



How to Install SentinelOne with Jamf Pro



Contents

Preface	3
Section 1: Packages and Scripts.....	4
Section 2: Create Smart Computer Groups	8
Section 3: Create a Configuration Profile	12
Section 4: Create a Policy	22



Preface

SentinelOne is a cutting-edge, cybersecurity platform designed to protect organizations from a wide range of threats, including malware, ransomware, and zero-day exploits. By leveraging autonomous technology, SentinelOne provides real-time threat detection, prevention, and remediation without requiring constant human intervention. Its integration of endpoint protection with forensic analysis ensures a robust defense against cyber threats while offering deep insights into security events. This makes SentinelOne an ideal solution for enterprises seeking to enhance their cybersecurity posture with minimal manual oversight.

This guide will walk you through installation steps and configurations required to silently deploy SentinelOne to your Mac computers using Jamf Pro. By following these guidelines and leveraging SentinelOne's autonomous capabilities, you can secure your macOS endpoints effectively while maintaining optimal performance.

This guide will focus on installing SentinelOne on Mac computers running macOS 15 (Sequoia)

Requirements for installing SentinelOne on macOS 15:

- SentinelOne macOS Agent version 24.2.2 or later. At the time of writing this guide SentinelOne is on version 24_4_1_7830
- Pre Authorized Configuration Profiles to prevent user prompts during deployment. This will be created in this guide.

This guide was written using the following:

- macOS 15.3.2
- Jamf Pro Server 11.4.1
- SentinelOne macOS Agent version 24_4_1_7830



Section 1: Packages and Scripts

What You'll Need

Learn what hardware, software, and information you'll need to complete the tutorials in this guide.

Hardware and Software

Requirements for following along with this guide:

- Administrative access to your Jamf Pro server.
- SentinelOne macOS Agent installer package version 24.2.2 or later. At the time of writing, SentinelOne is on version 24_4_1_7830
- SentinelOne organization token

You need to log into your organizations SentinelOne console to get the installer package and your organizational token. This guide will not cover getting the installer package or organizational token from SentinelOne.

In this section, we will upload the SentinelOne macOS Agent and create a script to install and license the SentinelOne Agent without any user interaction.

1. Log into your Jamf Pro server with administrative privileges.

A screenshot of the Jamf Pro login interface. It features a 'Pro' logo at the top. Below it are two input fields: 'Username' and 'Password'. The 'Username' field has a blue border and a blue 'Log in' button below it. The 'Password' field has a blue border and a blue 'Log in' button below it. Both fields are marked as 'Required'.

2. Click Settings (⚙️).
3. Enter **packages** in the search field.
4. Click Packages.

A screenshot of the Jamf Pro Settings page. The left sidebar shows a navigation menu with 'Settings' highlighted by a red box and a red arrow labeled '2'. The main content area is titled 'Settings' and contains a search bar with 'packages' entered, highlighted by a red box and a red arrow labeled '3'. Below the search bar, there are tabs for 'All', 'System', 'Global', 'Jamf apps', 'Self Service', 'Server', 'Network', and 'Computer management'. The 'Computer management' tab is selected, showing '1 result found for "packages"'. The result is a card titled 'Packages' with a red arrow labeled '4' pointing to it. The card contains the text 'Upload packages, configure settings, and set deployment priority'.



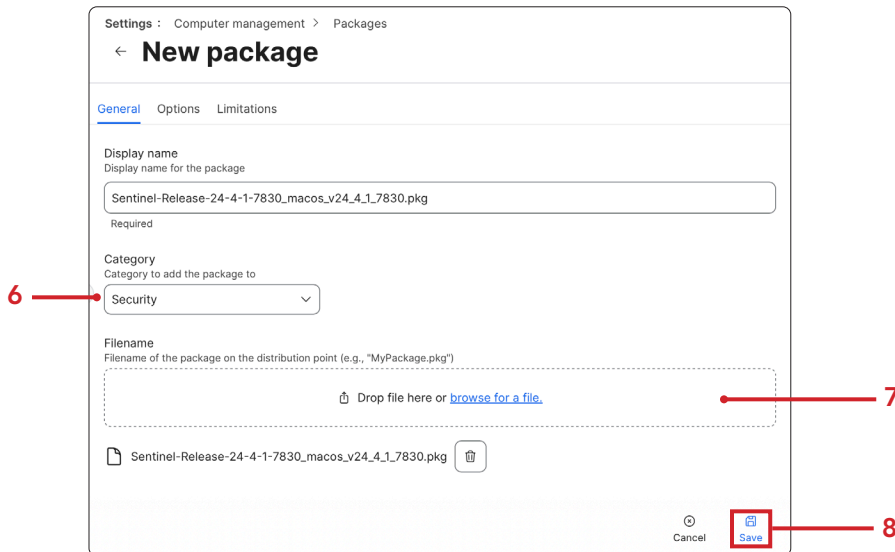
5. Click New (+).



