Click **Add** to select the scripts to add to the policy.
7. Add the following Parameter Values for the Endpoint script:
    1. Parameter 4 (Required): Type 'EES' (if you use ESET Endpoint Security) or 'EEA' (if you use ESET Endpoint Antivirus)
    2. Parameter 5 (Optional): License Key or Security 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



Priority: After

Parameter 4: EES

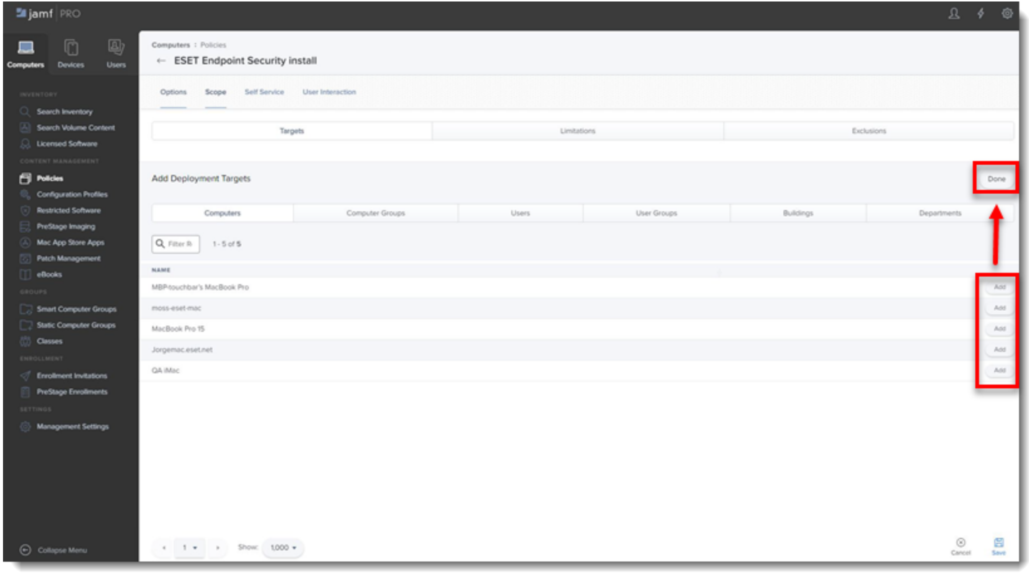
8. Click the **Scope** tab and click **Add**.



Target Computers: Specific Computers

Target Users: Specific Users

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**.

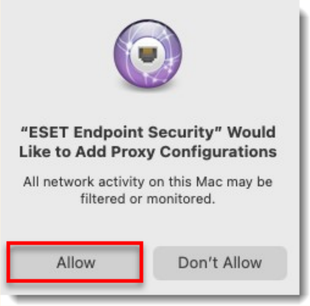


NAME	
MBP-touchbar's MacBook Pro	Add
moss-eset-mac	Add
MacBook Pro 15	Add
Jorgemac.eset.net	Add
QA iMac	Add

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**.



"ESET Endpoint Security" Would Like to Add Proxy Configurations

All network activity on this Mac may be filtered or monitored.

