How to Install SentinelOne with Jamf Pro

Contents

Preface

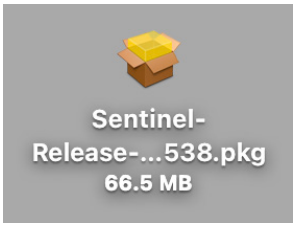
What is SentinalOne?
SentinelOne protects your computer and data with anti-malware and anti-exploit protection. The SentinelOne agent continually receives intelligence updates from SentinelOne servers. The agent is very lightweight on resources and offers minimal to no impact on work.

This guide was written using the following:
1. macOS Ventura 13.2
2. Jamf Pro 10.43
3. SentinelOne

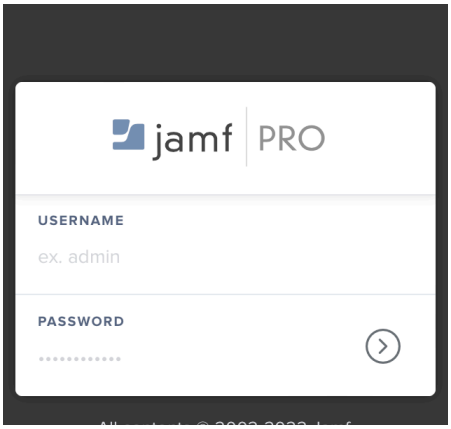
Section 1: Packages and Scripts

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

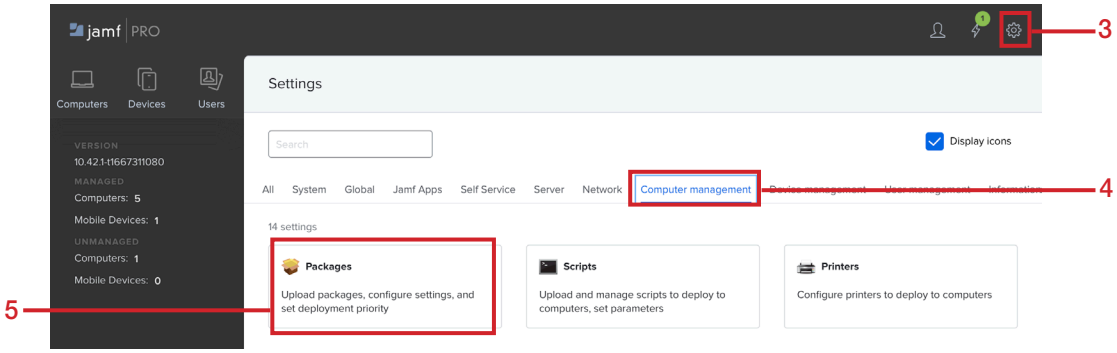
1. Acquire the SentinelOne package and your organization token from the SentinelOne console.



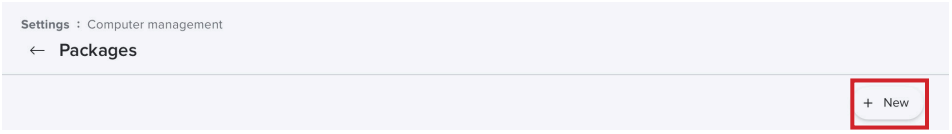
2. Log into your Jamf Pro server.



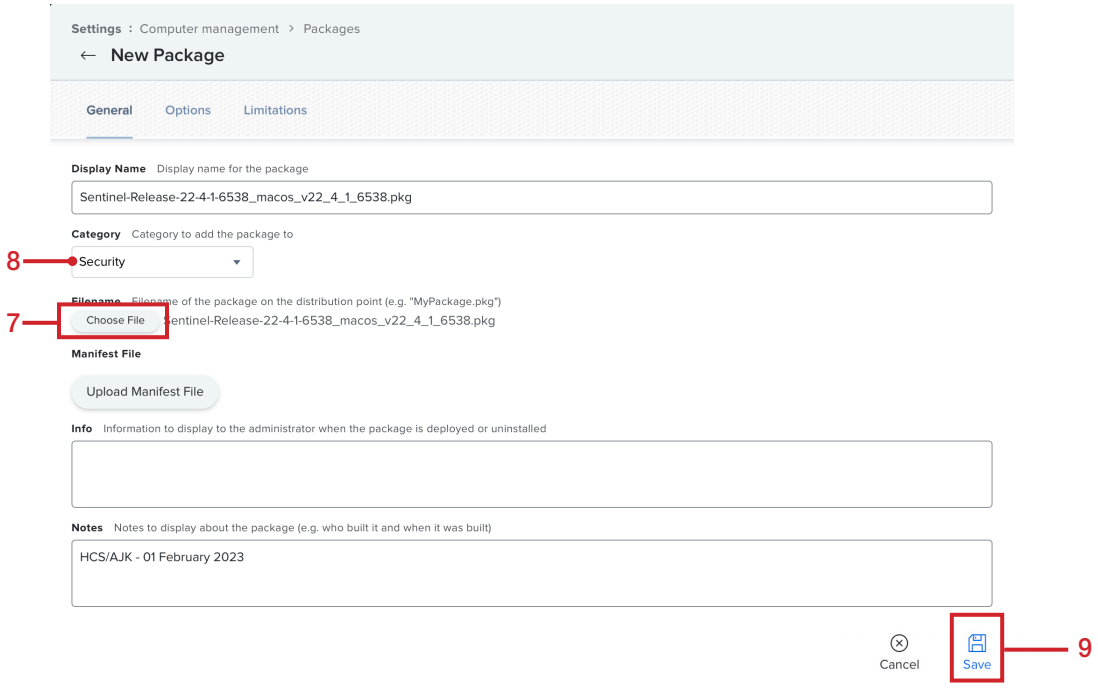
3. In Jamf Pro, Click Settings (⚙).
4. Click Computer management.
5. Click Packages.



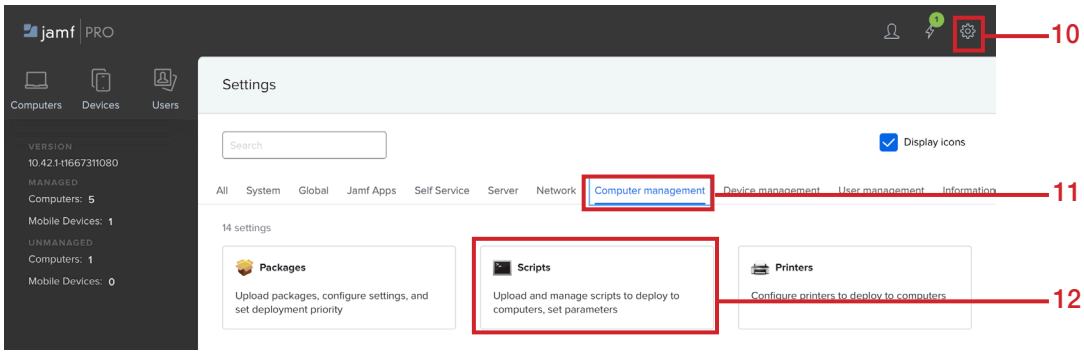
6. Click New (+).



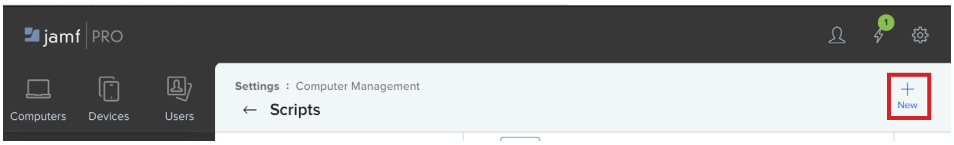
7. Click Choose File and select your SentinelOne package.
8. Select a category and add notes if desired.
9. Once you are ready to upload the package, click Save.



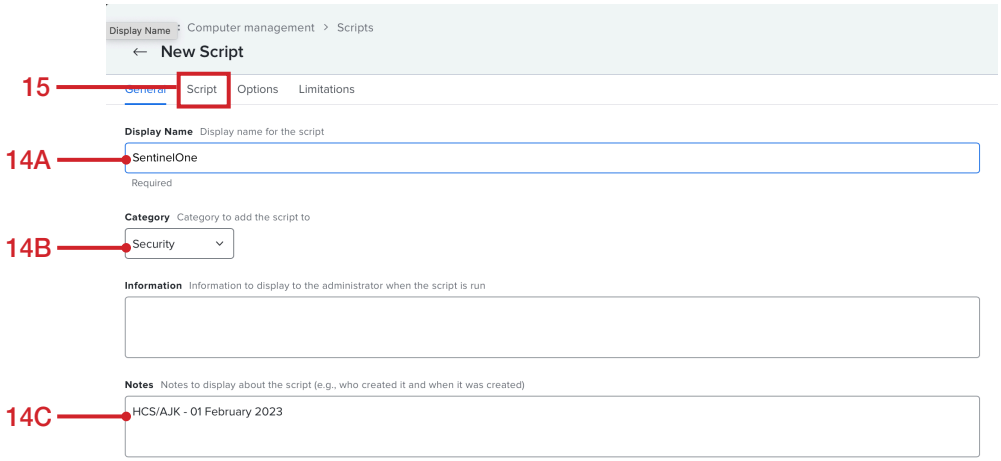
10. Click Settings (⚙).
11. Click Computer management.
12. Click Scripts.



