



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: Configuration Profiles.....	12
Section 4: Policies.....	21



Preface

What is SentinelOne?

SentinelOne protects your computer and data with anti-malware and anti-exploit protection. The SentinelOne agent continually receives intelligence updates from SentinelOne servers. The agent is very lightweight on resources and offers minimal to no impact on work.

This guide was written using the following:

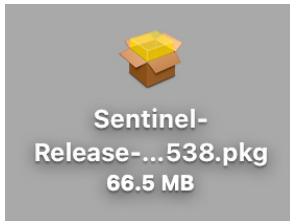
1. macOS Ventura 13.2
2. Jamf Pro 10.43
3. SentinelOne



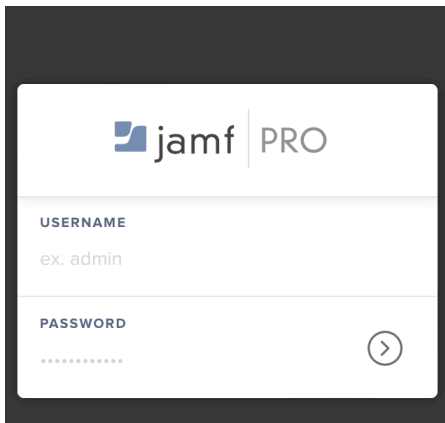
Section 1: Packages and Scripts

In this section, we will upload the SentinelOne package and script as well as create a category for organizational purposes.

1. Acquire the SentinelOne package and your organization token from the SentinelOne console.

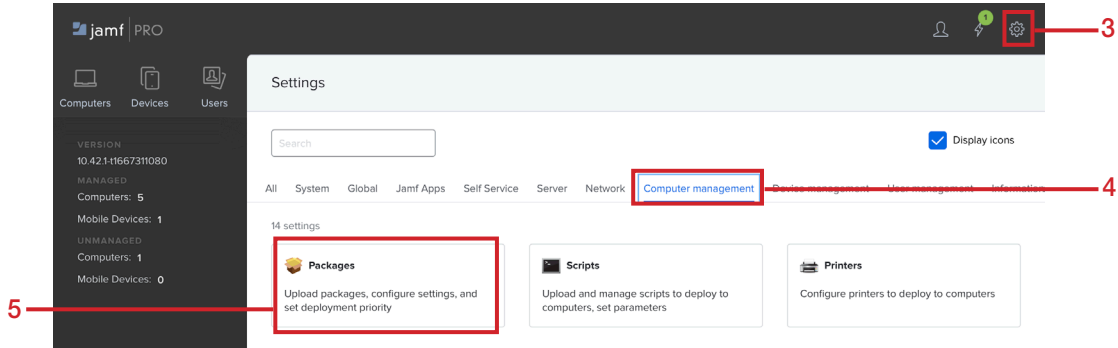


2. Log into your Jamf Pro server.

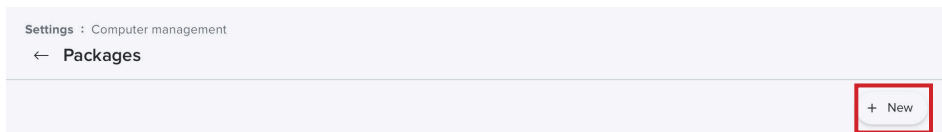




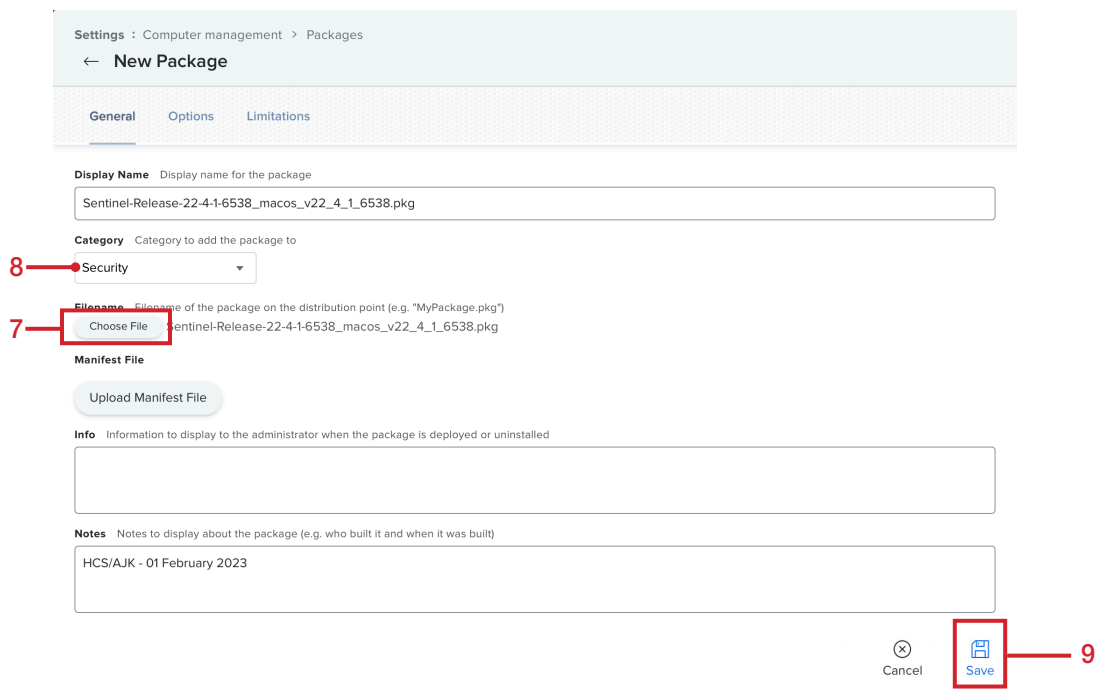
- 3. In Jamf Pro, Click Settings (⚙️).
- 4. Click Computer management.
- 5. Click Packages.



- 6. Click New (+).

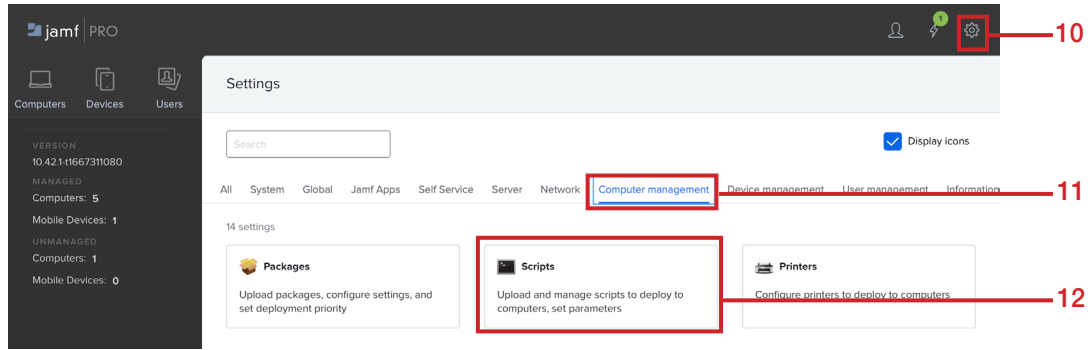


- 7. Click Choose File and select your SentinelOne package.
- 8. Select a category and add notes if desired.
- 9. Once you are ready to upload the package, click Save.