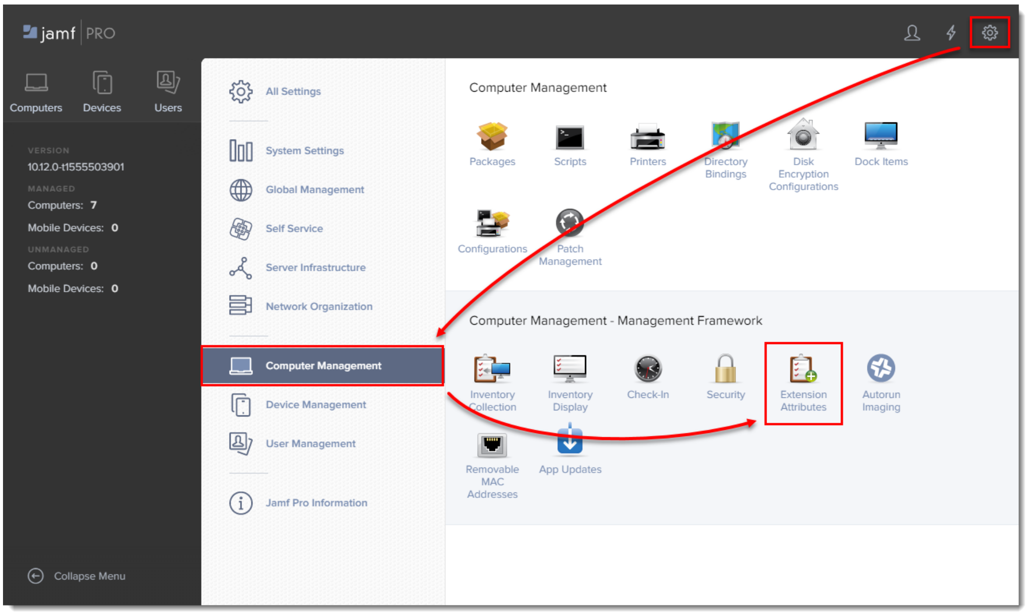
Figure 2-7

III. Additional options

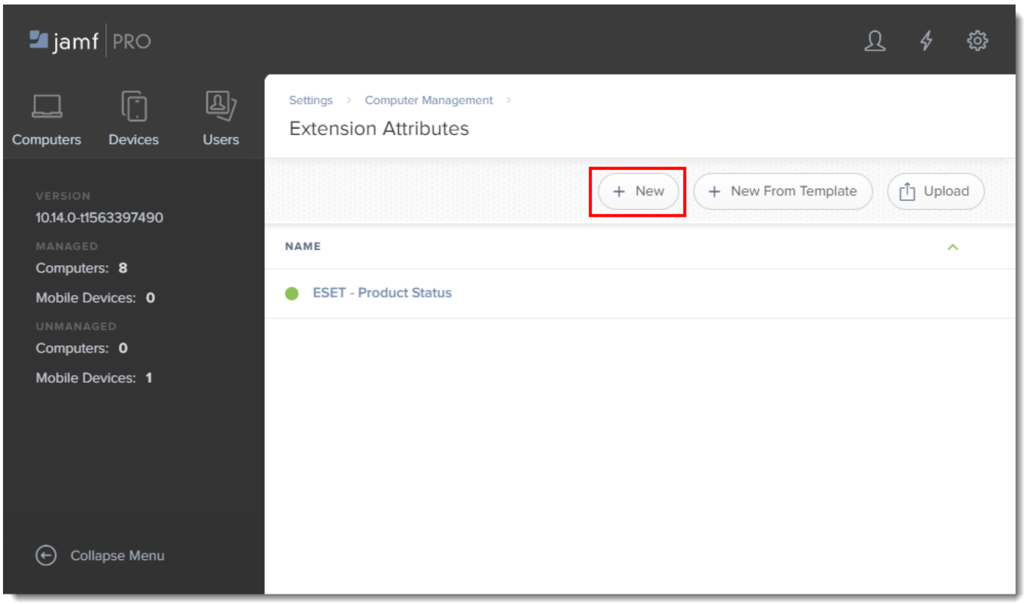
- Verify you can manage the ESET Endpoint using ESET Security Management Center: In the ESMC **Computers** section you will see the Jamf endpoint in the **All** Group.
- If you did not enter the License Key or Security Admin during the install scripts, you can activate using ESET Security Management 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**.

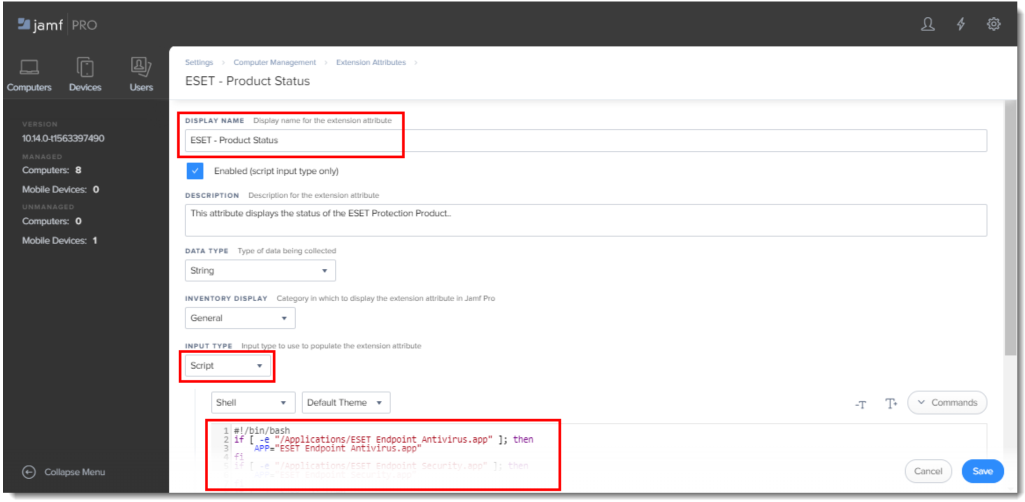


2. Click **New** to create a new extension attribute.



VERSION
10.14.0-t1563397490
MANAGED
Computers: 8
Mobile Devices: 0
UNMANAGED
Computers: 0
Mobile Devices: 1

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**.



DISPLAY NAME Display name for the extension attribute
ESET - Product Status

☑ Enabled (script input type only)

DESCRIPTION Description for the extension attribute
This attribute displays the status of the ESET Protection Product..