13. Click New (+).



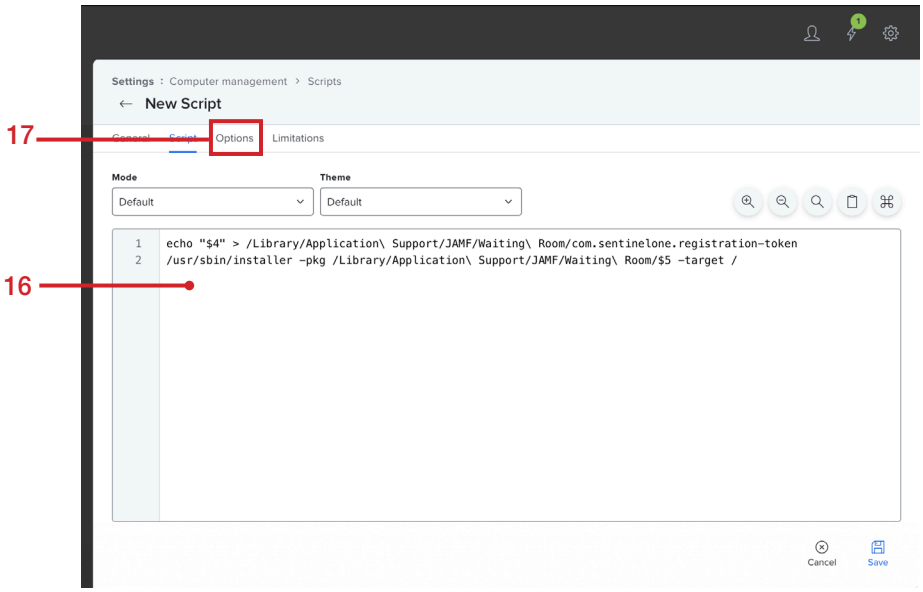
14. Configure the following:
    A. Display Name: **SentinelOne**
    B. Select a category
    C. Add notes if desired.
15. Click Script.