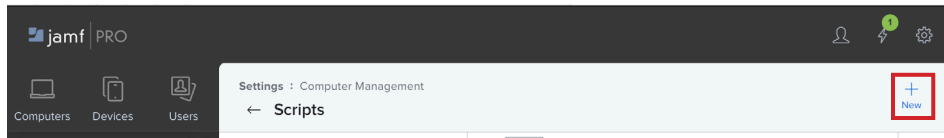




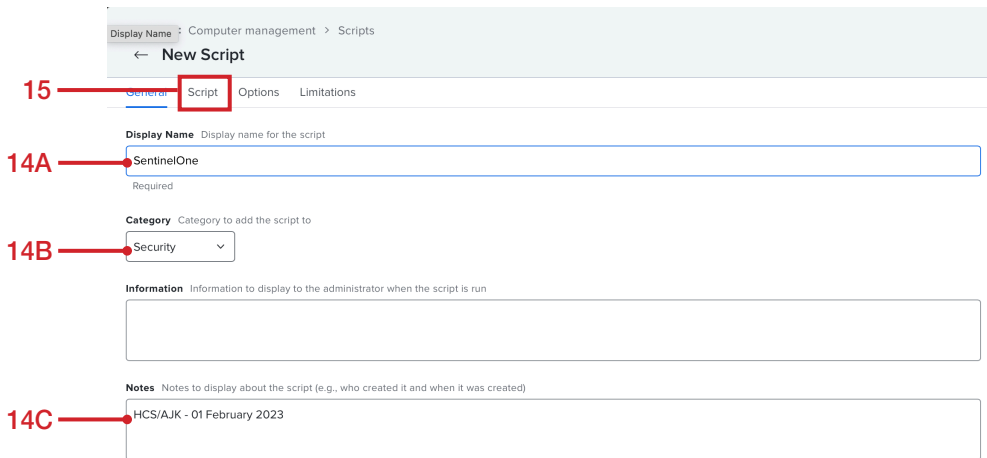
- 10. Click Settings (⚙️).
- 11. Click Computer management.
- 12. Click Scripts.



- 13. Click New (+).



- 14. Configure the following:
 - A. Display Name: **SentinelOne**
 - B. Select a category
 - C. Add notes if desired.
- 15. Click Script.

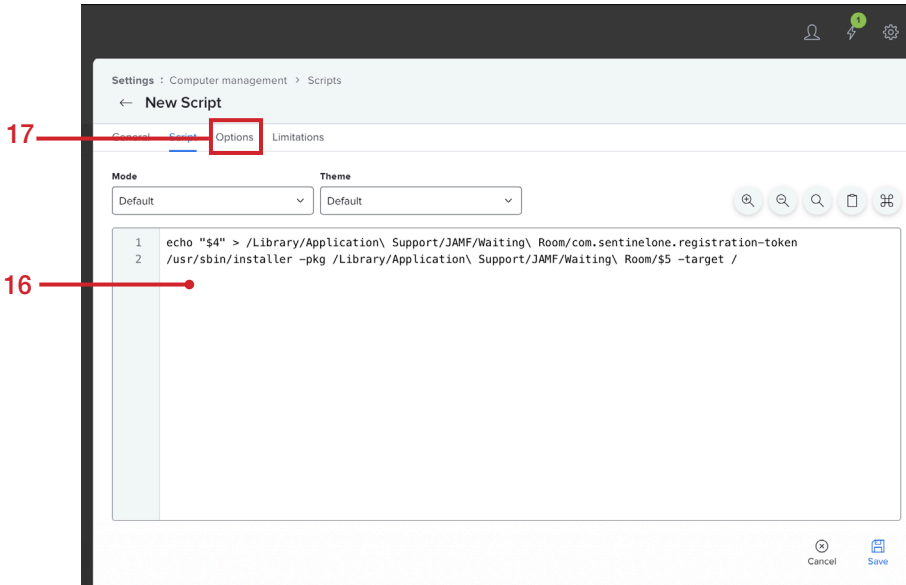




16. Enter the following code:

```
echo "$4" > /Library/Application\ Support/JAMF/Waiting\ Room/com.sentinelone.registration-token  
/usr/sbin/installer -pkg /Library/Application\ Support/JAMF/Waiting\ Room/$5 -target /
```

17. Click Options.

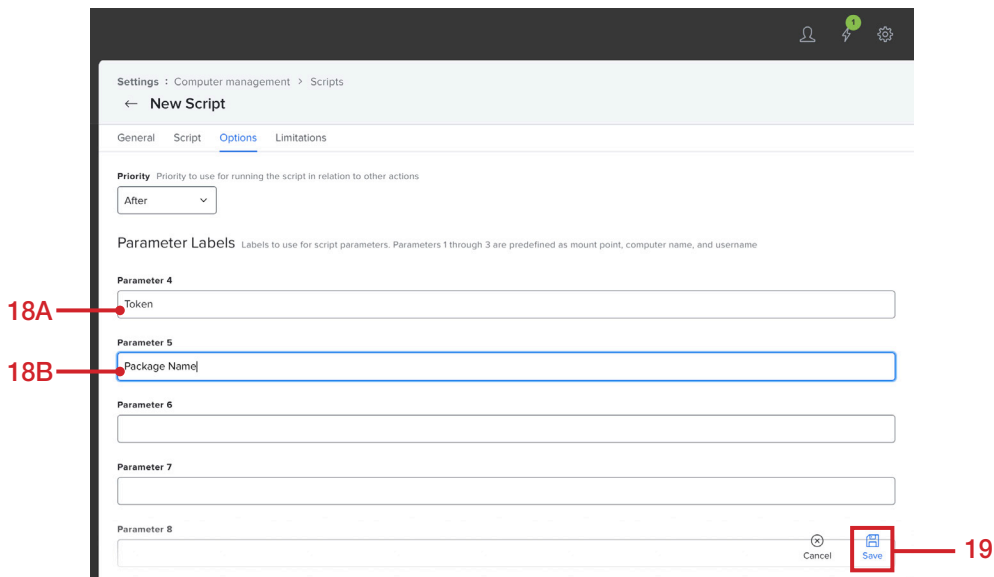


18. Configure the following:

- A. Parameter 4: **Token**
- B. Parameter 5: **Package Name**

Parameter 4 will be used for the registration token and parameter 5 will be used for the name of the package.