6. Select a category. This guide will use Security.

7. Drag and drop your SentinelOne installer package in the Drop file her section.

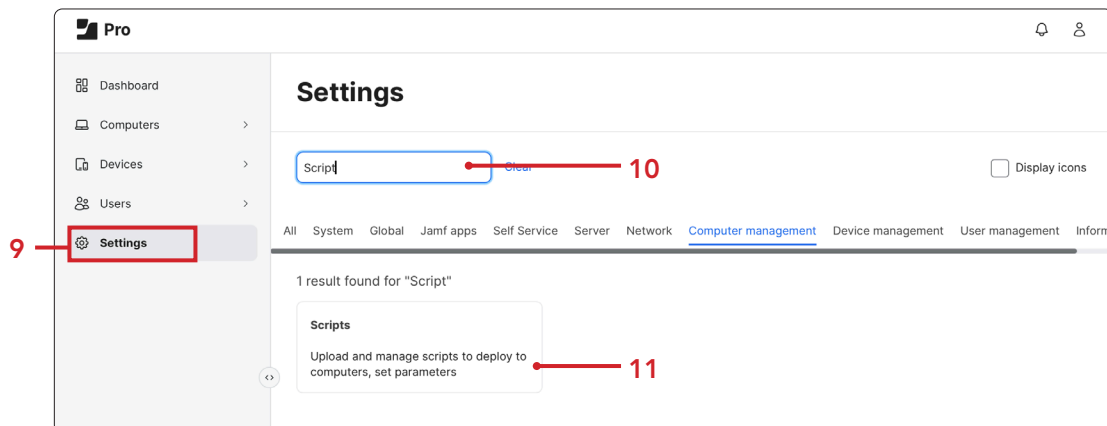
8. Click Save. This will start the package upload.



9. Click Settings.

10. Enter **scripts** in the search field.

11. Click Scripts.





12. Click New.



13. Click General

14. Enter **SentinelOne License and Install** for Display Name.

15. Select a category of your choosing. This guide will use Security

16. Enter **This script will install and license SentinelOne silently** for Information.

17. Click Script.

A screenshot of the 'New Script' form in a settings application. The form has tabs for 'General', 'Script', 'Options', and 'Limitations'. The 'General' tab is selected. The form contains the following fields:

- Display Name:** A text input field containing 'SentinelOne License and Install'. A red line points to this field with the number 14.
- Category:** A dropdown menu with 'Security' selected. A red line points to this dropdown with the number 15.
- Information:** A text input field containing 'This script will install and license SentinelOne silently.'. A red line points to this field with the number 16.
- Notes:** A text input field for additional notes.

At the bottom right, there are 'Cancel' and 'Save' buttons. A red line points to the 'Script' tab with the number 17. A red line points to the 'General' tab with the number 13.



18. Copy and paste the code below into the script field

```
#!/bin/zsh

#This will install SentinelOne and add the site token during the install.
#Make sure to change the installer package version to match the version
you're installing

echo "Your Token Goes Here" > /Library/Application\ Support/JAMF/Waiting\
Room/com.sentinelone.registration-token

/usr/sbin/installer -pkg /Library/Application\ Support/JAMF/Waiting\ Room/
Sentinel-Release-24-4-1-7830_macos_v24_4_1_7830.pkg -target /
```

19. Enter your organizational token in the "Your Token Goes Here" section of the script as shown on line 6. Be sure to enter the token in between the double quotes.

20. Enter the SentinelOne installer package name at the end of line 7 of the script. It may differ from what is shown in the screen shot below.

21. Click Save.

Settings : Computer management > Scripts

New Script

General Script Options Limitations

Mode: Default Theme: Default

```
1 #!/bin/zsh
2
3 #This will install SentinelOne and add the site token during the install.
4 #Make sure to change the installer package version to match the version
5 you're installing
6 echo "Your Token Goes Here" > /Library/Application\ Support/JAMF/Waiting\
7 Room/com.sentinelone.registration-token
8
9 /usr/sbin/installer -pkg /Library/Application\ Support/JAMF/Waiting\ Room/
10 Sentinel-Release-24-4-1-7830_macos_v24_4_1_7830.pkg -target /
```

Copied!

Cancel Save

This completes this section. In the next section, we will create two smart computer groups to use for scoping the installation of SentinelOne.



Section 2: Create Smart Computer Groups

What You'll Need

Learn what hardware, software, and information you'll need to complete the tutorials in this guide.