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 /
```

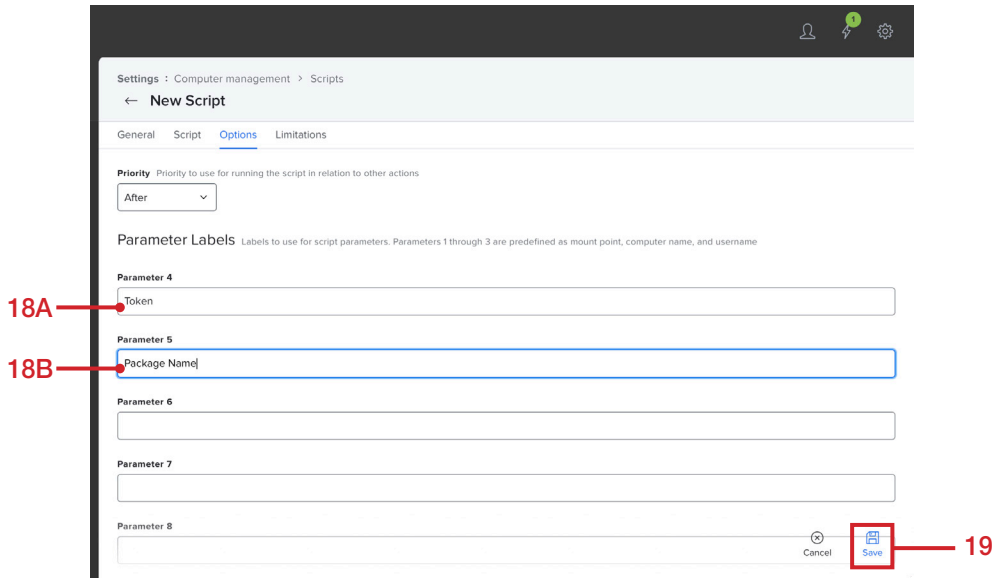
17. Click Options.



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.

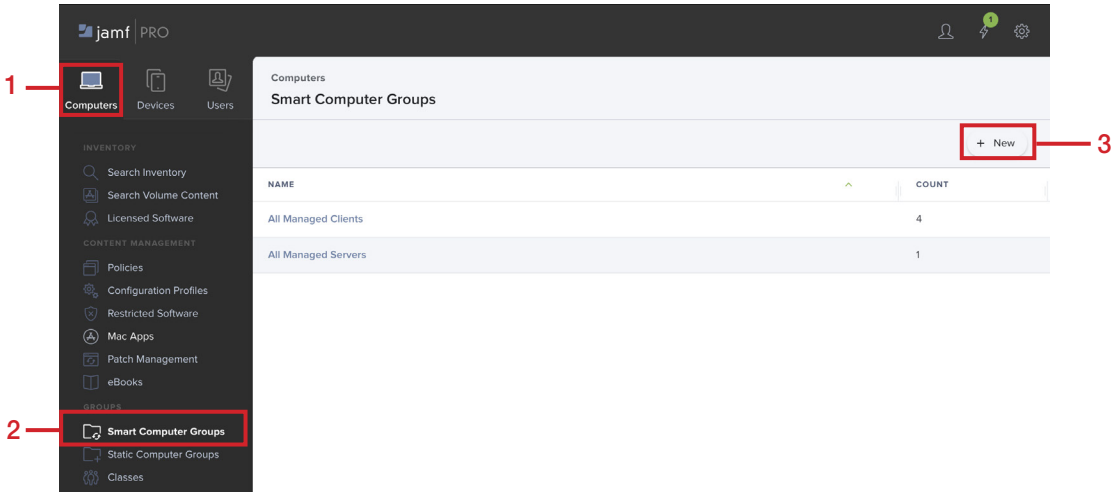
19. Click Save.



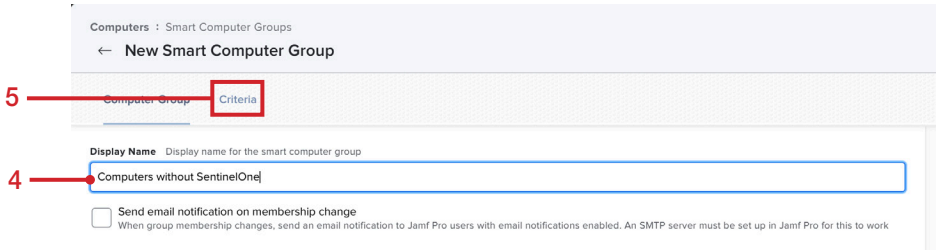
Section 2: Create Smart Computer Groups

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

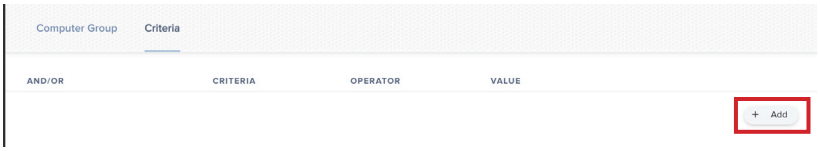
1. Click Computers.
2. Click Smart Computer Groups.
3. Click New.



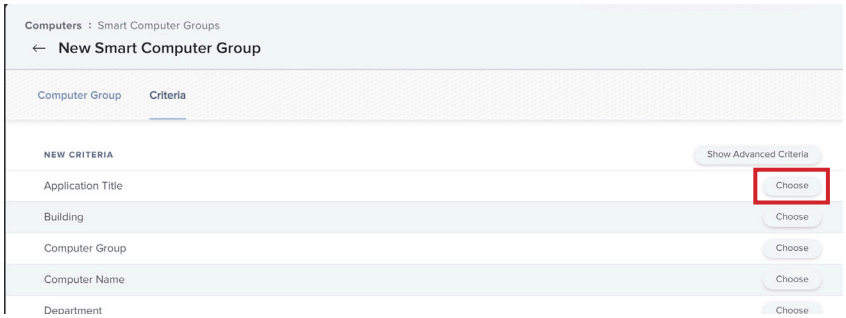
4. For the Display name, enter **Computers without SentinelOne**.
5. Click Criteria.



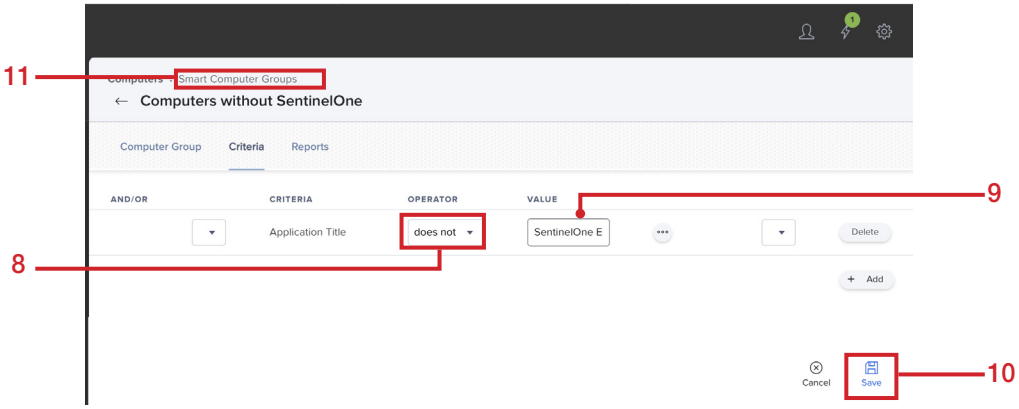
6. Click Add (+).



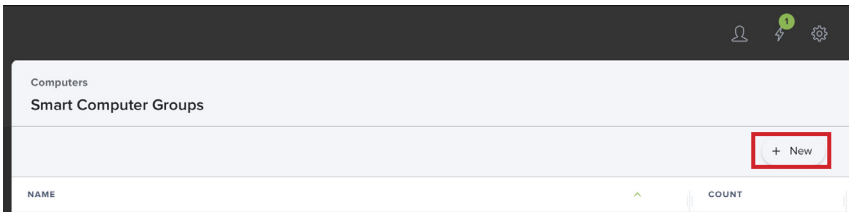
7. Choose Application Title.



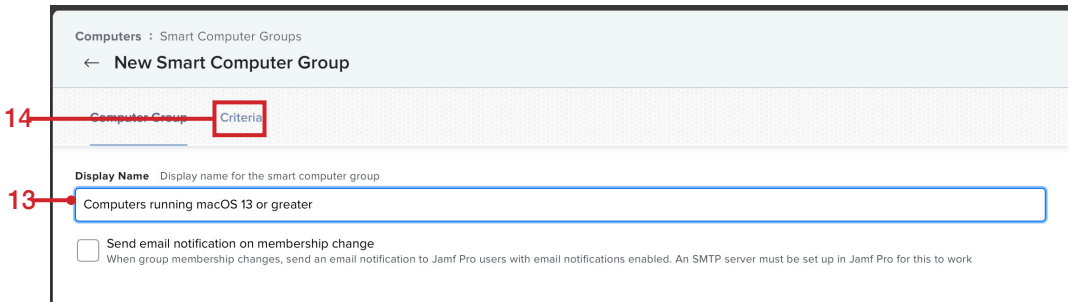
8. Change the operator to "does not have".
9. Enter the Value **SentinelOne Extensions.app**.
10. Click Save.
11. Click Smart Computer Groups.



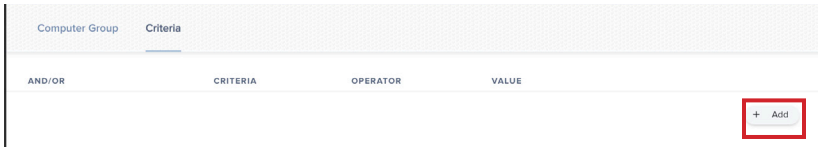
12. Click New.



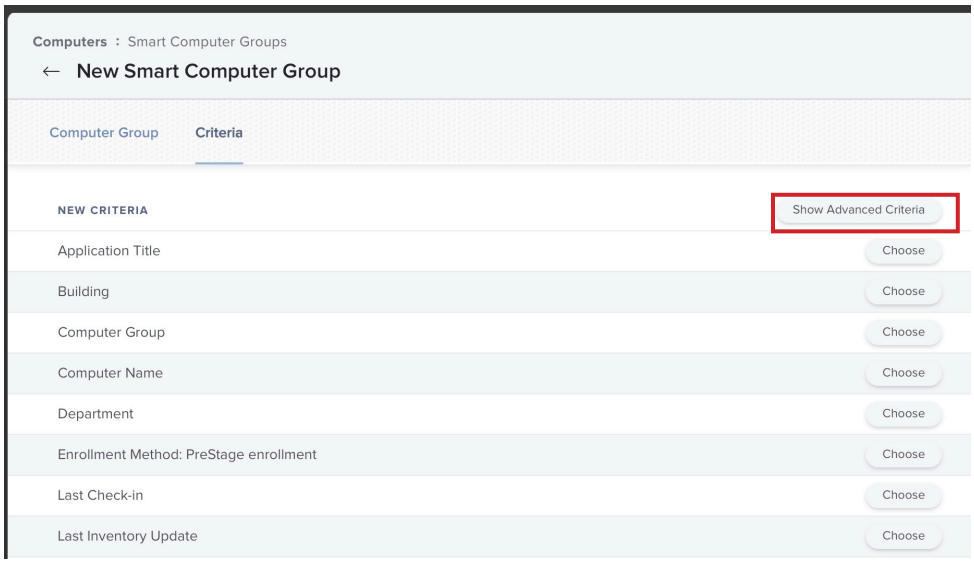
13. For the Display name, enter **Computers running macOS 13 or greater**.
14. Click Criteria.



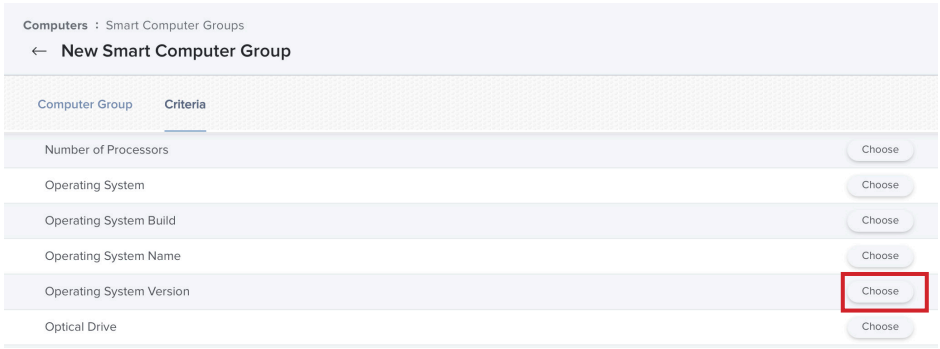
15. Click Add (+).



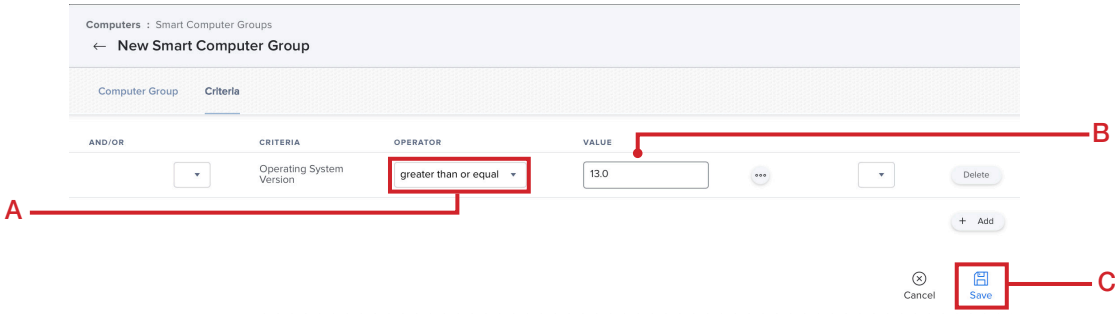