19. Click Save.

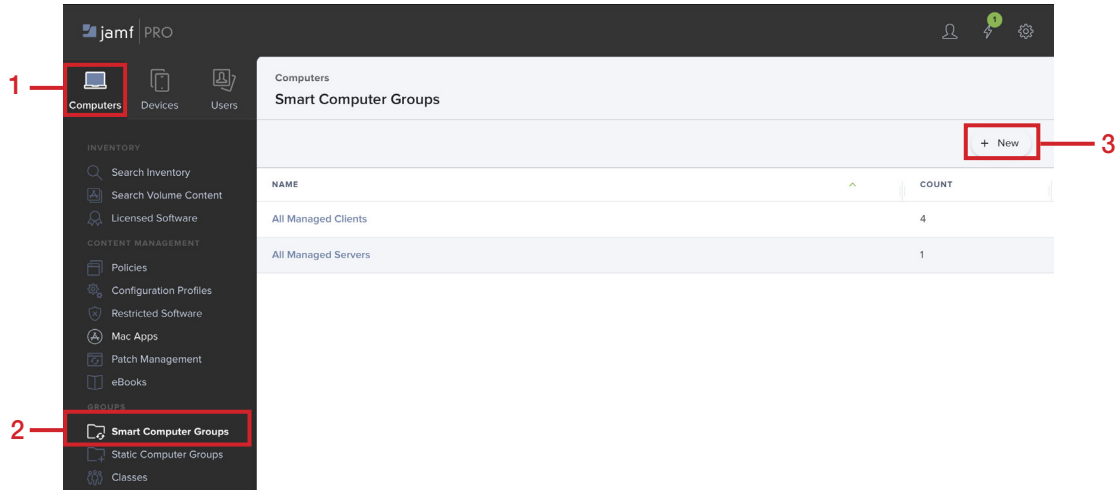




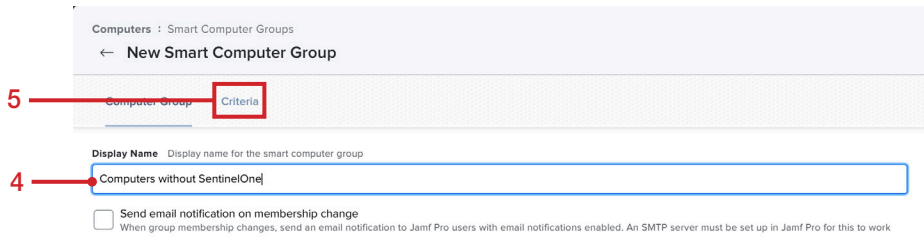
Section 2: Create Smart Computer Groups

In this section, we will create two smart groups for scoping purposes.

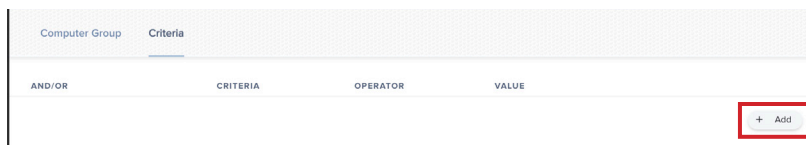
1. Click Computers.
2. Click Smart Computer Groups.
3. Click New.



4. For the Display name, enter **Computers without SentinelOne**.
5. Click Criteria.



6. Click Add (+).





7. Choose Application Title.

Computers : Smart Computer Groups
← New Smart Computer Group

Computer Group Criteria

NEW CRITERIA Show Advanced Criteria

Application Title	Choose
Building	Choose
Computer Group	Choose
Computer Name	Choose
Department	Choose

8. Change the operator to "does not have".

9. Enter the Value **SentinelOne Extensions.app**.

10. Click Save.

11. Click Smart Computer Groups.

Computers : Smart Computer Groups
← Computers without SentinelOne

Computer Group Criteria Reports

AND/OR	CRITERIA	OPERATOR	VALUE	
▼	Application Title	does not ▼	SentinelOne E	⋮

+ Add

Cancel Save

12. Click New.

Computers
Smart Computer Groups

+ New

NAME	COUNT
------	-------



13. For the Display name, enter **Computers running macOS 13 or greater**.

14. Click Criteria.

15. Click Add (+).

16. Click Show Advanced Criteria.



17. Scroll down, choose Operating System Version

Computers : Smart Computer Groups
← New Smart Computer Group

Computer Group	Criteria
	Number of Processors Choose
	Operating System Choose
	Operating System Build Choose
	Operating System Name Choose
	Operating System Version Choose
	Optical Drive Choose

18. Configure the following:

- A. Change the operator to "greater than or equal"
- B. Value: **13.0**
- C. Click Save

Computers : Smart Computer Groups
← New Smart Computer Group

AND/OR	CRITERIA	OPERATOR	VALUE	
▼	Operating System Version	greater than or equal ▼	13.0	***

+ Add

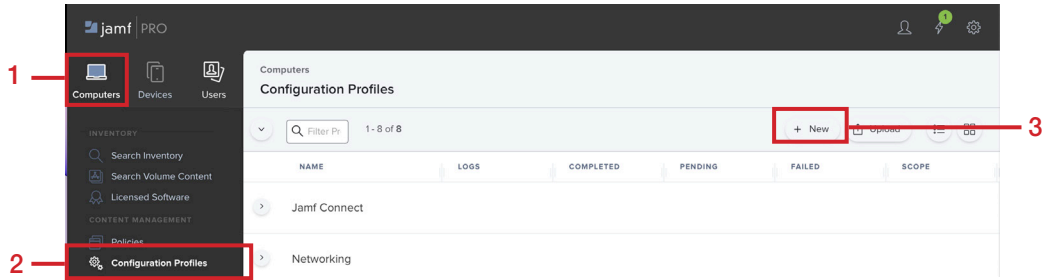
Cancel Save



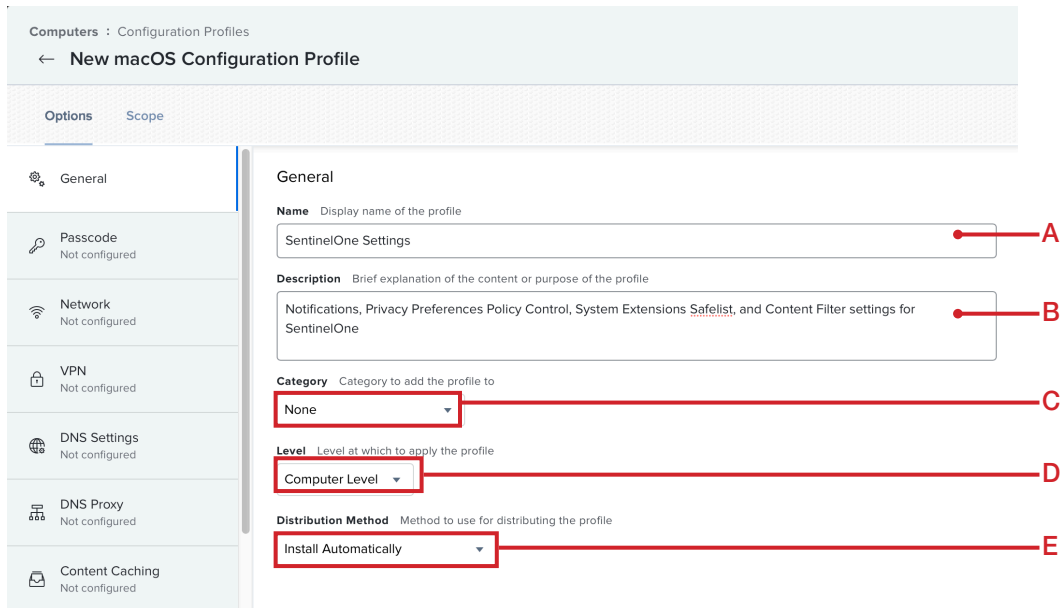
Section 3: Configuration Profiles

Create Configuration Profiles to ensure SentinelOne installs and operates properly.