DATA TYPE Type of data being collected
String

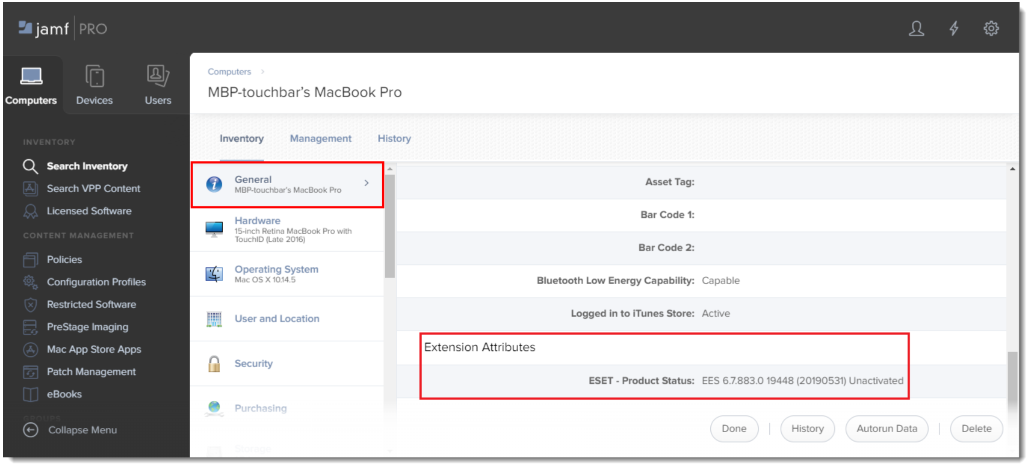
INVENTORY DISPLAY Category in which to display the extension attribute in Jamf Pro
General

INPUT TYPE Input type to use to populate the extension attribute
Script

Shell
Default Theme

```
#!/bin/bash
if [ -e "/Applications/ESET Endpoint Antivirus.app" ]; then
    APP="ESET Endpoint Antivirus.app"
fi
if [ -e "/Applications/ESET Endpoint Security.app" ]; then
    APP="ESET Endpoint Security.app"
```

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.



Asset Tag:
Bar Code 1:
Bar Code 2:
Bluetooth Low Energy Capability: Capable
Logged in to iTunes Store: Active

Extension Attributes

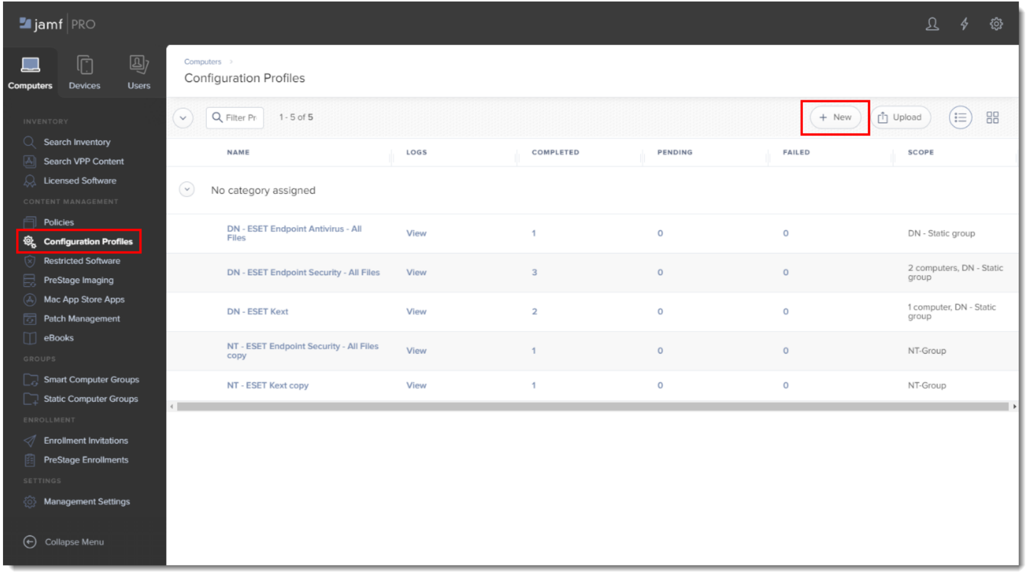
ESET - Product Status: EES 6.7.883.0 19448 (20190531) Unactivated

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).