16. Click Show Advanced Criteria.



17. Scroll down, choose Operating System Version



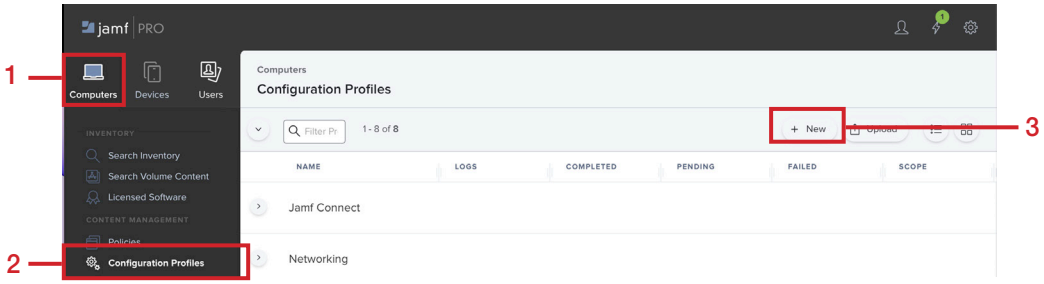
18. Configure the following:
    A. Change the operator to “greater than or equal”
    B. Value: **13.0**
    C. Click Save



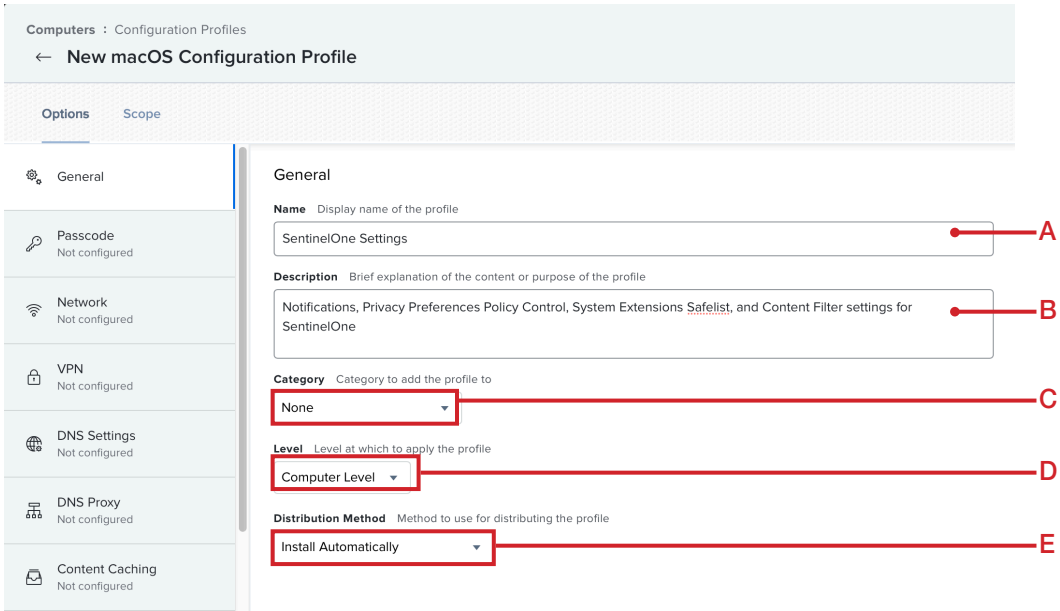
Section 3: Configuration Profiles

Create Configuration Profiles to ensure SentinelOne installs and operates properly.

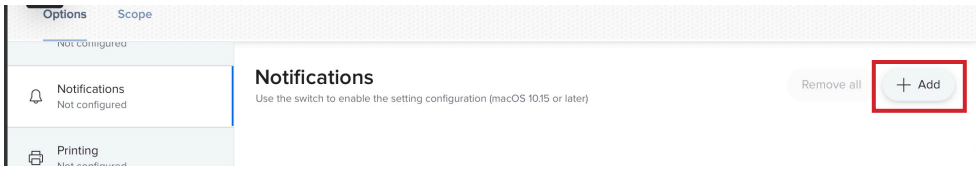
1. Click Computers.
2. Click Configuration Profiles.
3. Click New (+).



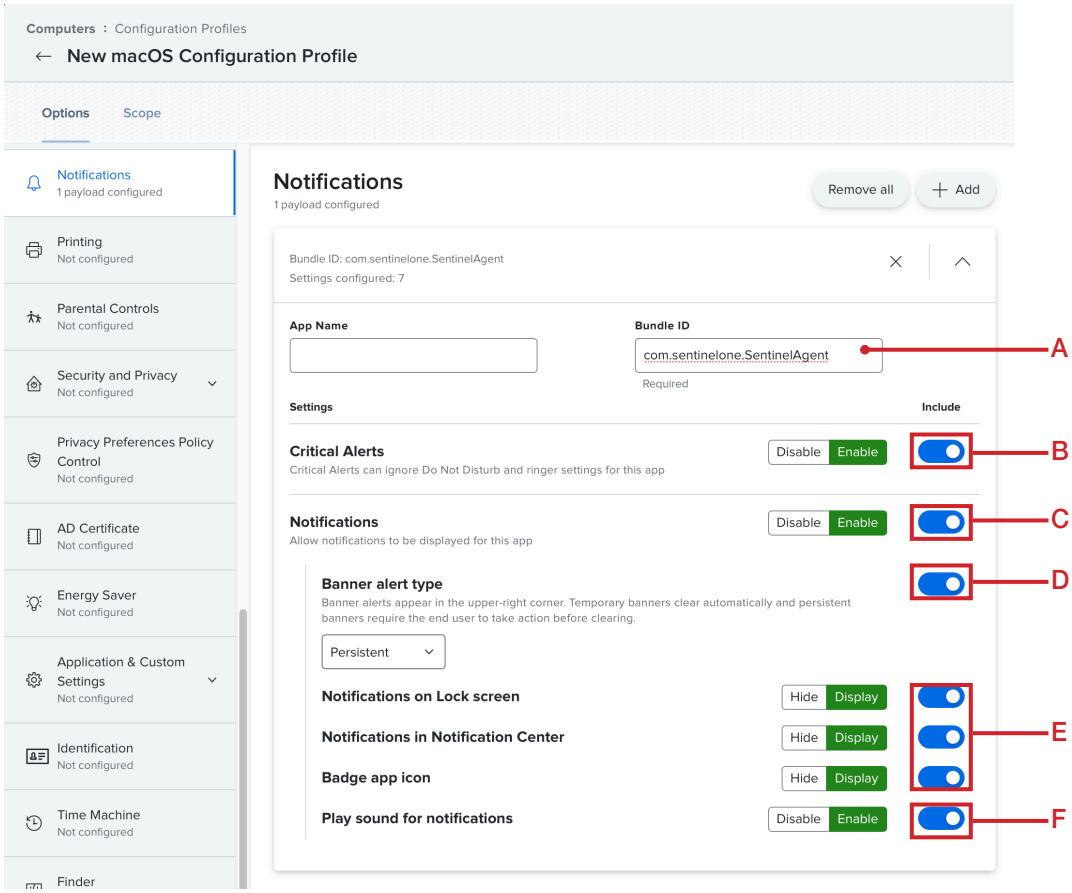
4. Configure the profile with the following:
   A. Name: **SentinelOne Settings**
   B. Enter a description
   C. Select a category
   D. Level is set to Computer Level
   E. Distribution Method is set to Install Automatically.



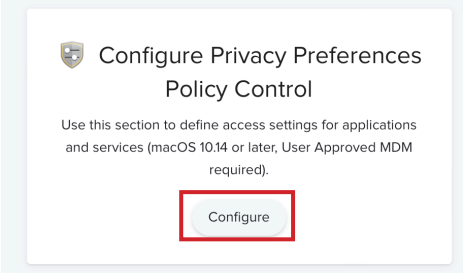
5. Scroll to the Notifications payload.
6. Click Add (+).



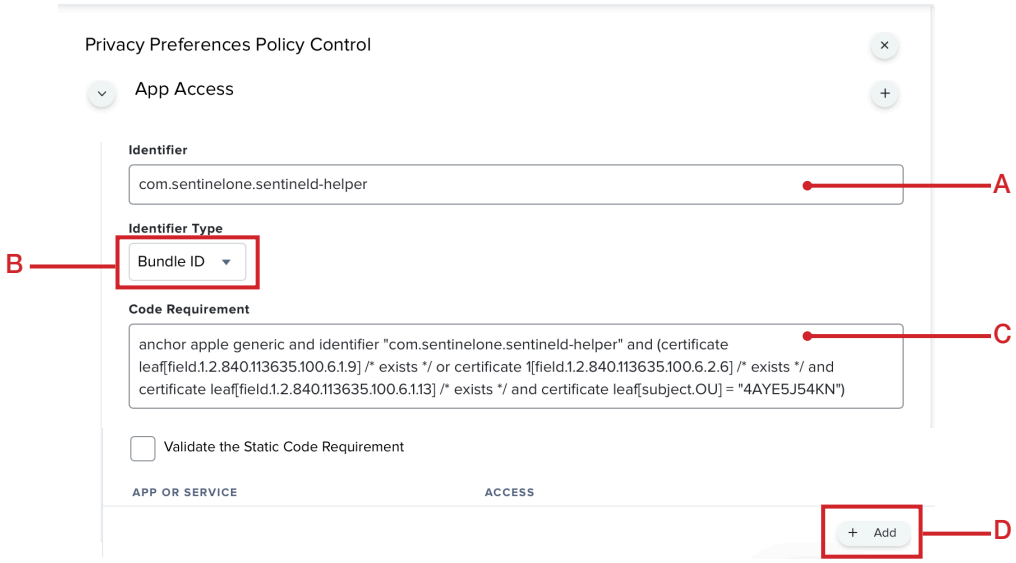
7. Configure the payload with the following:
   A. Enter the Bundle ID: **com.sentinelone.SentinelAgent**
   B. Enable Critical Alerts
   C. Enable Notifications
   D. Banner alert type, set to Persistent
   E. Select Display for:
      - Notifications on Lock Screen
      - Notifications in Notification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