Hardware and Software

Requirements for following along with this guide:

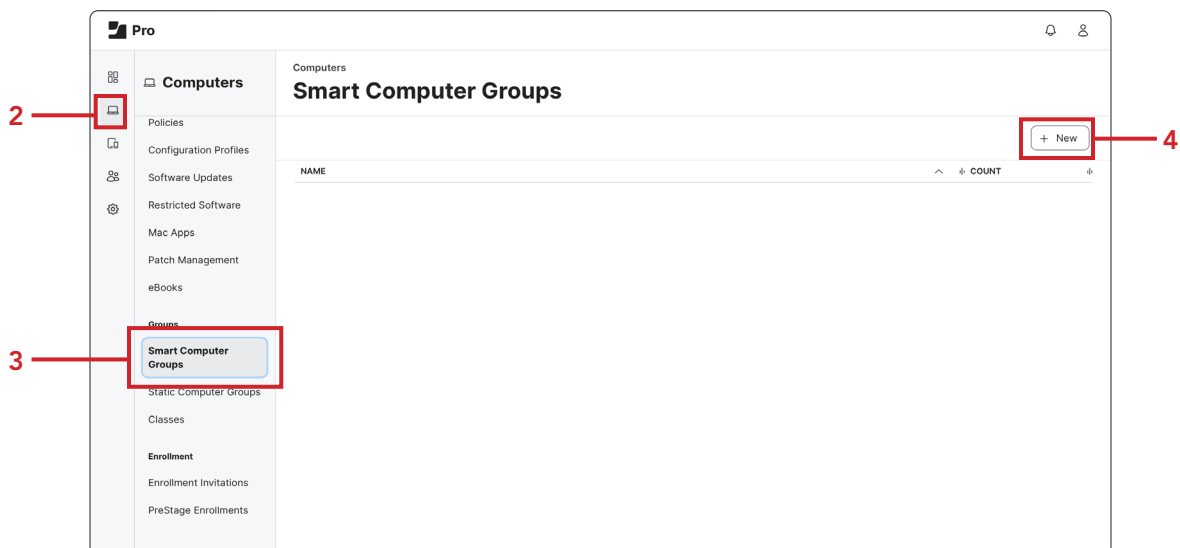
- Administrative access to your Jamf Pro server.

In this section, we will create two smart computer groups to use for scoping the installation of SentinelOne.

1. If necessary, Log into your Jamf Pro server with administrative privileges.

A screenshot of the Jamf Pro login interface. It features a 'Pro' logo at the top. Below it are two input fields: 'Username' and 'Password'. The 'Username' field has a blue border and a small 'i' icon. The 'Password' field has a blue border and a small eye icon. Below the password field is a blue 'Log in' button.

2. Click Computers.
3. Smart Computer Groups.
4. Click New.





5. Click Computer Group.
6. Enter **SentinelOne Installed** for Display Name.
7. Click Criteria.

The screenshot shows the 'Computer Group' configuration page. At the top, there are three tabs: 'Computer Group' (highlighted with a red box and number 5), 'Criteria' (highlighted with a red box and number 7), and 'Reports'. Below the tabs, the 'Display Name' section has a text input field containing 'SentinelOne Installed' (highlighted with a red box and number 6). Below this is a checkbox labeled 'Send email notification on membership change' with a descriptive note. At the bottom, there is a 'Site' dropdown menu currently set to 'None'.

8. Click Add.

The screenshot shows the 'Criteria' tab of the configuration page. It features a table with four columns: 'AND/OR', 'CRITERIA', 'OPERATOR', and 'VALUE'. The table currently contains one row with the text 'No Criteria Specified'. At the bottom right of the table, there is a button labeled '+ Add' (highlighted with a red box).

9. Click Choose for Application Title.

The screenshot shows a text input field labeled 'Application Title'. To the right of the input field is a button labeled 'Choose' (highlighted with a red box).

10. Select "has" for the Operator
11. Enter **SentinelOne Extensions.app** for the Value.
12. Click Save.

The screenshot shows the 'Criteria' tab with the table populated. The first row has a dropdown in the 'AND/OR' column, 'Application Title' in the 'CRITERIA' column, 'has' in the 'OPERATOR' column (highlighted with a red box and number 10), and 'SentinelOne Extensions.app' in the 'VALUE' column (highlighted with a red box and number 11). To the right of the value field are three buttons: a three-dot menu, a dropdown, and a 'Delete' button. Below the table is an '+ Add' button. At the bottom right of the page, there are 'Cancel' and 'Save' buttons (the 'Save' button is highlighted with a red box and number 12).