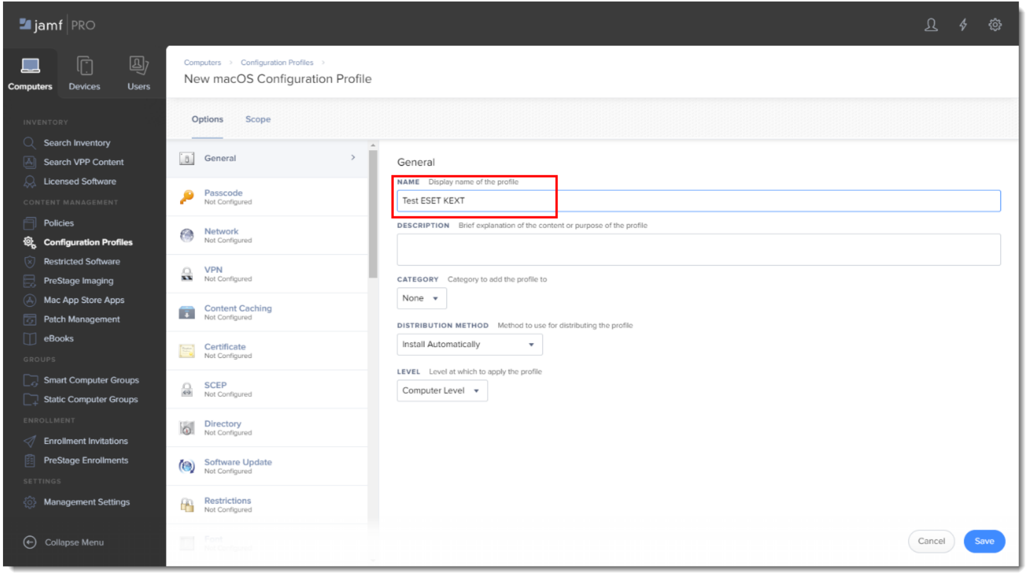


Configuration Profiles

No category assigned

NAME	LOGS	COMPLETED	PENDING	FAILED	SCOPE
DN - ESET Endpoint Antivirus - All Files	View	1	0	0	DN - Static group
DN - ESET Endpoint Security - All Files	View	3	0	0	2 computers, DN - Static group
DN - ESET Kext	View	2	0	0	1 computer, DN - Static group
NT - ESET Endpoint Security - All Files copy	View	1	0	0	NT-Group
NT - ESET Kext copy	View	1	0	0	NT-Group

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



New macOS Configuration Profile

General

NAME Display name of the profile: Test ESET KEXT

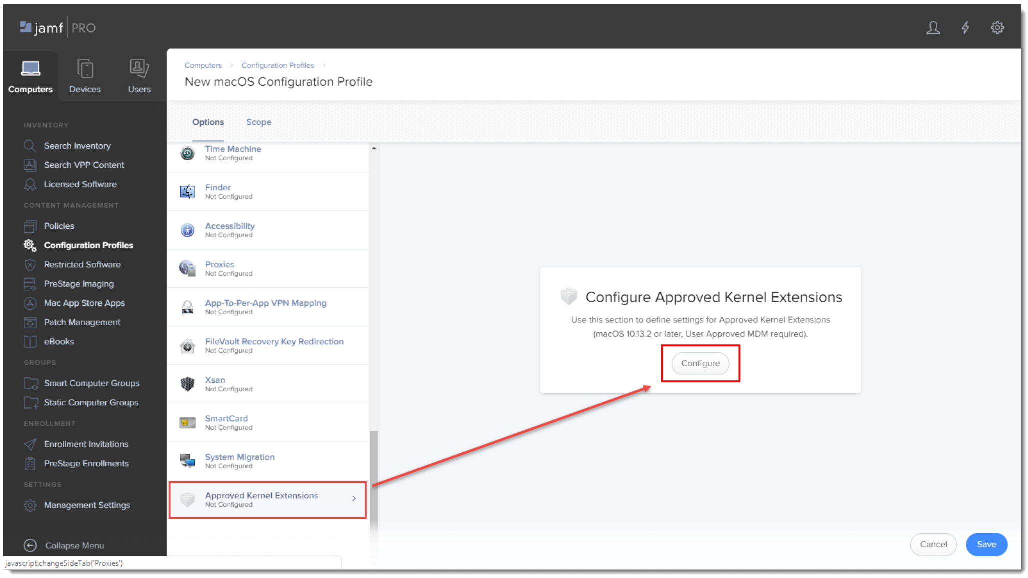
DESCRIPTION Brief explanation of the content or purpose of the profile:

CATEGORY Category to add the profile to: None

DISTRIBUTION METHOD Method to use for distributing the profile: Install Automatically