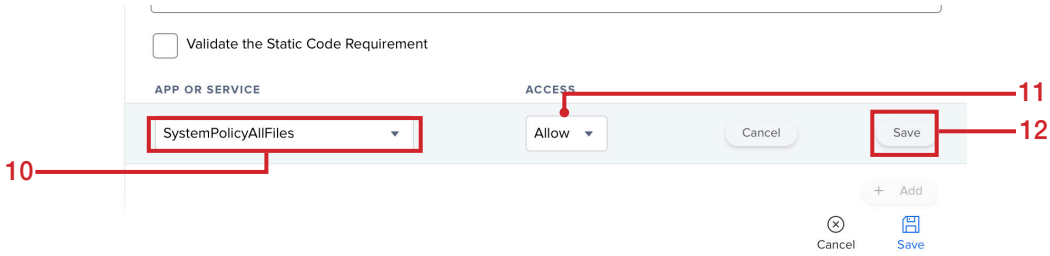
8. Click Configure.



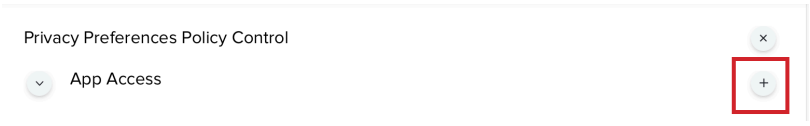
9. Configure the payload with the following:
   A. Identifier: **com.sentinelone.sentineld-helper.**
   B. Identifier Type: select Bundle ID.
   C. Code Requirement, enter the following:
   anchor apple generic and identifier "com.sentinelone.sentineld-helper" and (certificate leaf[field.1.2.840.113635.100.6.1.9] /* 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")
   D. Click Add (+).



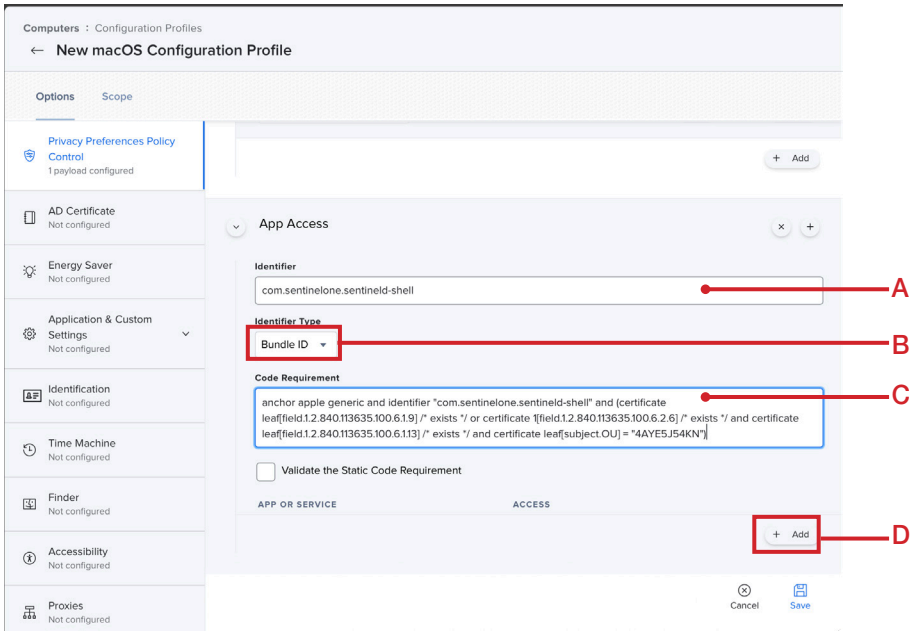
10. Choose SystemPolicyAllFiles.
11. Select Allow for Access.
12. Click Save.



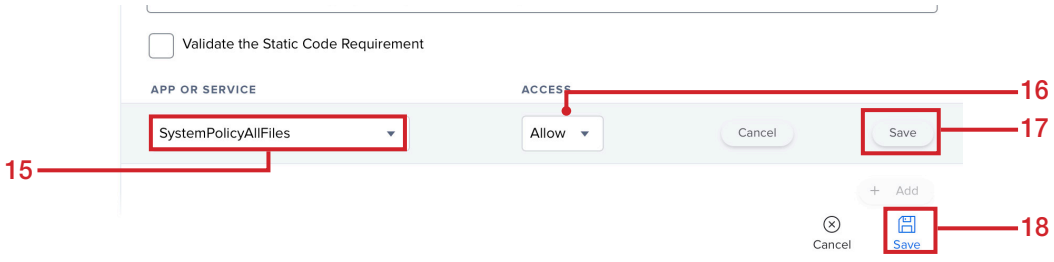
13. Click Add (+) to add another App Access.



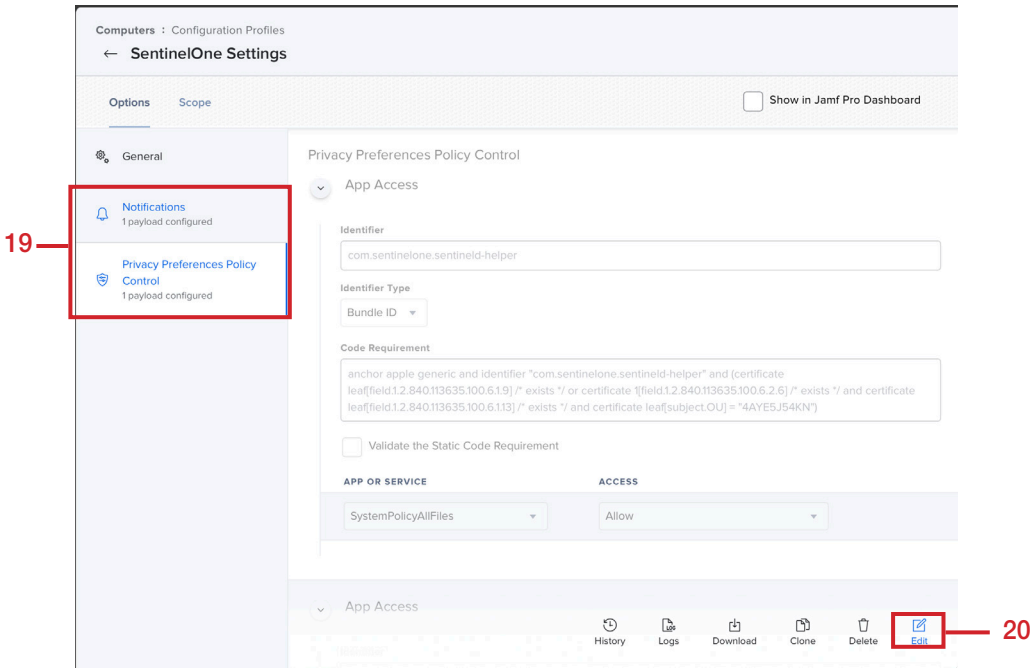
14. Scroll down and configure the following:
    A. Identifier: **com.sentinelone.sentineld-shell**
    B. Identifier Type: select Bundle ID
    C. Code Requirement, enter the following:
    anchor apple generic and identifier "com.sentinelone.sentineld-shell" and (certificate leaf[field.1.2.840.113635.100.6.1.9] /* 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 (+).



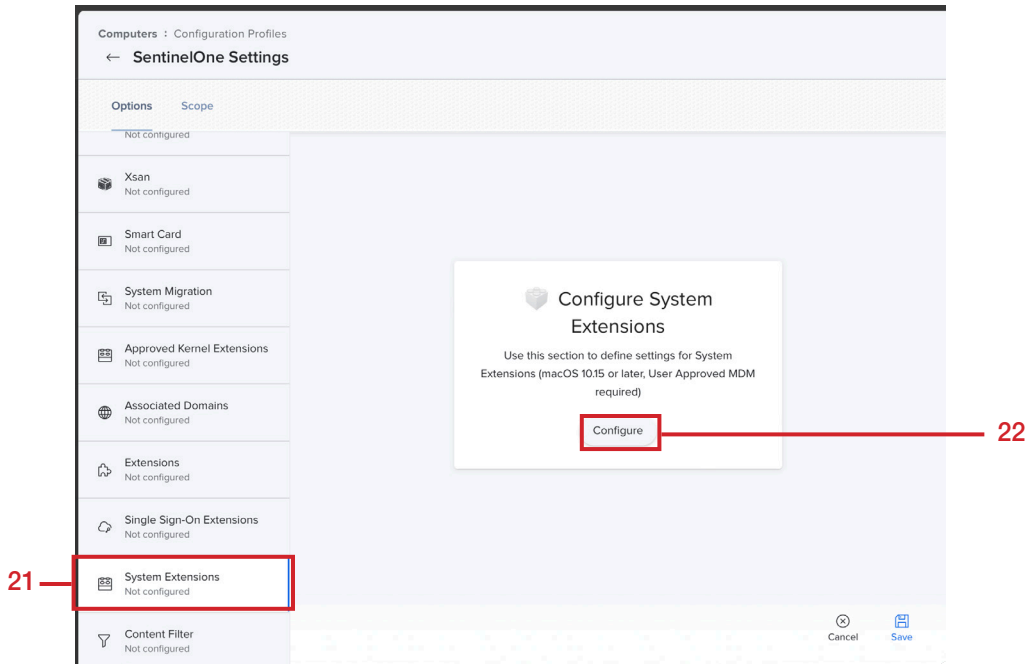
15. Choose SystemPolicyAllFiles.