13. Click Previous (←).

Computers : Smart Computer Groups

← **SentinelOne Installed**

Computer Group Criteria Reports

☐ Show in Jamf Pro Dashboard

AND/OR CRITERIA OPERATOR VALUE

14. Click New (+).

Computers

Smart Computer Groups

+ New

NAME ^ ▾ COUNT ▾

15. Click Computer Group.

16. Enter **SentinelOne NOT Installed** for Display Name.

17. Select Criteria.

15 — Computer Group

17 — Criteria

16 — Display Name

Display name for the smart computer group

SentinelOne NOT Installed

☐ Send email notification on membership change

When group membership changes, send an email notification to Jamf Pro users with email notifications enabled. An SMTP server must be set up in Jamf Pro for this to work

18. Click Add.

Computer Group Criteria

AND/OR CRITERIA OPERATOR VALUE

No Criteria Specified

+ Add

19. Click Choose for Application Title.

Application Title

Choose

20. Select "does not have" for the Operator:

21. Enter **SentinelOne Extensions.app** for the Value.

22. Click Add.

20 — does not have

21 — SentinelOne Extensions.app

22 — + Add

Computer Group Criteria

AND/OR CRITERIA OPERATOR VALUE

Application Title does not have SentinelOne Extensions.app

+ Add



23. Click Show Advanced Criteria.

Computer Group **Criteria**

NEW CRITERIA

Show Advanced Criteria

24. Click Choose for Profile Name.

Profile Name

Choose

25. Select "and".

26. Select "has" for the Operator

27. Enter **SentinelOne Settings** for the Value.

28. Click Save.

Computer Group **Criteria**

AND/OR	CRITERIA	OPERATOR	VALUE
<input type="button" value="v"/>	Application Title	does not have <input type="button" value="v"/>	SentinelOne Extensions.app <input type="button" value="v"/>
25 <input type="button" value="and"/> <input type="button" value="v"/>	Profile Name	26 has <input type="button" value="v"/>	27 SentinelOne Settings <input type="button" value="v"/>

+ Add

Cancel **28** Save

This completes this section. In the next section, we will create a configuration profile with all the required settings to silently install SentinelOne.



Section 3: Create a Configuration Profile

What You'll Need

Learn what hardware, software, and information you'll need to complete the tutorials in this guide.

Hardware and Software

Requirements for following along with this guide:

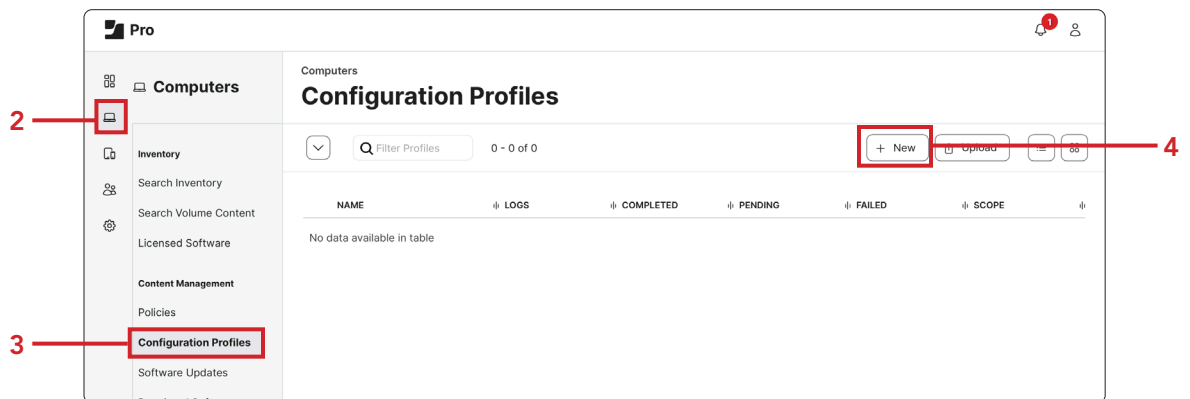
- Administrative access to your Jamf Pro server.

In this section, we will create a configuration profile with all the required settings to silently install SentinelOne.

1. If necessary, Log into your Jamf Pro server with administrative privileges.

The image shows the Jamf Pro login interface. It features a 'Pro' logo at the top. Below it are two input fields: 'Username' and 'Password'. The 'Username' field has a blue border and a blue 'Log in' button below it. The 'Password' field has a blue border and a blue 'Log in' button below it. The 'Log in' button is blue with white text.

2. Click Computers.
3. Click Configuration Profiles.
4. Click New.





5. Click General.
6. Enter **SentinelOne Settings** for the Name. (The name MUST be spelled exactly as shown or the smart group we created in Section 2 will NOT work).
7. Select a category. This guide will use Security.

The screenshot shows the 'Options' tab of the MDM console. On the left, a sidebar lists various settings categories, with 'General' highlighted by a red box and a red line labeled '5'. The main area displays the 'General' settings for a profile named 'SentinelOne Settings'. The 'Name' field is filled with 'SentinelOne Settings' and is highlighted by a red line labeled '6'. The 'Description' field is empty. The 'Site' dropdown is set to 'None'. The 'Category' dropdown is set to 'Security' and is highlighted by a red line labeled '7'. The 'Level' dropdown is set to 'Computer Level'. At the bottom right, there are 'Cancel' and 'Save' buttons.

Options Scope

Search...