LEVEL Level at which to apply the profile: Computer Level

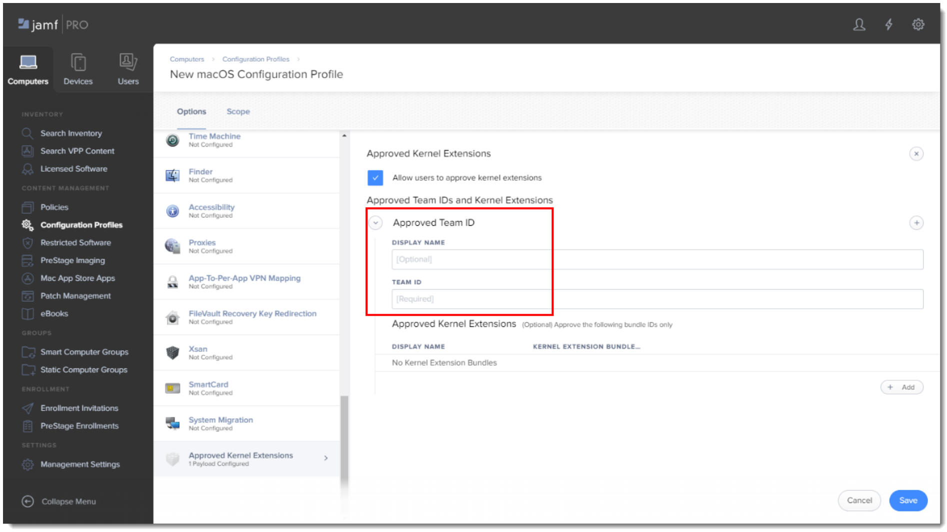
3. In the **Options** tab, scroll down and click **Approved Kernel Extensions → Configure**.



Configure Approved Kernel Extensions

Use this section to define settings for Approved Kernel Extensions (macOS 10.13.2 or later, User Approved MDM required).

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


jamf | PRO
Computers
Devices
Users
Computers > Configuration Profiles >
New macOS Configuration Profile
Options
Scope
Time Machine
Finder
Accessibility
Proxies
App-To-Per-App VPN Mapping
FileVault Recovery Key Redirection
Xsan
SmartCard
System Migration
Approved Kernel Extensions
1 Payload Configured
+ Add
Cancel
Save

Approved Kernel Extensions

☑ Allow users to approve kernel extensions

Approved Team IDs and Kernel Extensions

Approved Team ID

DISPLAY NAME: (Optional)

TEAM ID: (Required)

Approved Kernel Extensions (Optional) Approve the following bundle IDs only

DISPLAY NAME | KERNEL EXTENSION BUNDLE...

No Kernel Extension Bundles

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

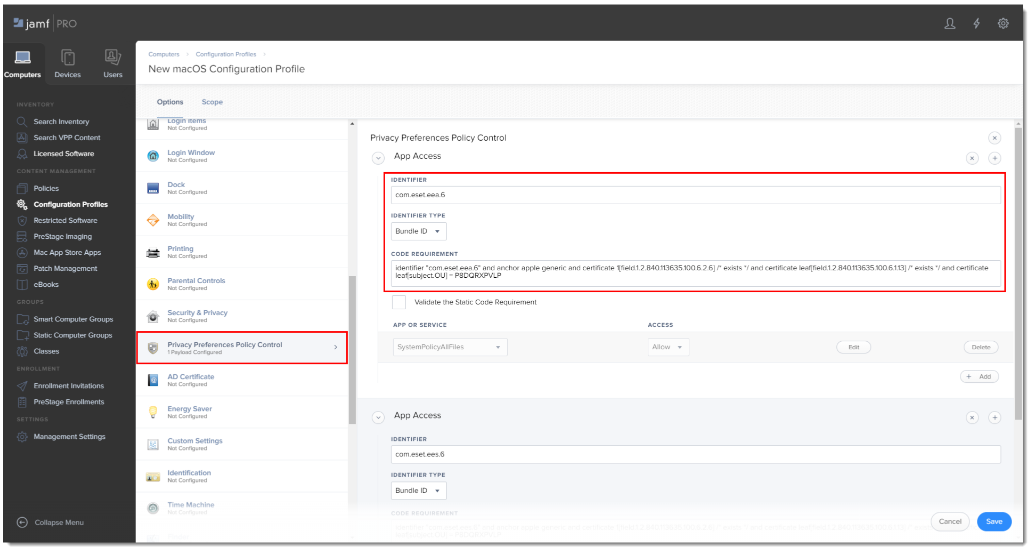
Add both ESET Endpoint Antivirus and ESET Endpoint Security in the same PPPC setting