16. Select Allow for Access.
17. Click Save for the configuration.
18. Click Save to save the profile.



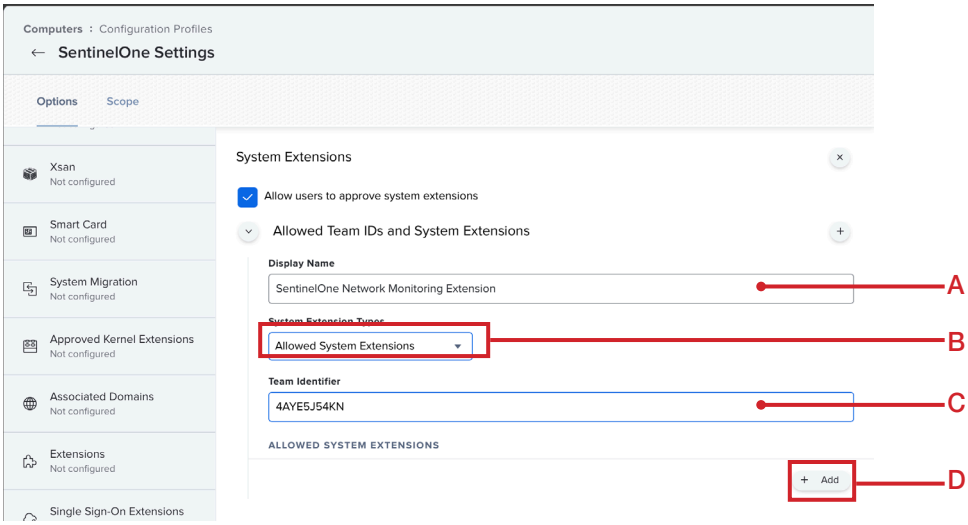
19. Confirm You have two payloads configured.
20. Click Edit.



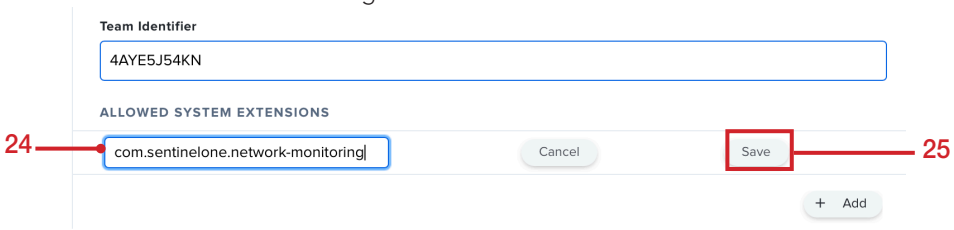
21. Scroll down and click System Extensions.
22. Click Configure.



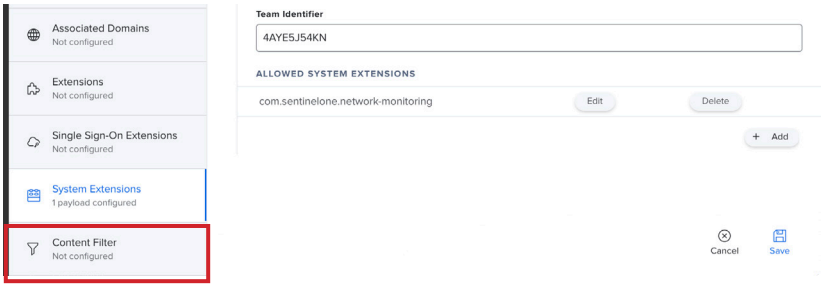
23. Configure the payload with the following:
    A. Display Name, enter: **SentinelOne Network Monitoring Extension**
    B. System Extension Types, select: Allowed System Extensions
    C. Team Identifier, enter: **4AYE5J54KN**
    D. Click Add (+)



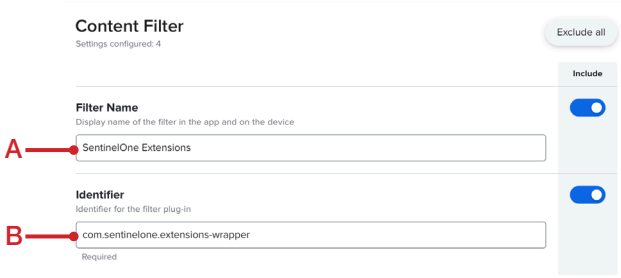
24. Enter **com.sentinelone.network-monitoring**.
25. Click Save to save the configuration.



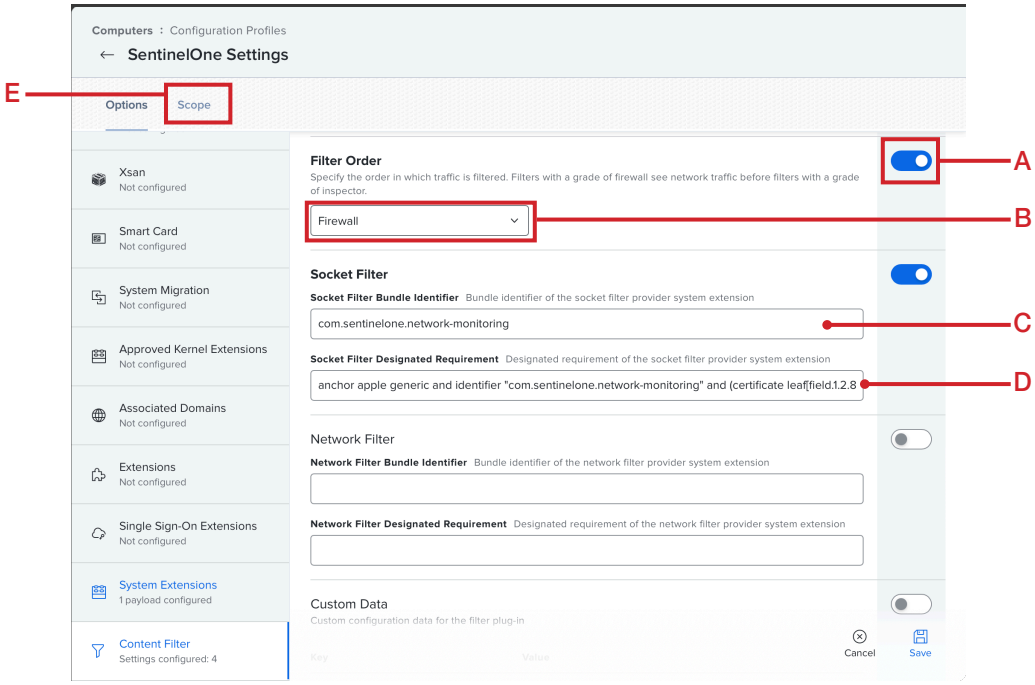
26. Click Content Filter.



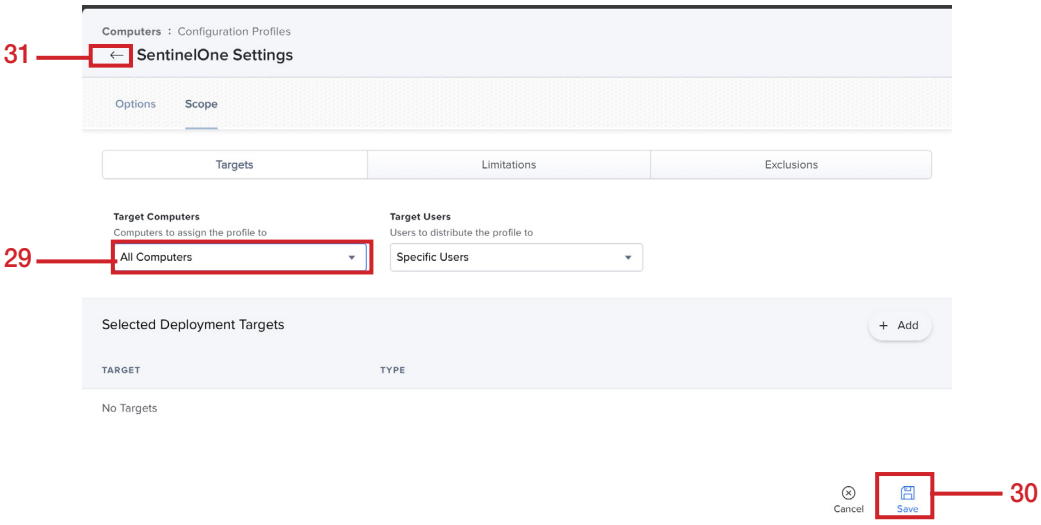
27. Configure the payload with the following:
    A. Filter Name, enter: **SentinelOne Extensions**
    B. Identifier, enter: **com.sentinelone.extensions-wrapper**



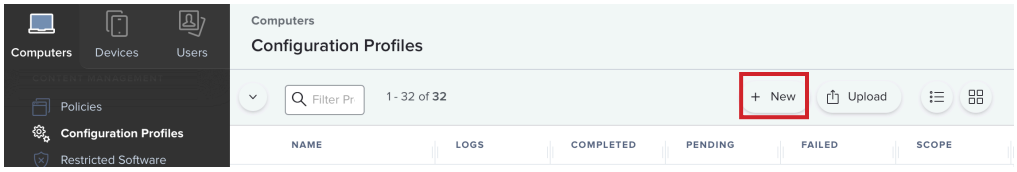
28. Scroll down and continue to configure the payload with the following:
    A. Enable Filter Order
    B. Confirm Firewall is selected.