1. Click Computers.
2. Click Configuration Profiles.
3. Click New (+).

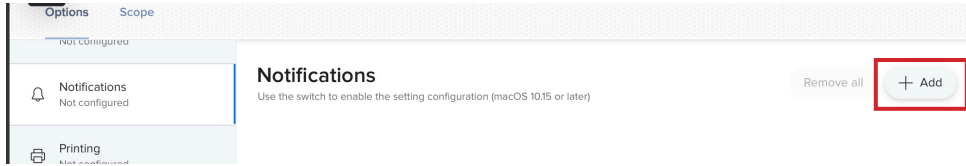


4. Configure the profile with the following:
 - A. Name: **SentinelOne Settings**
 - B. Enter a description
 - C. Select a category
 - D. Level is set to Computer Level
 - E. Distribution Method is set to Install Automatically.

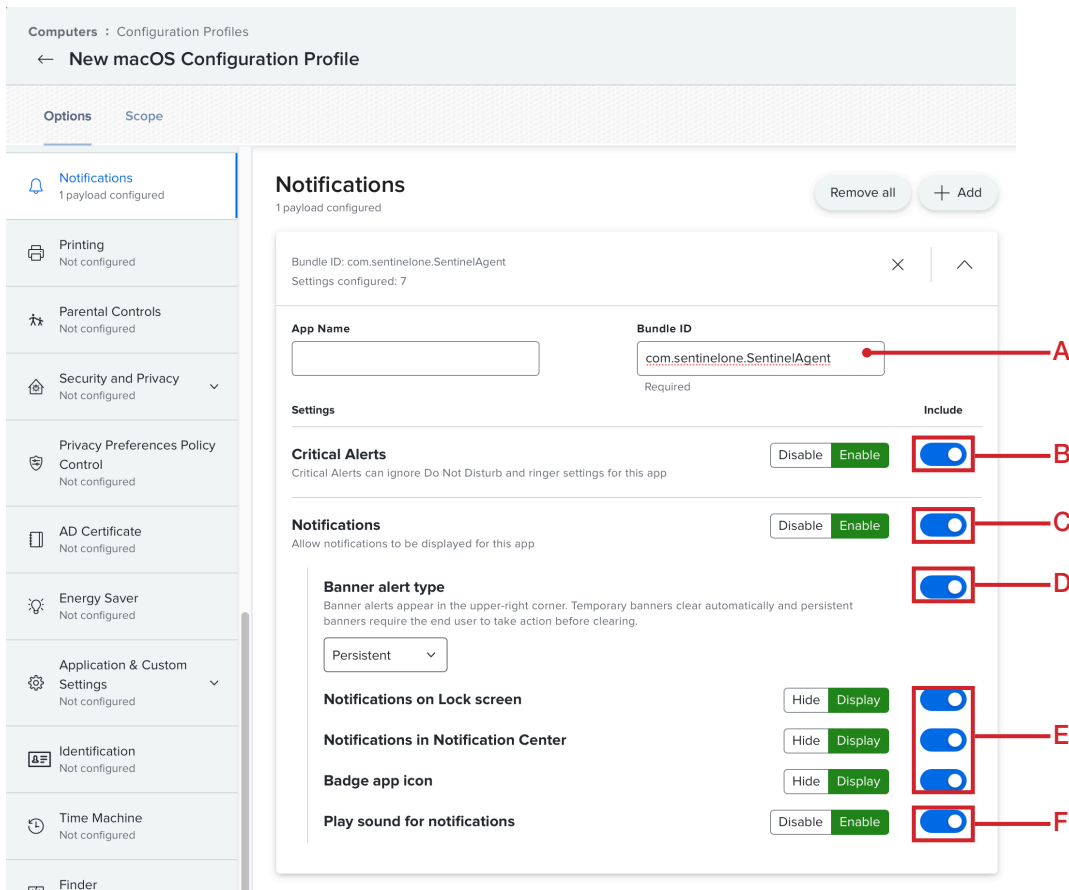




5. Scroll to the Notifications payload.
6. Click Add (+).

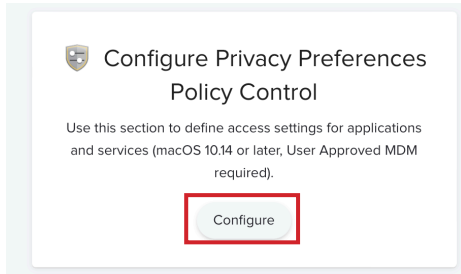


7. Configure the payload with the following:
 - A. Enter the Bundle ID: **com.sentinelone.SentinelAgent**
 - B. Enable Critical Alerts
 - C. Enable Notifications
 - D. Banner alert type, set to Persistent
 - E. Select Display for:
 - Notifications on Lock Screen
 - Notifications in Notification Center
 - Badge app icon
 - F. Enable Play sound for notifications
 - G. Click Privacy Preferences Policy Control





8. Click Configure.



9. Configure the payload with the following:

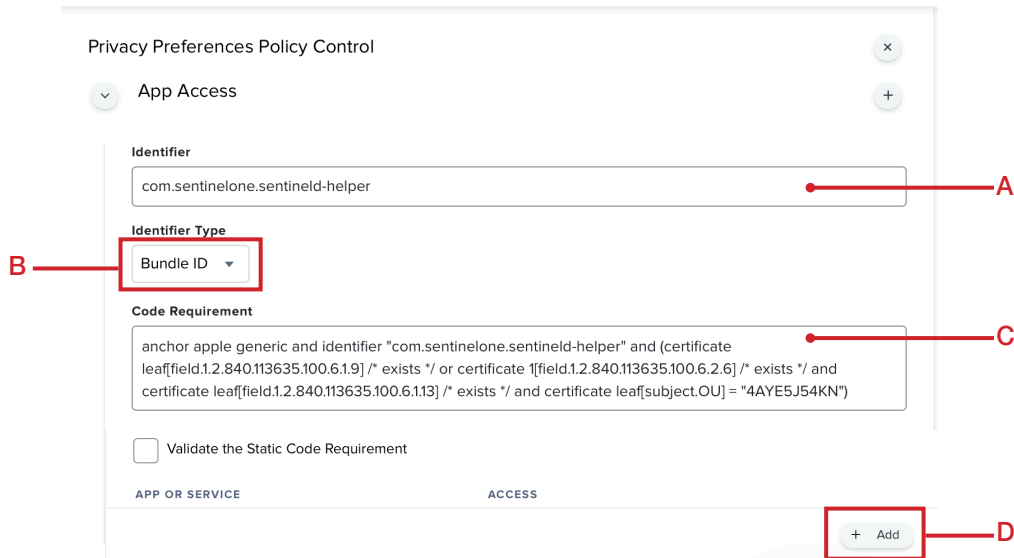
A. Identifier: **com.sentinelone.sentinel-helper**.