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



New macOS Configuration Profile

Privacy Preferences Policy Control

App Access

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

□ Validate the Static Code Requirement

APP OR SERVICE	ACCESS
SystemPolicyAllFiles	Allow

App Access

IDENTIFIER: com.eset.ees.6

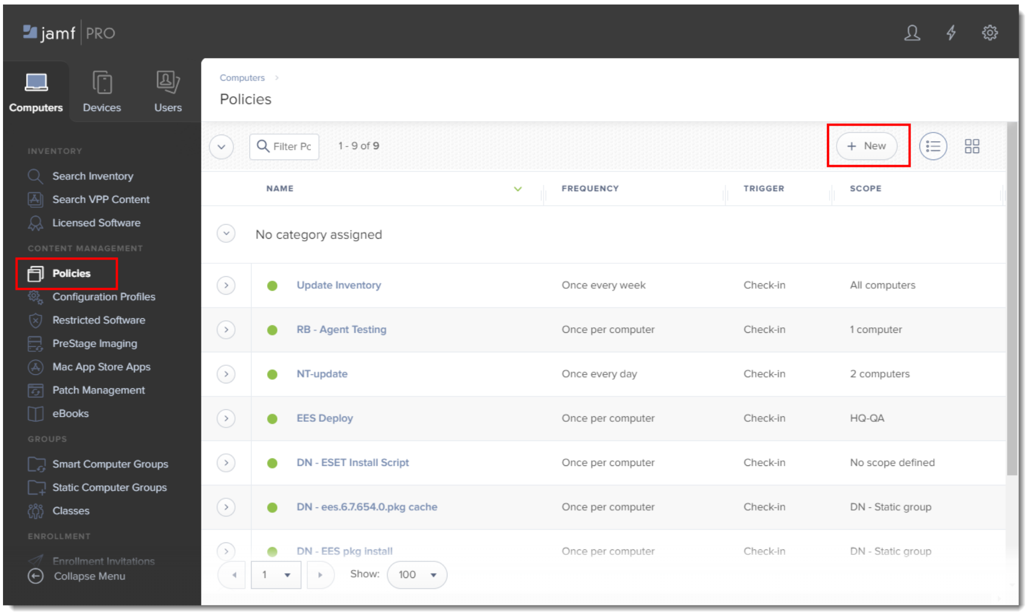
IDENTIFIER TYPE: Bundle ID

CODE REQUIREMENT

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

II. Create policies

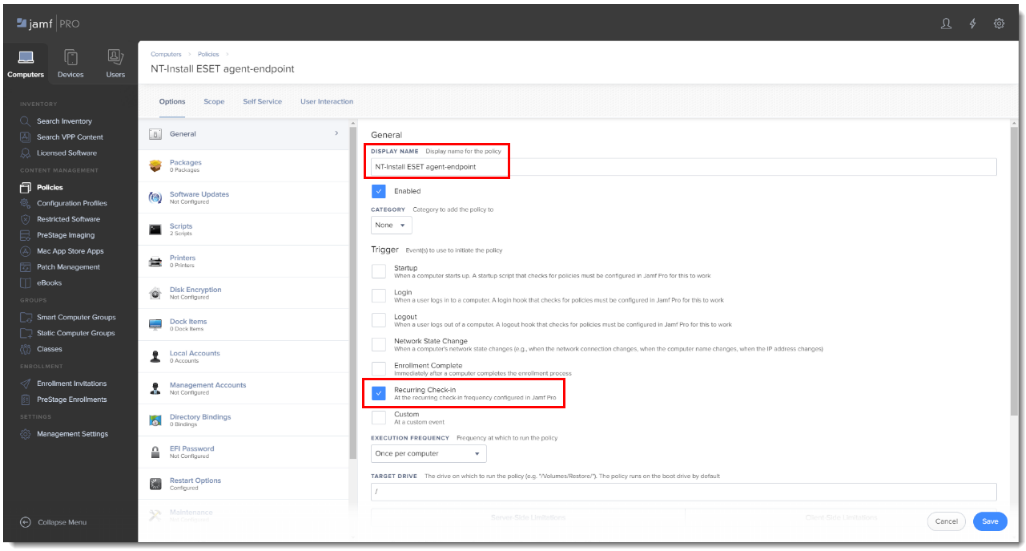
1. Click **Policies** in the left menu and click **New**.



Policies

NAME	FREQUENCY	TRIGGER	SCOPE
No category assigned			
Update Inventory	Once every week	Check-in	All computers
RB - Agent Testing	Once per computer	Check-in	1 computer
NT-update	Once every day	Check-in	2 computers
EES Deploy	Once per computer	Check-in	HQ-QA
DN - ESET Install Script	Once per computer	Check-in	No scope defined
DN - ees.6.7.654.0.pkg cache	Once per computer	Check-in	DN - Static group
DN - EES pkg install	Once per computer	Check-in	DN - Static group

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



NT-Install ESET agent-endpoint

General

DISPLAY NAME Display name for the policy: NT-Install ESET agent-endpoint

☑ Enabled

CATEGORY Category to add the policy to: None

Trigger Event(s) to use to initiate the policy

- ☐ Startup — When a computer starts up. A startup script that checks for policies must be configured in Jamf Pro for this to work
- ☐ Login — When a user logs in to a computer. A login hook that checks for policies must be configured in Jamf Pro for this to work
- ☐ Logout — When a user logs out of a computer. A logout hook that checks for policies must be configured in Jamf Pro for this to work
- ☐ Network State Change — When a computer's network state changes (e.g., when the network connection changes, when the computer name changes, when the IP address changes)
- ☐ Enrollment Complete — Immediately after a computer completes the enrollment process
- ☑ Recurring Check-in — At the recurring check-in frequency configured in Jamf Pro
- ☐ Custom — At a custom event