    C. Socket Filter Bundle Identifier, enter: **com.sentinelone.network-monitoring**
    D. Socket Filter Designated Requirement, enter:
    anchor apple generic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



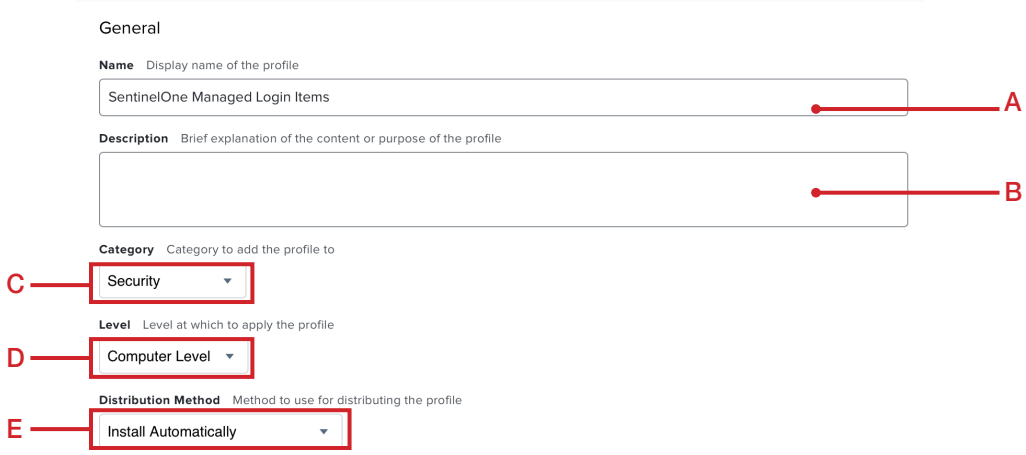
29. Scope to your needs. In this example, we are scoping to All Computers.
30. Click Save to save the profile.
31. Click Previous (←)



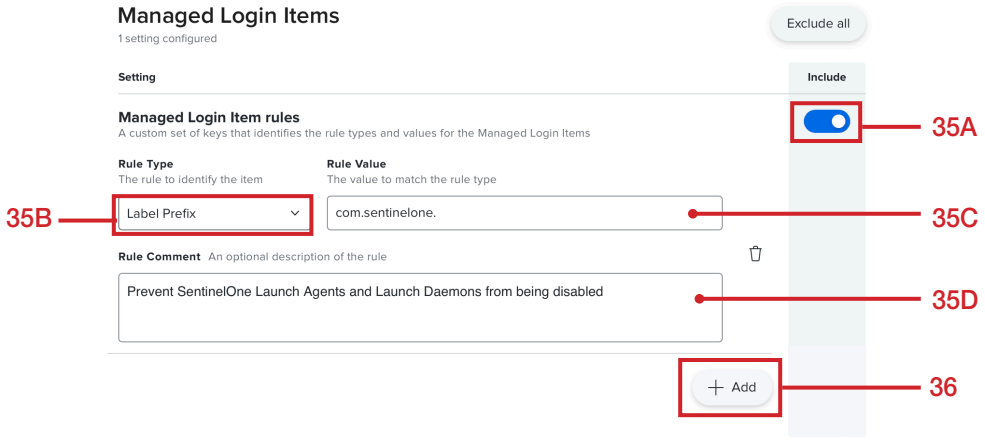
32. Click New (+).



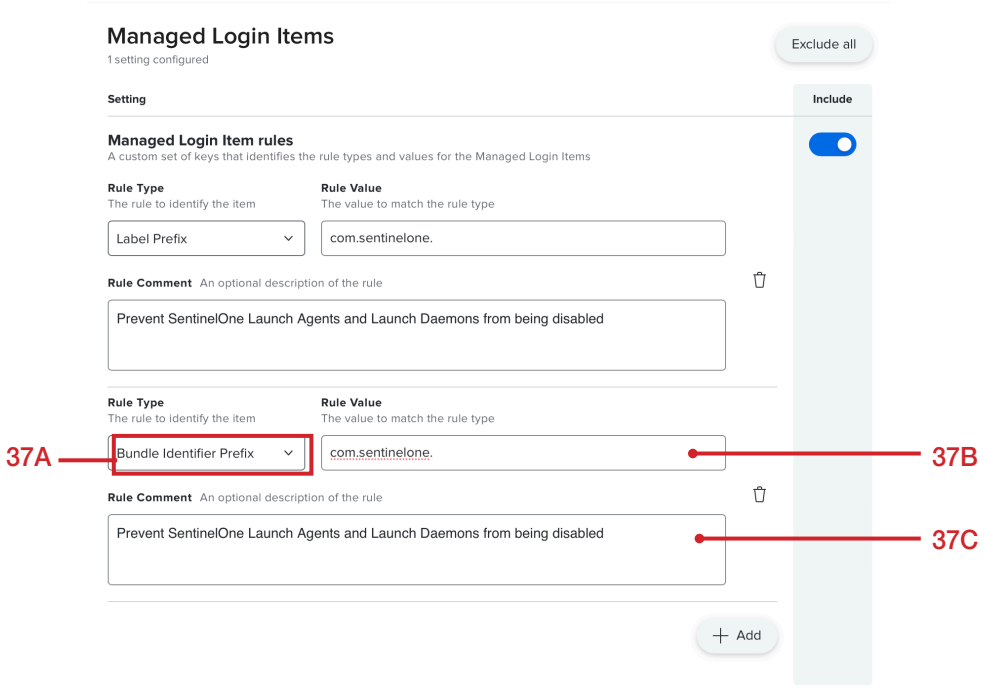
33. Configure the profile with the following:
    A. Name: **SentinelOne Managed Login Items**
    B. Enter a description
    C. Select a category
    D. Level is set to Computer Level
    E. Distribution Method is set to Install Automatically.



34. Scroll to the Managed Login Items payload.
35. Configure the following payload:
    A. Enable the Managed Login Item rile,
    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 (+).



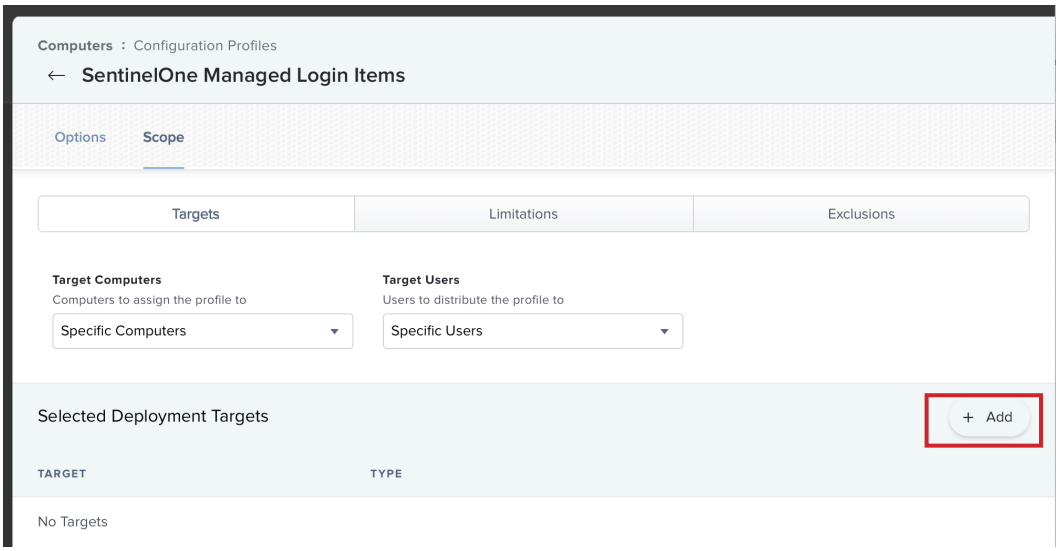
37. Configure the following:
    A. Select Bundle Identifier Prefix from the Rule Type menu.
    B. Rule Value, enter: **com.sentinelone.**
       NOTE: include the trailing period
    C. add a Rule Comment if desired
38. Click Scope.



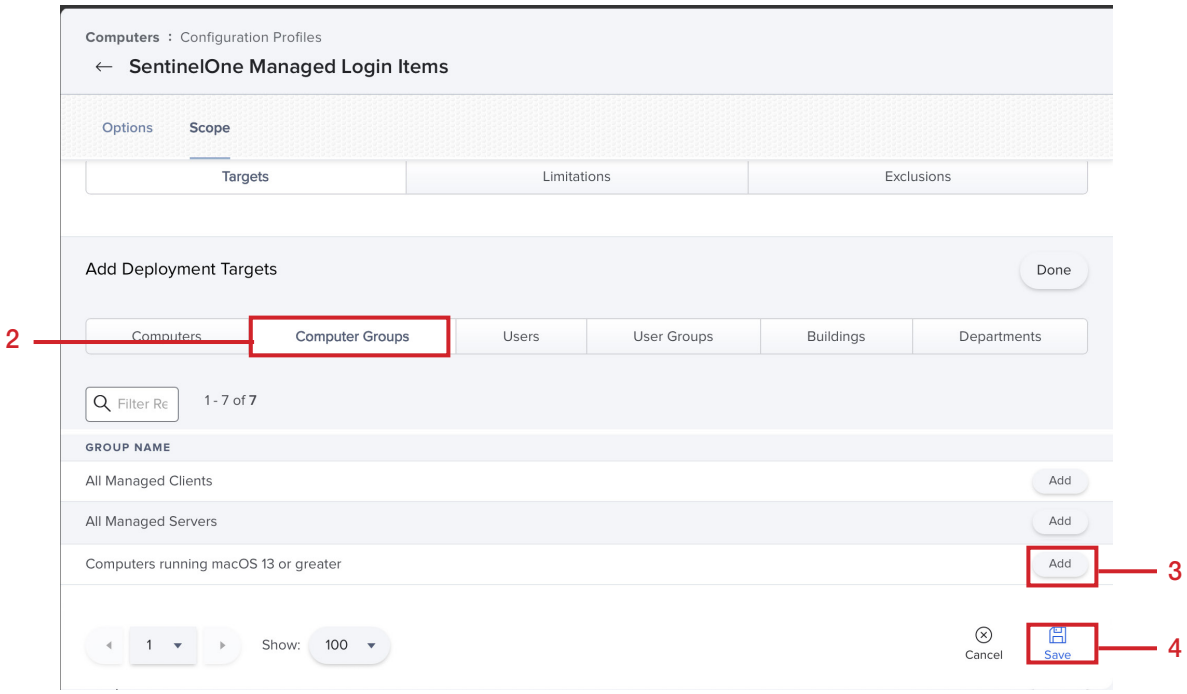
Section 4: Policies