B. Identifier Type: select Bundle ID.

C. Code Requirement, enter the following:

anchor apple generic and identifier "com.sentinelone.sentinel-helper" and (certificate leaf[field.1.2.840.113635.100.6.1.9] /* exists */ or certificate [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")

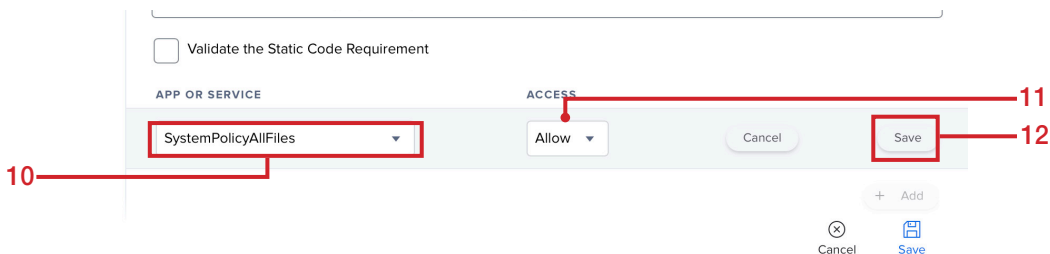
D. Click Add (+).



10. Choose SystemPolicyAllFiles.

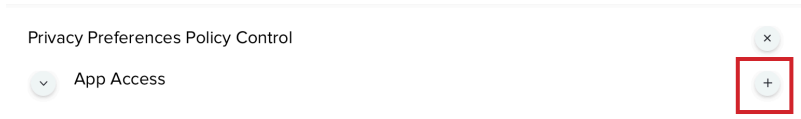
11. Select Allow for Access.

12. Click Save.





13. Click Add (+) to add another App Access.



14. Scroll down and configure the following:

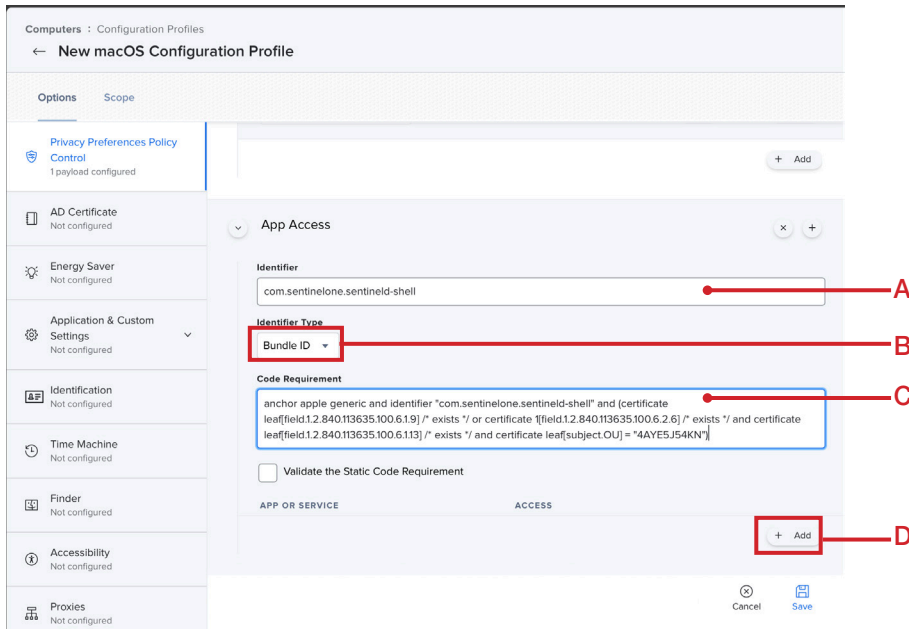
A. Identifier: **com.sentinelone.sentinel-d-shell**

B. Identifier Type: select Bundle ID

C. Code Requirement, enter the following:

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")

D. Click Add (+).

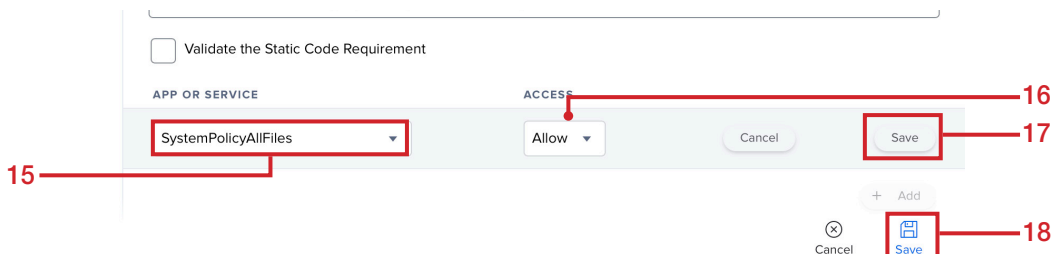


15. Choose SystemPolicyAllFiles.

16. Select Allow for Access.

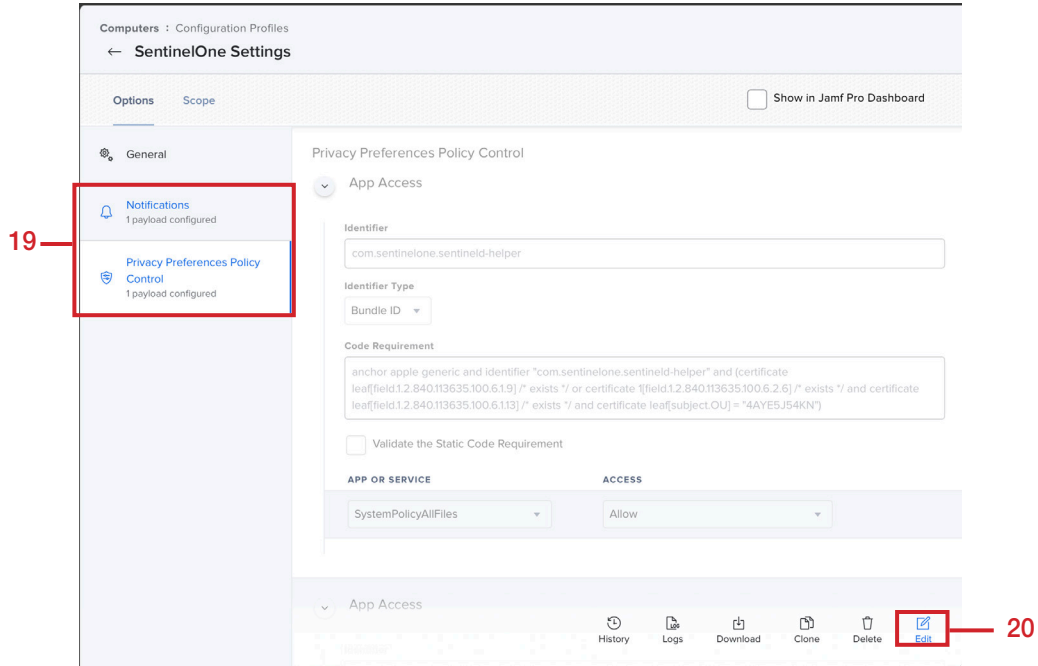
17. Click Save for the configuration.