General

Name
Display name of the profile

SentinelOne Settings

Description
Brief explanation of the content or purpose of the profile

Site
Site to add the profile to

None

Category
Category to add the profile to

Security

Level
Level at which to apply the profile

Computer Level

Distribution Method
Method to use for distributing the profile

Cancel Save



8. Scroll down and select Content Filter
9. Enter **SentinelOne Content Filter** for Filter Name
10. Enter **com.sentinelone.extensions-wrapper** for Identifier
11. Select "Firewall" for Filter Order.
12. Select "Enable" for Socket Filter.
13. Enter **com.sentinelone.network-monitoring** for Socket Filter Bundle Identifier.
14. For Socket Filter Designated Requirement, Enter:

```
identifier "com.sentinelone.network-monitoring" and anchor apple generic  
and (certificate leaf[field.1.2.840.113635.100.6.1.9] /* exists */ or  
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] = "4AYE5J54KN")
```
15. Select "Ignore" for Network Filter.

The screenshot shows the 'Content Filter' configuration page. On the left, a sidebar lists various settings: 'Content Filter' (highlighted with a red box and callout 8), 'Content Caching', 'Directory', 'DNS Proxy', and 'DNS Settings'. The main area is titled 'Content Filter' and contains several sections. The 'Filter Name' field is set to 'SentinelOne Content Filter' (callout 9). The 'Identifier' field is set to 'com.sentinelone.extensions-wrapper' (callout 10). The 'Filter Order' dropdown is set to 'Firewall' (callout 11). The 'Socket Filter' section has the 'Enable' button highlighted with a green box and callout 12. The 'Socket Filter Bundle Identifier' field is set to 'com.sentinelone.network-monitoring' (callout 13). The 'Socket Filter Designated Requirement' field contains a complex identifier string (callout 14). The 'Network Filter' section at the bottom has the 'Ignore' button highlighted with a blue box and callout 15.



16. Scroll down and select Managed Login Items
17. Select "Label Prefix" for Rule Type.
18. Enter **com.sentinelone.** for Rule Value (there is a trailing period at the end of com.sentinelone. it must contain the trailing period)
19. Enter **Prevent removal of SentinelOne Launch Agents and Launch Daemons** for Rule Comment
20. Click Add (+).

The screenshot shows the 'Managed Login Items' configuration page. On the left, a sidebar lists various settings, with 'Managed Login Items' highlighted and annotated with a red line and the number 16. The main area is titled 'Managed Login Items' and shows '1 setting configured'. Below this, there's a 'Setting' section with a toggle for 'Managed Login Item rules' (annotated with 17). The 'Rule type' dropdown is set to 'Label Prefix' (annotated with 17). The 'Rule value' field contains 'com.sentinelone.' (annotated with 18). The 'Rule comment' field contains 'Prevent removal of SentinelOne Launch Agents and Launch Daemons' (annotated with 19). At the bottom right, there's a '+ Add' button (annotated with 20).

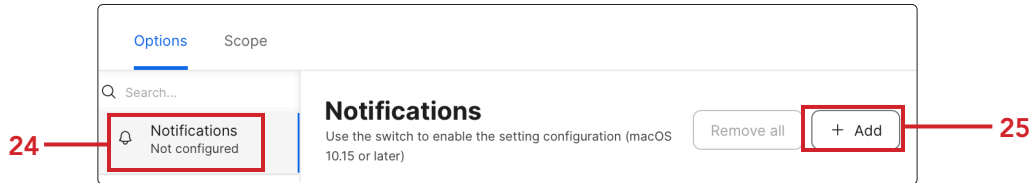
21. Enter **Bundle Identifier** for Rule Type.
22. Enter **com.sentinelone** for Rule Value:
23. Enter **Prevent removal of SentinelOne Launch Agents and Launch Daemons** for Rule Comment.

This is a close-up of the rule configuration fields. The 'Rule type' dropdown is set to 'Bundle Identifier' (annotated with 21). The 'Rule value' field contains 'com.sentinelone' (annotated with 22). The 'Rule comment' field contains 'Prevent removal of SentinelOne Launch Agents and Launch Daemons' (annotated with 23).