EXECUTION FREQUENCY Frequency at which to run the policy: Once per computer

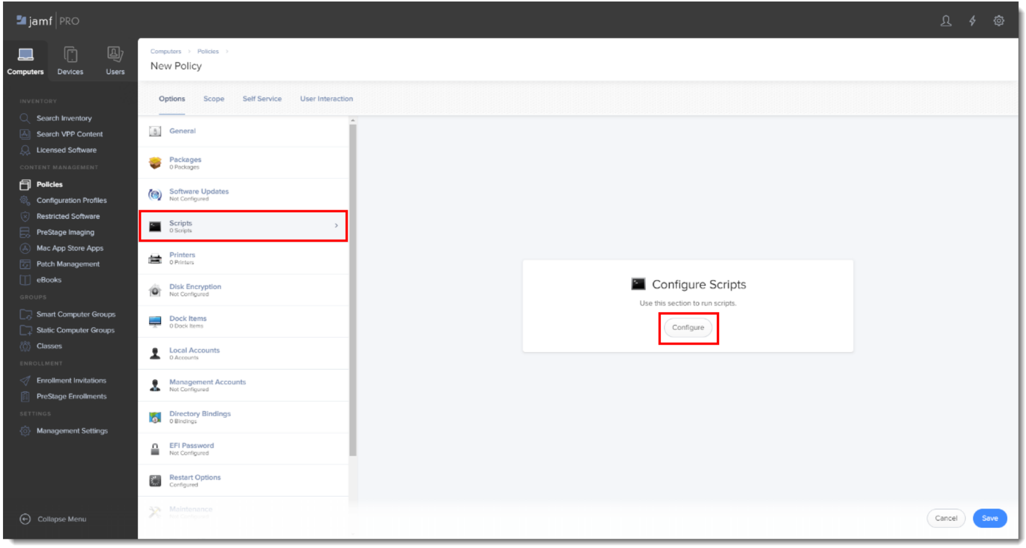
TARGET DRIVE The drive on which to run the policy (e.g. "/Volumes/Restore/"). The policy runs on the boot drive by default: /

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.

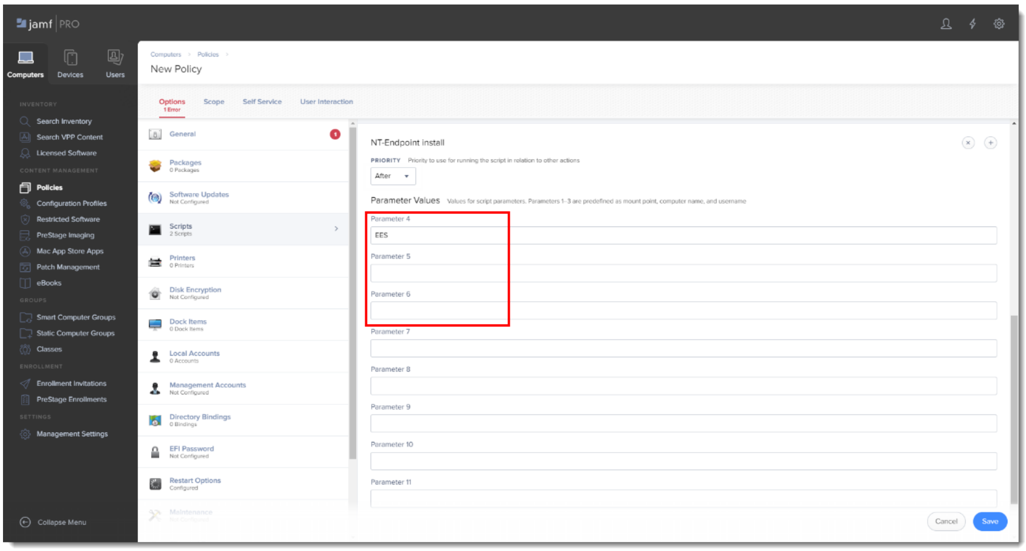
4. After downloading the scripts, add the scripts to Jamf (this link takes you to the Jamf Pro Administrator's Guide).