18. Click Save to save the profile.

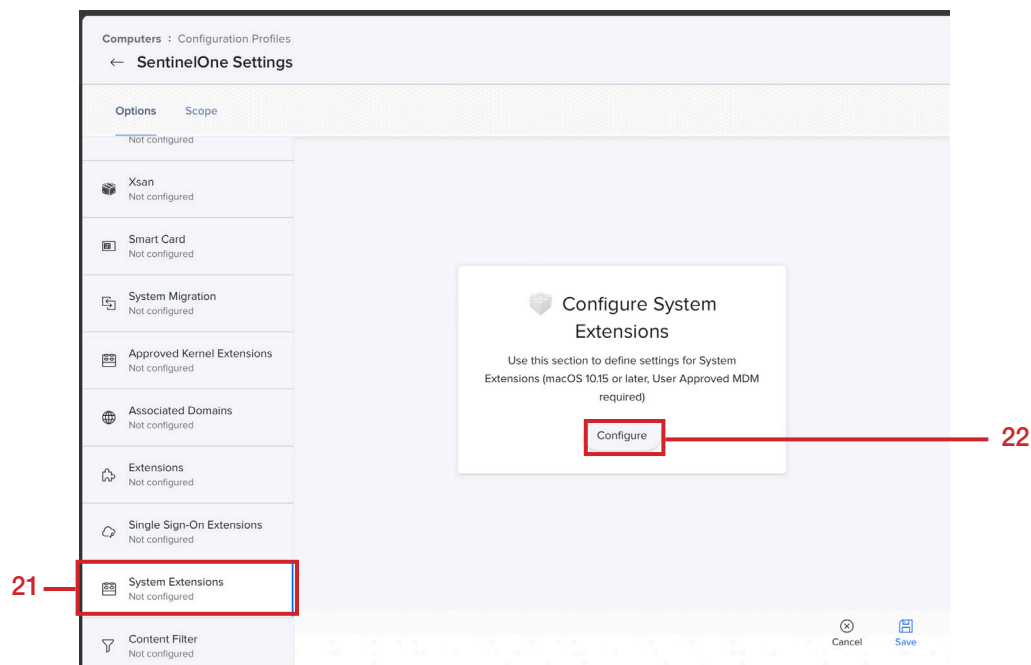




- 19. Confirm You have two payloads configured.
- 20. Click Edit.



- 21. Scroll down and click System Extensions.
- 22. Click Configure.





- 23. Configure the payload with the following:
 - A. Display Name, enter: **SentinelOne Network Monitoring Extension**
 - B. System Extension Types, select: Allowed System Extensions
 - C. Team Identifier, enter: **4AYE5J54KN**
 - D. Click Add (+)

Computers : Configuration Profiles
← SentinelOne Settings

Options Scope

Xsan Not configured

Smart Card Not configured

System Migration Not configured

Approved Kernel Extensions Not configured

Associated Domains Not configured

Extensions Not configured

Single Sign-On Extensions

System Extensions

Allow users to approve system extensions

Allowed Team IDs and System Extensions

Display Name
SentinelOne Network Monitoring Extension

System Extension Types
Allowed System Extensions

Team Identifier
4AYE5J54KN

ALLOWED SYSTEM EXTENSIONS

+ Add

- 24. Enter **com.sentinelone.network-monitoring**.
- 25. Click Save to save the configuration.

Team Identifier
4AYE5J54KN

ALLOWED SYSTEM EXTENSIONS

com.sentinelone.network-monitoring

Cancel Save

+ Add

- 26. Click Content Filter.

Associated Domains Not configured

Extensions Not configured

Single Sign-On Extensions Not configured

System Extensions 1 payload configured

Content Filter Not configured

Team Identifier
4AYE5J54KN

ALLOWED SYSTEM EXTENSIONS

com.sentinelone.network-monitoring

Edit Delete

+ Add

Cancel Save



- 27. Configure the payload with the following:
 - A. Filter Name, enter: **SentinelOne Extensions**
 - B. Identifier, enter: **com.sentinelone.extensions-wrapper**

- 28. Scroll down and continue to configure the payload with the following:
 - A. Enable Filter Order
 - B. Confirm Firewall is selected.
 - C. Socket Filter Bundle Identifier, enter: **com.sentinelone.network-monitoring**
 - D. Socket Filter Designated Requirement, enter:
anchor apple generic and identifier "com.sentinelone.network-monitoring" and (certificate leaf[field.1.2.840.113635.100.6.1.9] or certificate 1[field.1.2.840.113635.100.6.2.6] and certificate leaf[field.1.2.840.113635.100.6.1.13] and certificate leaf[subject.OU] = "4AYE5J54KN")
 - E. Click Scope.



29. Scope to your needs. In this example, we are scoping to All Computers.

30. Click Save to save the profile.

31. Click Previous (←)

Computers : Configuration Profiles

← SentinelOne Settings

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

32. Click New (+).

Computers Configuration Profiles

Filter Pr 1 - 32 of 32

+ New Upload

NAME	LOGS	COMPLETED	PENDING	FAILED	SCOPE
------	------	-----------	---------	--------	-------

33. Configure the profile with the following:

A. Name: **SentinelOne Managed Login Items**

B. Enter a description

C. Select a category

D. Level is set to Computer Level

E. Distribution Method is set to Install Automatically.

General

Name Display name of the profile
SentinelOne Managed Login Items A

Description Brief explanation of the content or purpose of the profile
B

Category Category to add the profile to
C Security

Level Level at which to apply the profile
D Computer Level

Distribution Method Method to use for distributing the profile
E Install Automatically



- 34. Scroll to the Managed Login Items payload.
- 35. Configure the following payload:
 - A. Enable the Managed Login Item rule,
 - B. Select Label Prefix from the Rule Type menu
 - C. Rule Value, enter: **com.sentinelone.**
NOTE: include the trailing period
 - D. add a Rule Comment if desired
- 36. Click Add (+).

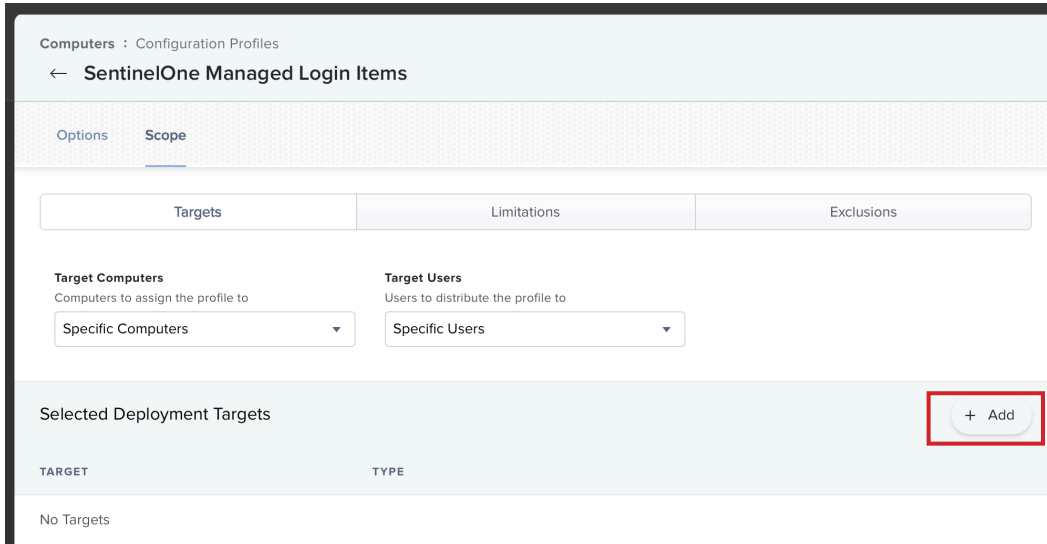
- 37. Configure the following:
 - A. Select Bundle Identifier Prefix from the Rule Type menu.
 - B. Rule Value, enter: **com.sentinelone.**
NOTE: include the trailing period
 - C. add a Rule Comment if desired
- 38. Click Scope.