24. Scroll down the payloads and select Notifications.

25. Click Add.



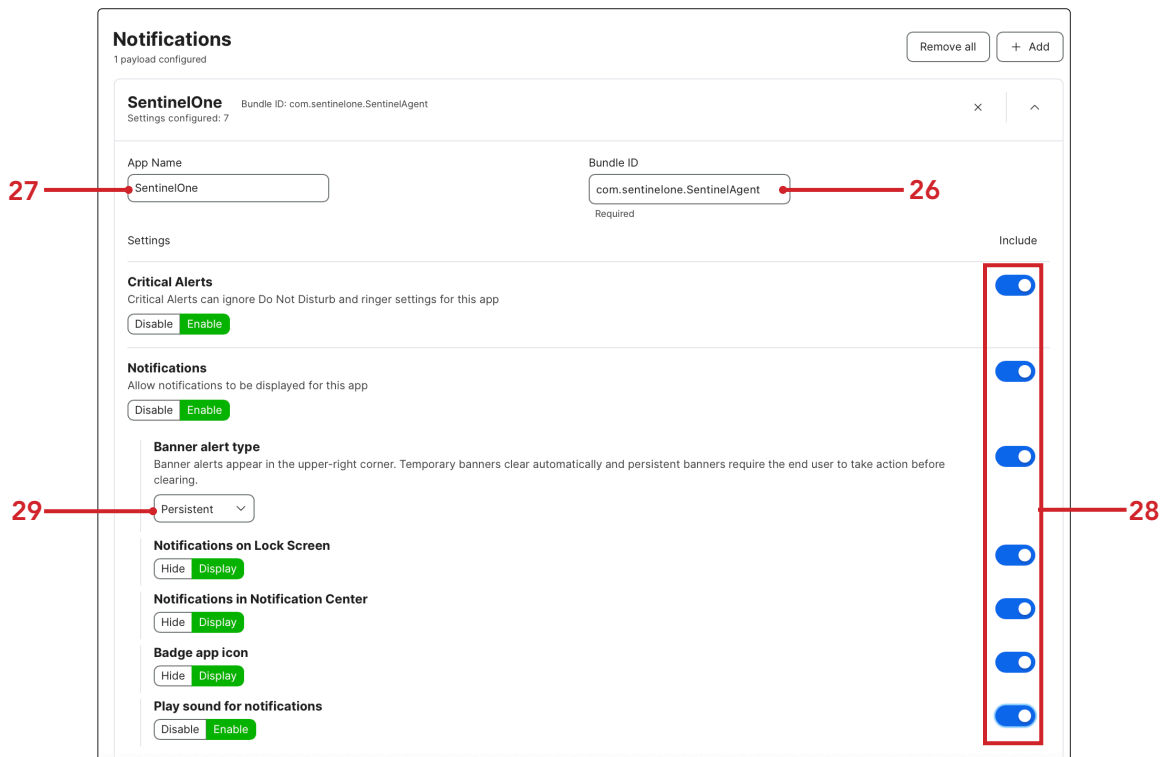
26. Enter **SentinelOne** for App Name.

27. Enter **com.sentinelone.SentinelAgent** for Bundle ID.

28. Enable the following settings as shown below:

- Critical Alerts
- Notifications
- Banner Type Alert
- Notifications on Lock Screen
- Notifications in Notification Center
- Badge app icon
- Play sound for notifications

29. Set "Banner Type Alert" to your liking. This guide will set to Persistent.





30. Scroll down and select Privacy Preferences Policy Control

31. Click Configure

Options Scope

Search...

Not configured

Privacy Preferences Policy Control
Not configured

Proxies
Not configured

Restrictions
Not configured

SCEP
Not configured

Security and Privacy
Not configured

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).

Configure

32. Enter `com.sentinelone.sentinelid` for Identifier.

33. Select "Bundle ID" for Identifier Type.

34. Enter the following for Code Requirement:

```
anchor apple generic and identifier "com.sentinelone.sentinelid" and  
(certificate leaf[field.1.2.840.113635.100.6.1.9] /* exists */ or  
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] = "4AYE5J54KN")
```

35. Click Add (+) for App or Service.

Inventory

Search Inventory

Search Volume Content

Licensed Software

Content Management

Policies

Configuration Profiles

Software Updates

Restricted Software

Mac Apps

Patch Management

eBooks

Groups

Smart Computer Groups

Static Computer Groups

Options Scope

Search...

Privacy Preferences Policy Control
1 payload configured

Proxies
Not configured

Restrictions
Not configured

SCEP
Not configured

Security and Privacy
Not configured

Single Sign-On Extensions
Not configured

Smart Card
Not configured

Privacy Preferences Policy Control

App access

Identifier

com.sentinelone.sentinelid

Identifier Type

Bundle ID

Code Requirement

anchor apple generic and identifier "com.sentinelone.sentinelid" and (certificate leaf[field.1.2.840.113635.100.6.1.9] /* exists */ or 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] = "4AYE5J54KN")

☐ Validate the Static Code Requirement

APP OR SERVICE ACCESS

+ Add



36. Select "SystemPolicyAllFiles".
37. Select "Allow".
38. Click Save.
39. Click Add (+) in the upper right corner to create a new Privacy Preferences Policy Control.