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



New Policy

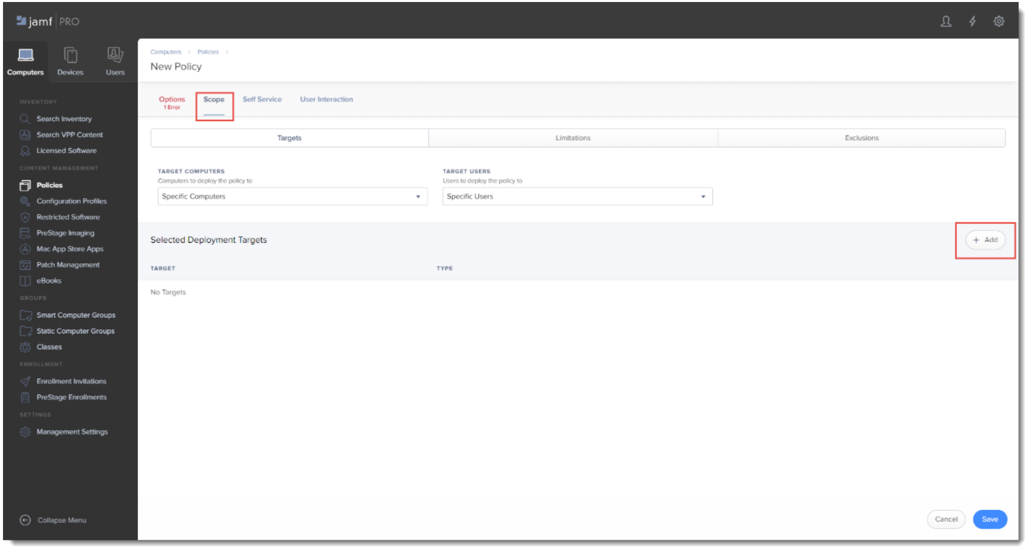
NT-Endpoint install

PRIORITY Priority to use for running the script in relation to other actions: After

Parameter Values Values for script parameters. Parameters 1–3 are predefined as mount point, computer name, and username

Parameter 4: EES

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



New Policy

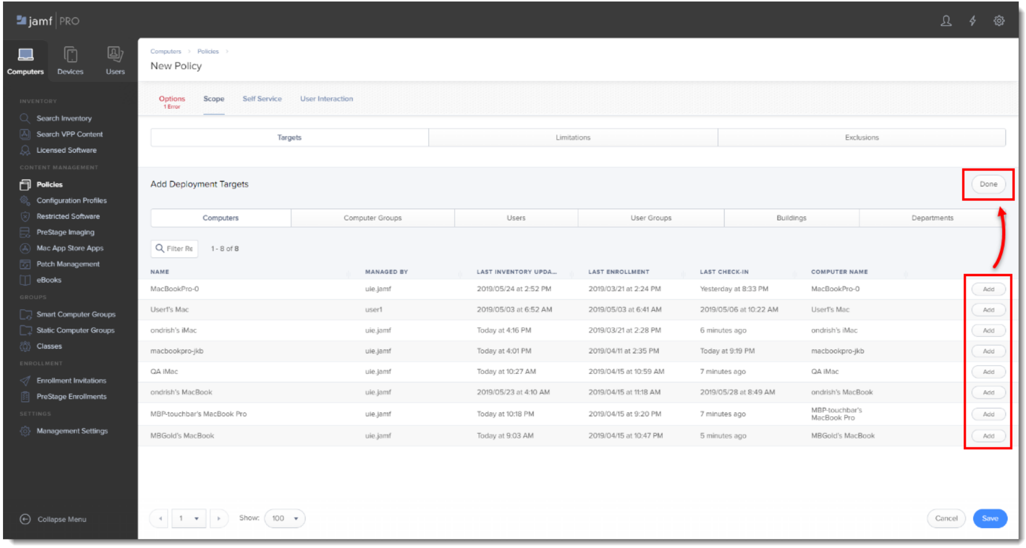
TARGET COMPUTERS Computers to deploy the policy to: Specific Computers

TARGET USERS Users to deploy the policy to: Specific Users

Selected Deployment Targets

No Targets

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



Add Deployment Targets

1 - 8 of 8

NAME	MANAGED BY	LAST INVENTORY UPDA...	LAST ENROLLMENT	LAST CHECK-IN	COMPUTER NAME	
MacBookPro-0	uie.jamf	2019/05/24 at 2:52 PM	2019/03/21 at 2:24 PM	Yesterday at 8:33 PM	MacBookPro-0	Add
User1's Mac	user1	2019/05/03 at 6:52 AM	2019/05/03 at 6:41 AM	2019/05/06 at 10:22 AM	User1's Mac	Add
ondrish's iMac	uie.jamf	Today at 4:16 PM	2019/03/21 at 2:28 PM	6 minutes ago	ondrish's iMac	Add
macbookpro-jkb	uie.jamf	Today at 4:01 PM	2019/04/11 at 2:35 PM	Today at 9:19 PM	macbookpro-jkb	Add
QA iMac	uie.jamf	Today at 10:27 AM	2019/04/15 at 10:59 AM	7 minutes ago	QA iMac	Add
ondrish's MacBook	uie.jamf	2019/05/23 at 4:10 AM	2019/04/15 at 11:18 AM	2019/05/28 at 8:49 AM	ondrish's MacBook	Add
MBP-touchbar's MacBook Pro	uie.jamf	Today at 10:18 PM	2019/04/15 at 9:20 PM	7 minutes ago	MBP-touchbar's MacBook Pro	Add
MBGold's MacBook	uie.jamf	Today at 9:03 AM	2019/04/15 at 10:47 PM	5 minutes ago	MBGold's MacBook	Add

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

Gerelateerde inhoud

- 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