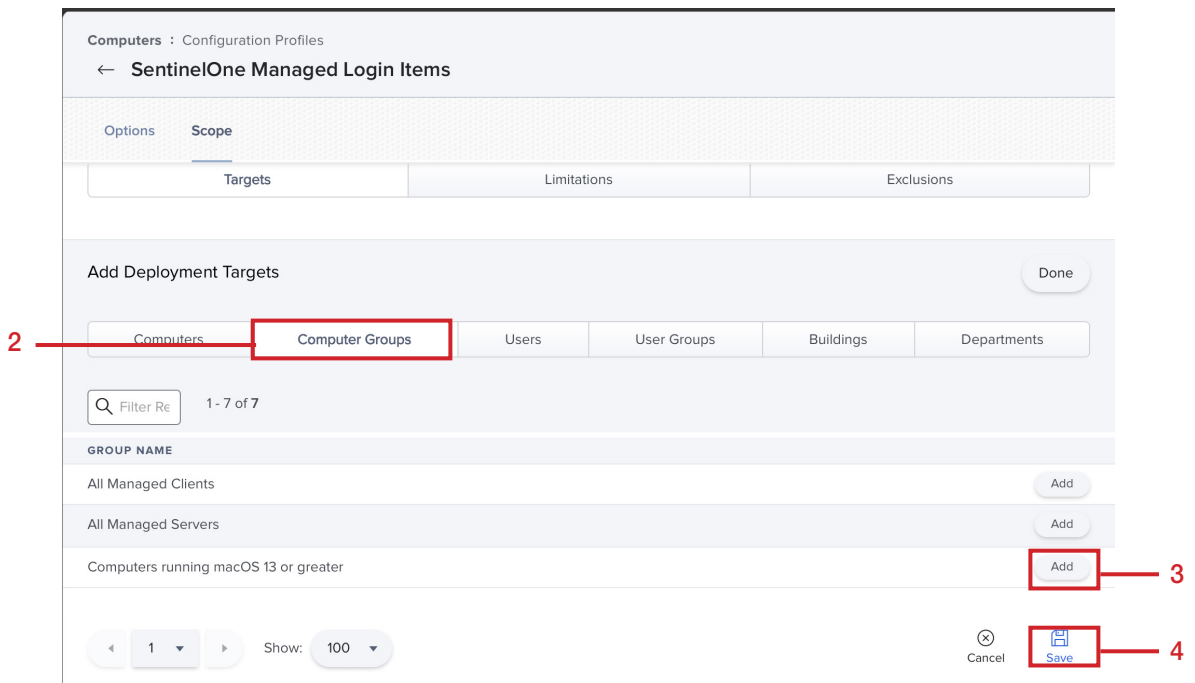
Section 4: Policies

Create a policy to deploy SentinelOne

1. Click Add (+).



2. Click Computer Groups.
3. Click Add for Computers running macOS 13 or greater.
4. Click Save.





5. If you are using Automated Device Enrollment, make sure that the SentinelOne configuration profiles are installed during the setup assistant.

Computers : PreStage Enrollments
← HCS Computers

Options Scope

General
Account Settings
Configuration Profiles 0 Profiles
User and Location
Purchasing
Attachments 0 Attachments

Configuration Profiles

CONFIGURATION PROFILE SCOPE
To ensure the selected configuration profiles remain installed on computers after enrollment, ensure the scope of the configuration profile includes the computers in the scope of the PreStage enrollment.

	NAME	SCOPE
Security		
<input checked="" type="checkbox"/>	SentinelOne Managed Login Items	Computers running macOS 13 or greater
<input checked="" type="checkbox"/>	SentinelOne Settings	All computers

6. Click Computers.
7. Click Policies.
8. Click New (+).

jamf PRO

Computers Policies

Filter Pc 1 - 47 of 47 + New

NAME	FREQUENCY	TRIGGER	SCOPE
------	-----------	---------	-------



- 9. Configure the policy with the following:
 - A. Name the policy. For the purposes of this guide, we have named it **Deploy SentinelOne 22-4-1-6538**
 - B. Select a Category
 - C. Set Trigger to Recurring Check-In
 - D. Set Execution Frequency to Once per computer
 - E. Select the checkbox for Automatically re-run policy on failure.
 - F. Click Packages

The screenshot shows the 'New Policy' configuration page in Jamf Pro. The left sidebar lists various policy categories, with 'Packages' highlighted by a red box and labeled 'F'. The main configuration area is titled 'General' and contains the following settings:

- Display Name:** Deploy SentinelOne 22-4-1-6538 (labeled 'A')
- Enabled:**
- Category:** Security (labeled 'B')
- Trigger:** Recurring Check-in (checked, labeled 'C'). Other options include Startup, Login, Network State Change, and Enrollment Complete.
- Execution Frequency:** Once per computer (labeled 'D')
- Automatically re-run policy on failure:** (labeled 'E')
- Retry Event:** On next recurring check-in
- Retry Attempts:** 3
- Send notifications for each failed policy retry:**



10. Click Configure.

The screenshot shows the Jamf Pro configuration interface. On the left, there is a sidebar with menu items: General, Packages (0 Packages), Software Updates (Not Configured), Scripts (0 Scripts), Printers (0 Printers), Disk Encryption (Not Configured), and Dock Items (0 Dock Items). The main content area is titled 'Configure Packages' and contains the following text: 'Use this section to install, cache, and uninstall packages. Also use this section to install a single cached package.' Below this text is a button labeled 'Configure', which is highlighted with a red rectangular box.

11. Add the SentinelOne package.

The screenshot shows the 'Deploy SentinelOne 22-4-1-6538' configuration page. The left sidebar is the same as in the previous screenshot. The main content area shows a table with the following data:

NAME	CATEGORY
Sentinel-Release-22-4-1-6538_macos_v22_4_1_6538.pkg	Security

An 'Add' button is located to the right of the table, highlighted with a red rectangular box.

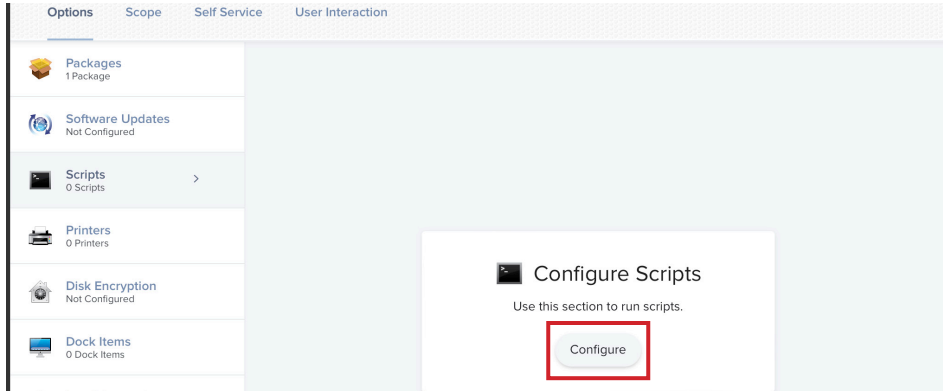
12. Click Scripts.