40. Enter `com.sentinelone.sentinelid-helper` for Identifier
41. Select "Bundle ID" for Identifier Type
42. Code Requirement:

```
anchor apple generic and identifier "com.sentinelone.sentinelid-helper"
and (certificate leaf[field.1.2.840.113635.100.6.1.9] /* exists */ or
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] = "4AYE5J54KN")
```

43. Click Add (+) for App or Service [Not Shown].
44. Select "SystemPolicyAllFiles".
45. Set to "Allow".
46. Click Save.
47. Click Add (+) in the upper-right corner



48. Enter **com.sentinelone.sentinel-d-shell** for Identifier

49. Select "Bundle ID" for Identifier Type.

50. For Code Requirement, enter:

```
anchor apple generic and identifier "com.sentinelone.sentinel-d-shell"
and (certificate leaf[field.1.2.840.113635.100.6.1.9] /* exists */ or
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] = "4AYE5J54KN")
```

51. Click Add (+) for App or Service [Not Shown].

52. Select "SystemPolicyAllFiles".

53. Set to "Allow".

54. Click Save.

App access

Identifier:

Identifier Type:

Code Requirement:

☐ Validate the Static Code Requirement

APP OR SERVICE:

ACCESS:

55. Scroll down and select System Extensions.

56. Click Configure

Configure System Extensions

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

System Extensions (Not configured)



57. Enter **SentinelOne Network Monitoring Extension** for Display Name.

58. Select "Allowed system extensions" for System Extension Types.

59. Enter **4AYE5J54KN** for Team Identifier.

60. Click Add (+) for Allowed System Extensions [Not Shown].

61. Enter **com.sentinelone.network-monitoring**.

62. Click Save.

63. Click Add (+) in the upper right corner to create a allowed extension.

64. Enter **SentinelOne System Extension** for Display Name.

65. Select "Non-removable system extensions from UI" for System Extension Types.

66. Enter **4AYE5J54KN** for Team Identifier.

67. Click Scope.



68.Scope to your Target computers. This guide will use All Computers.

69.Click Save.

68

Options **Scope**

Targets Limitations Exclusions

Target Computers
Computers to assign the profile to
All Computers

Target Users
Users to distribute the profile to
Specific Users

Selected Deployment Targets + Add

TARGET	TYPE
No Targets	

Cancel Save 69

This completes this section. In the next section, we will create a policy to install the SentinelOne Mac Agent.



Section 4: Create a Policy

What You'll Need

Learn what hardware, software, and information you'll need to complete the tutorials in this guide.

Hardware and Software

Requirements for following along with this guide:

- Administrative access to your Jamf Pro server.
- A Non-Production Test Mac computer enrolled in Jamf Pro without SentinelOne installed.

In this section, we will create a policy to install SentinelOne and test our workflow to make sure it gets installed.

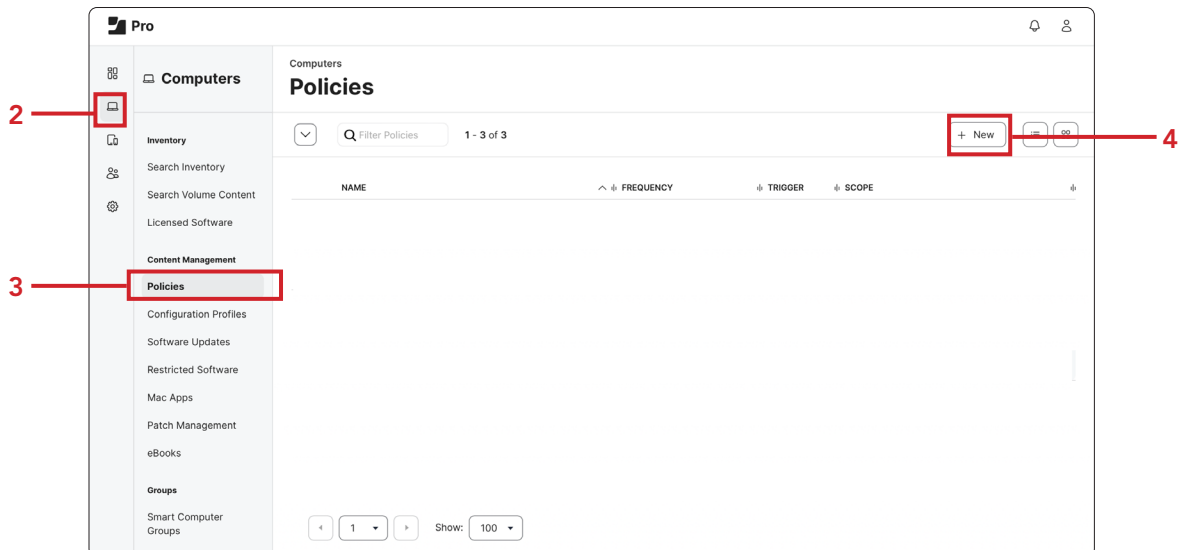
1. If necessary, Log into your Jamf Pro server with administrative privileges.

A screenshot of the Jamf Pro login interface. It features a 'Pro' logo at the top. Below it are two input fields: 'Username' and 'Password'. The 'Username' field has a blue border and a blue 'i' icon. The 'Password' field has a blue border and a blue eye icon. Below the password field is a blue 'Log in' button.