The screenshot shows the 'Deploy SentinelOne 22-4-1-6538' configuration page. The left sidebar is the same as in the previous screenshot. The main content area shows the configuration for the package 'Sentinel-Release-22-4-1-6538_macos_v22_4_1_6538.pkg'. The 'Scripts' menu item in the sidebar is highlighted with a red rectangular box. The configuration details for the package are as follows:

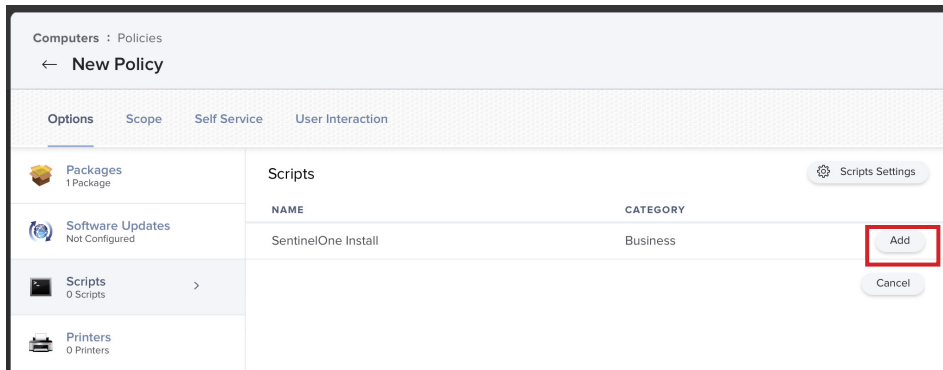
- Distribution Point:** Each computer's default distribution point
- Action:** Cache



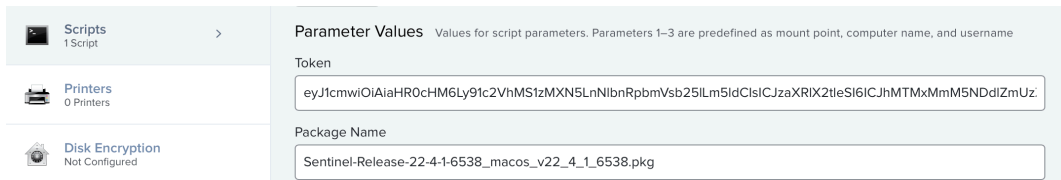
13. Click Configure.



14. Add the SentinelOne Install script.



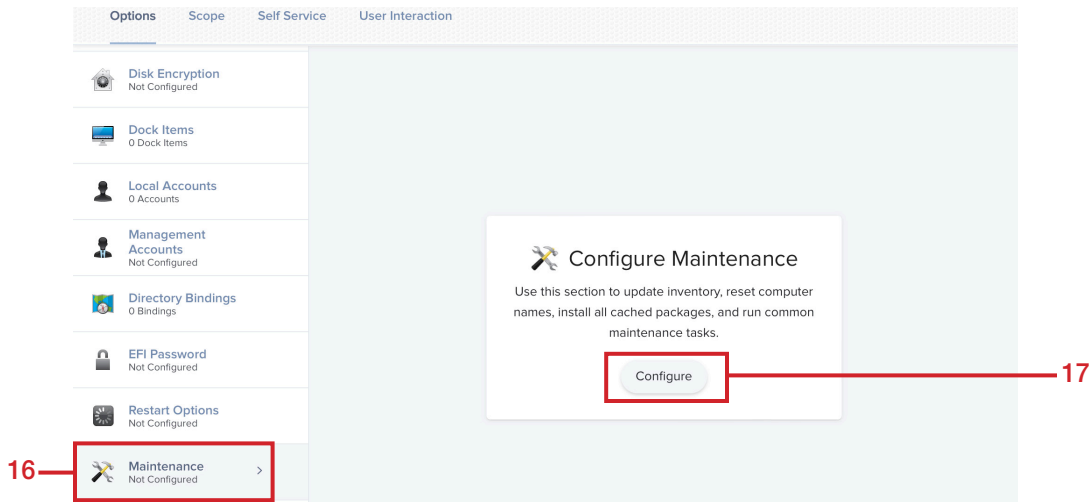
15. Enter your organization token in the parameter labeled Token and the name of the Package in the Package Name parameter.





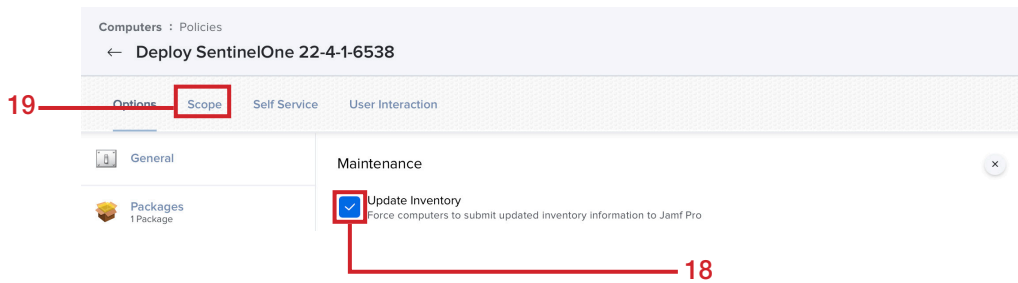
16. Click Maintenance.

17. Click Configure.

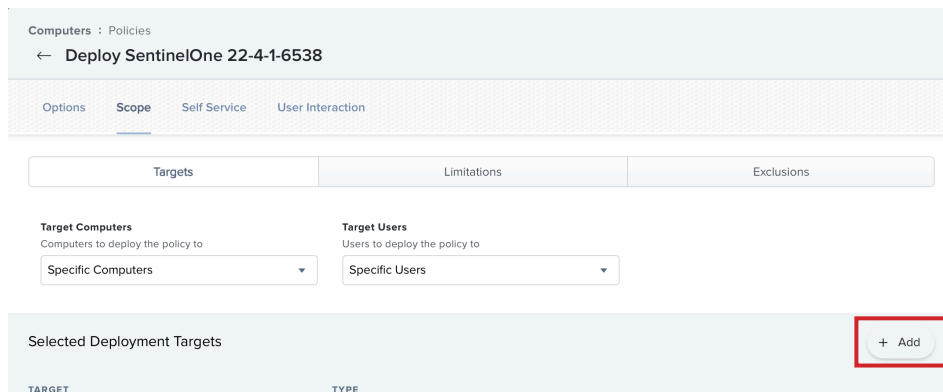


18. Confirm the checkbox for Update Inventory is selected.

19. Click Scope.



20. Click Add (+).





21. Click Computer Groups.
22. Click Add for Computers without SentinelOne.
23. Click Save.

Computers : Policies
← Deploy SentinelOne 22-4-1-6538

Options Scope Self Service User Interaction

Targets Limitations Exclusions

Add Deployment Targets Done

Computers Computer Groups Users User Groups Buildings Departments

Filter Re: 1 - 6 of 6

GROUP NAME	Add
All Managed Clients	Add
All Managed Servers	Add
Computers without SentinelOne	Add
Computers running macOS 13 or greater	Add

1 Show: 100

Cancel Save

This completes this guide.