2. Click Computers.

3. Click Policies.

4. Click New.





5. Click General.
6. Enter **Install SentinelOne** for Display Name.
7. Select a category of your choosing. This guide will use Security.
8. Select "Recurring Check-in" for the Trigger.
9. Select "Once per computer" for the Execution Frequency.
10. Select the checkbox for "Automatically re-run policy on failure".
11. Select "On next recurring check-in" for Retry Event.
12. Select 3 for Retry Attempts:

The screenshot shows the 'General' tab of a policy configuration in Jamf Pro. The left sidebar lists various system categories, with 'General' selected. The main area contains the following settings:

- Display Name:** Install SentinelOne (indicated by line 6)
- Enabled:** Checked (checkbox)
- Site:** None (dropdown)
- Category:** Security (indicated by line 7)
- Trigger:** Recurring Check-in (checked, indicated by line 8)
- Execution Frequency:** Once per computer (dropdown, indicated by line 9)
- Automatically re-run policy on failure:** Checked (checkbox, indicated by line 10)
- Retry Event:** On next recurring check-in (dropdown, indicated by line 11)
- Retry Attempts:** 3 (dropdown, indicated by line 12)

13. Click Packages
14. Click Configure

The screenshot shows the 'Configure Packages' section. The left sidebar has 'Packages' selected (indicated by line 13). The main area has a 'Configure' button (indicated by line 14).

15. Click Add for your version of the SentinelOne installer package.

The screenshot shows a table of packages. The first row is highlighted:

Sentinel-Release-24-4-1-7830_macos_v24_4_1_7830.pkg	Security	Add
---	----------	-----



16. Set your distribution point. This guide will use "Each computers default distribution point".

17. Select "Cache" for Action.

Packages

Distribution Point
Distribution point to download the package(s) from

16 → Each computer's default distribution point ▼

Sentinel-Release-24-4-1-7830_macos_v24_4_1_7830.pkg

Action
Action to take on computers

17 → Cache ▼

18. Click Scripts

19. Click Configure

Options Scope Self Service User Interaction

Packages
1 Package

Software Updates
Not Configured

18 → **Scripts**
0 Scripts

Configure Scripts
Use this section to run scripts.

19 → Configure

20. Click Add for SentinelOne License and Install.

SentinelOne License and Install Security **Add**

21. Select After for the Priority.

Scripts

SentinelOne License and Install

Priority
Priority to use for running the script in relation to other actions

After ▼

22. Click Maintenance.

23. Click Configure

Directory Bindings
0 Bindings

EFI Password
Not Configured

Restart Options
Not Configured

22 → **Maintenance**
Not Configured

Files and Processes
Not Configured

Configure Maintenance
Use this section to update inventory, reset computer names, install all cached packages, and run common maintenance tasks.

23 → Configure



24. Confirm Update Inventory is enabled.

Maintenance

☒ **Update Inventory**
Force computers to submit updated inventory information to Jamf Pro

☐ **Reset Computer Names**
Change the computer name on computers to match the computer name in Jamf Pro

☐ **Install Cached Packages**
Install packages cached by Jamf Pro

25. Click Scope.

26. Click Add.

Options **Scope** Self Service User Interaction

Targets Limitations Exclusions

Target Computers
Computers to deploy the policy to
Specific Computers

Target Users
Users to deploy the policy to
Specific Users

Selected Deployment Targets **+ Add**

27. Click Computer Groups.

28. Enter **sentinelOne Not** in the search field.

29. Click Add for SentinelOne NOT Installed.

Add Deployment Targets Done

Computers **Computer Groups** Users User Groups Buildings

Departments

Q sentinelOne Not 1 - 1 of 1

GROUP NAME
SentinelOne NOT Installed **Add**



30. Click Save.

A screenshot of the 'Add Deployment Targets' dialog box in Jamf Pro. The dialog has tabs for 'Options', 'Scope' (selected), 'Self Service', and 'User Interaction'. Under the 'Scope' tab, there are sections for 'Targets', 'Limitations', and 'Exclusions'. The 'Targets' section contains a table with columns: 'Computers', 'Computer Groups', 'Users', 'User Groups', 'Buildings', and 'Departments'. A search bar shows 'sentinelOne Not' and '1 - 1 of 1'. Below the table is a 'GROUP NAME' field. At the bottom right, there are 'Cancel' and 'Save' buttons, with the 'Save' button highlighted by a red rectangle.

Let's test our workflow. Please use a Non-production test Mac computer enrolled in Jamf Pro without SentinelOne installed.

31. Open Terminal.app located in /Applications/Utilities



Terminal.app

32. Run the following command:

```
sudo jamf policy
```

Enter your admin credentials when prompted.

If all went well, SentinelOne should be installed on your Mac computer without any user interaction.

This completes the guide.