Create a policy to deploy SentinelOne

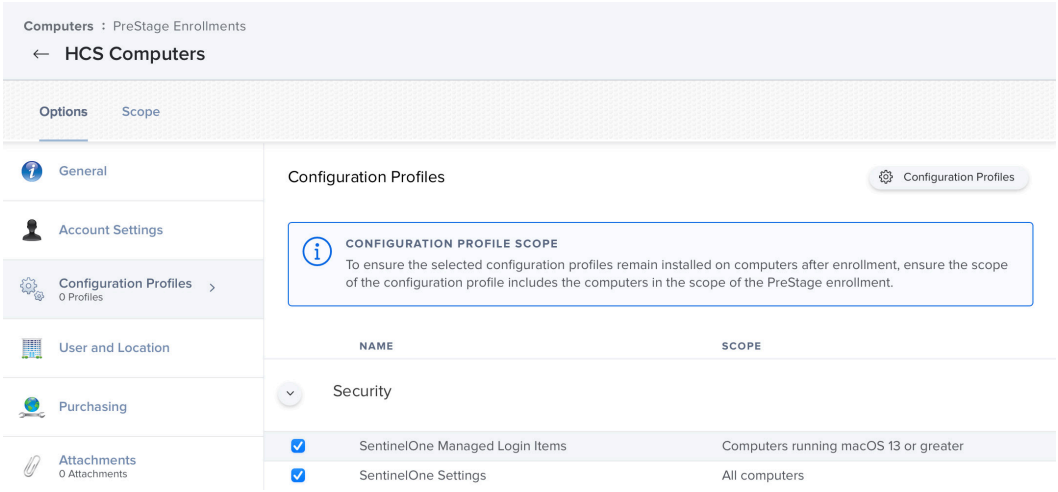
1. Click Add (+).



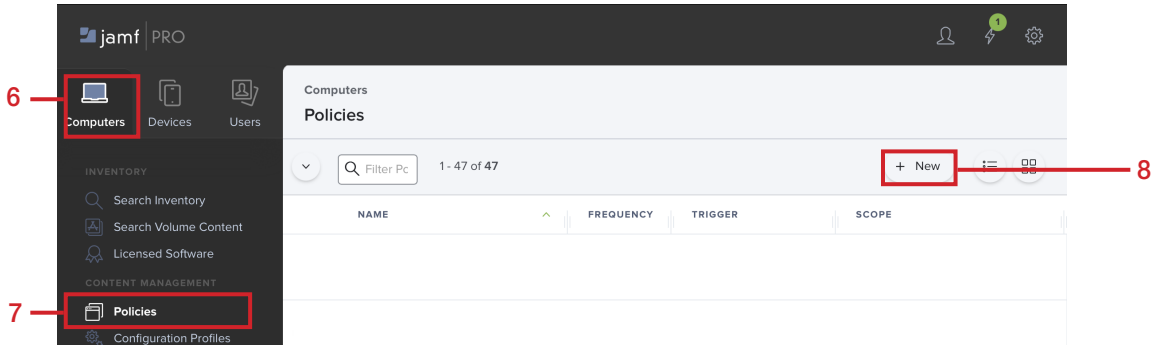
2. Click Computer Groups.
3. Click Add for Computers running macOS 13 or greater.
4. Click Save.



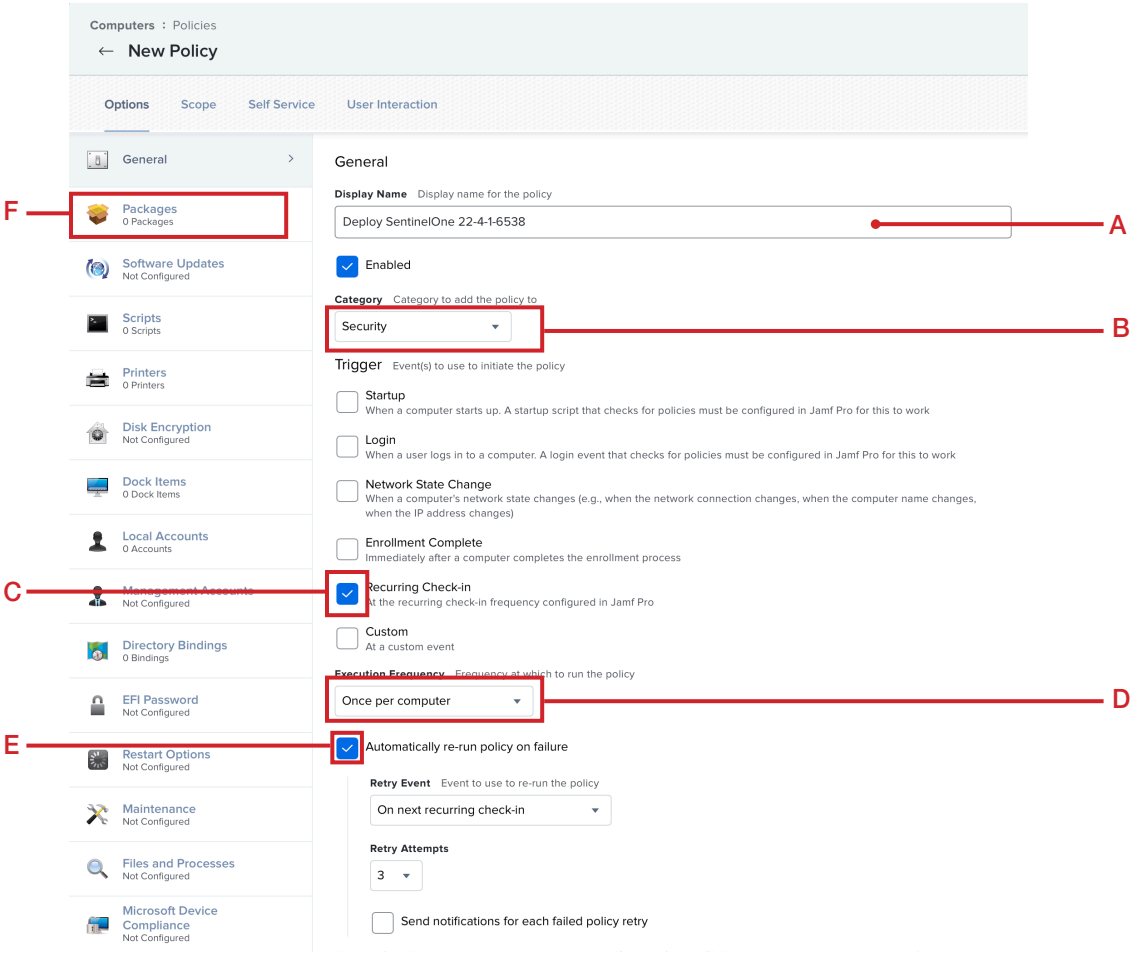
5. If you are using Automated Device Enrollment, make sure that the SentinelOne configuration profiles are installed during the setup assistant.



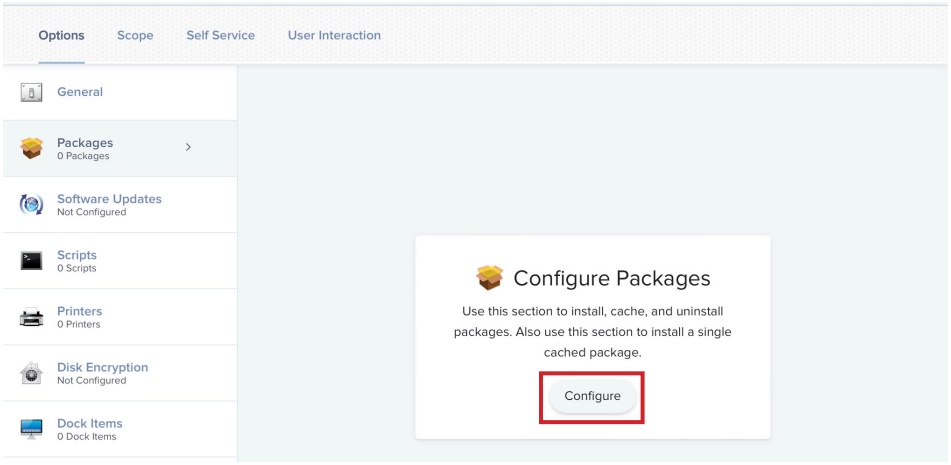
6. Click Computers.
7. Click Policies.
8. Click New (+).



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 Catergory
   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

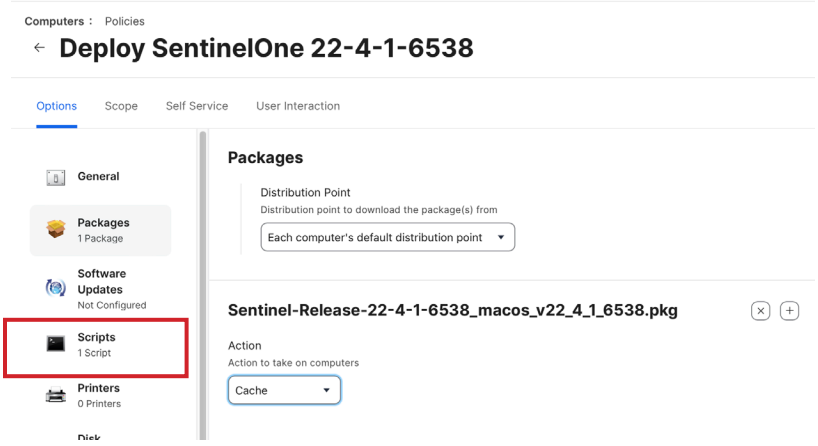


10. Click Configure.

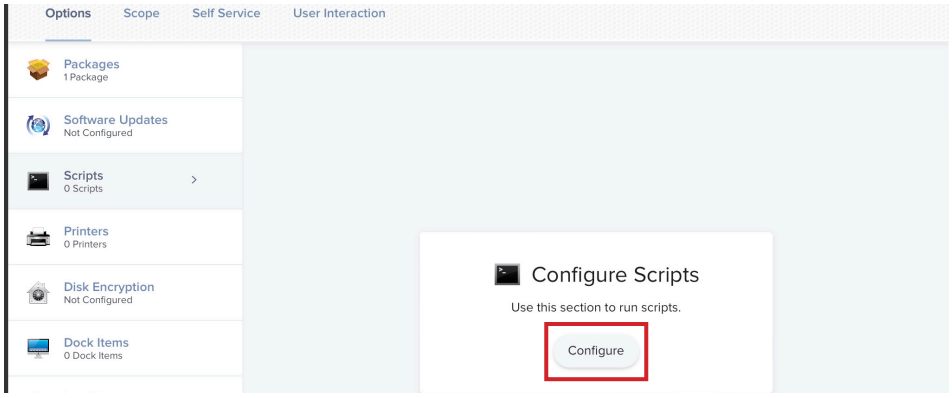


11. Add the SentinelOne package.

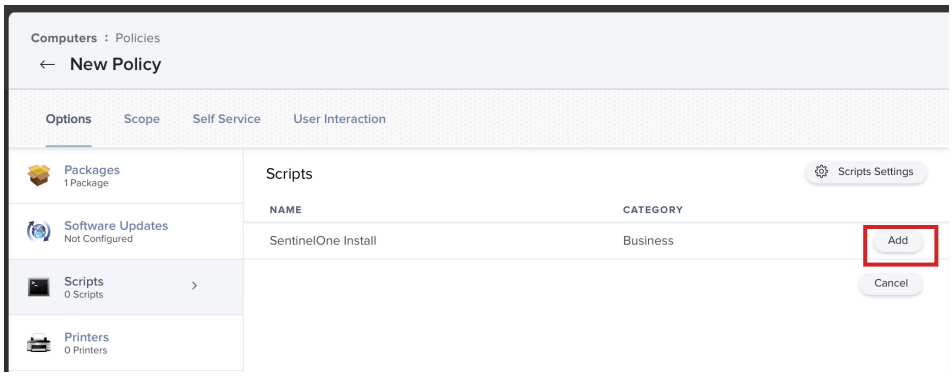
12. Click Scripts.



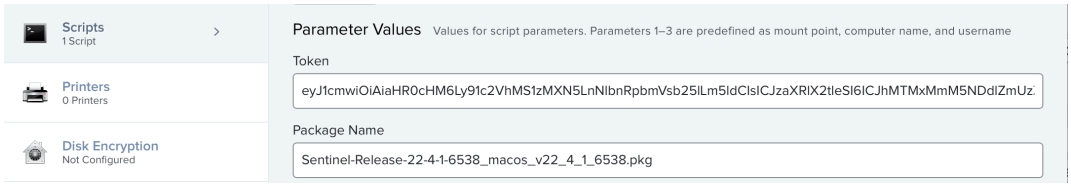
13. Click Configure.



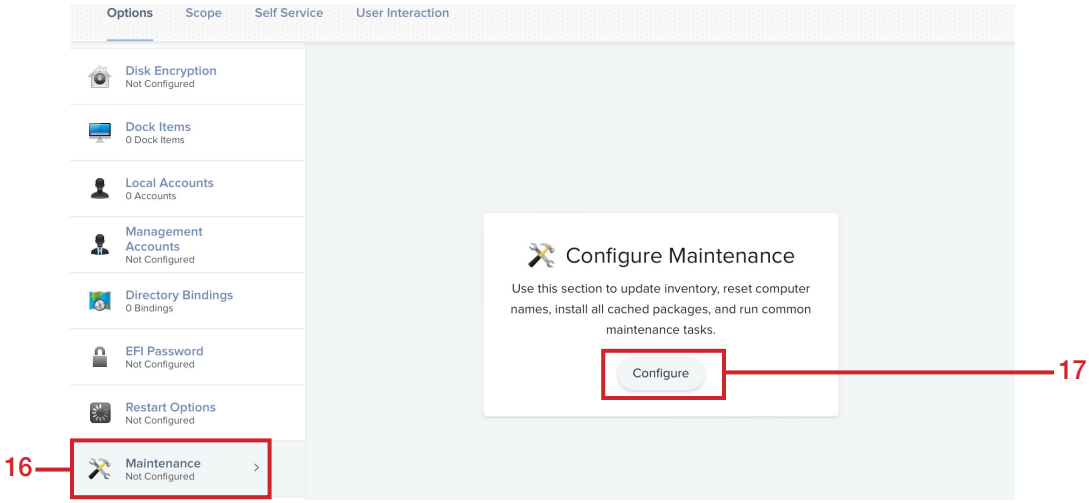
14. Add the SentinelOne Install script.



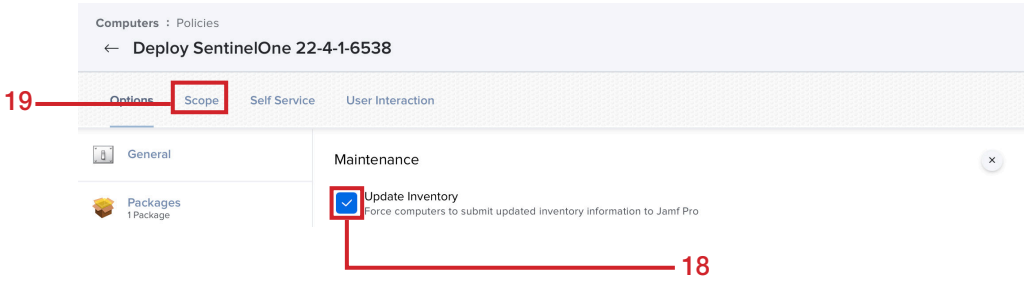
15. Enter your organization token in the parameter labeled Token and the name of the Package in the Package Name parameter.



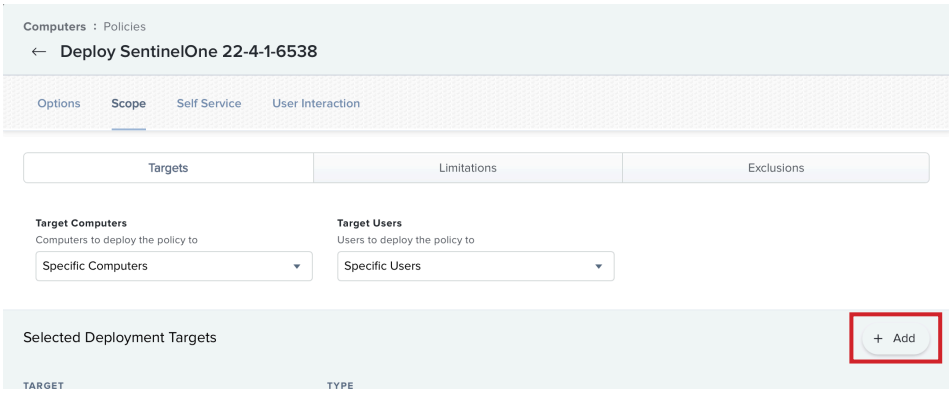
16. Click Maintenance.
17. Click Configure.



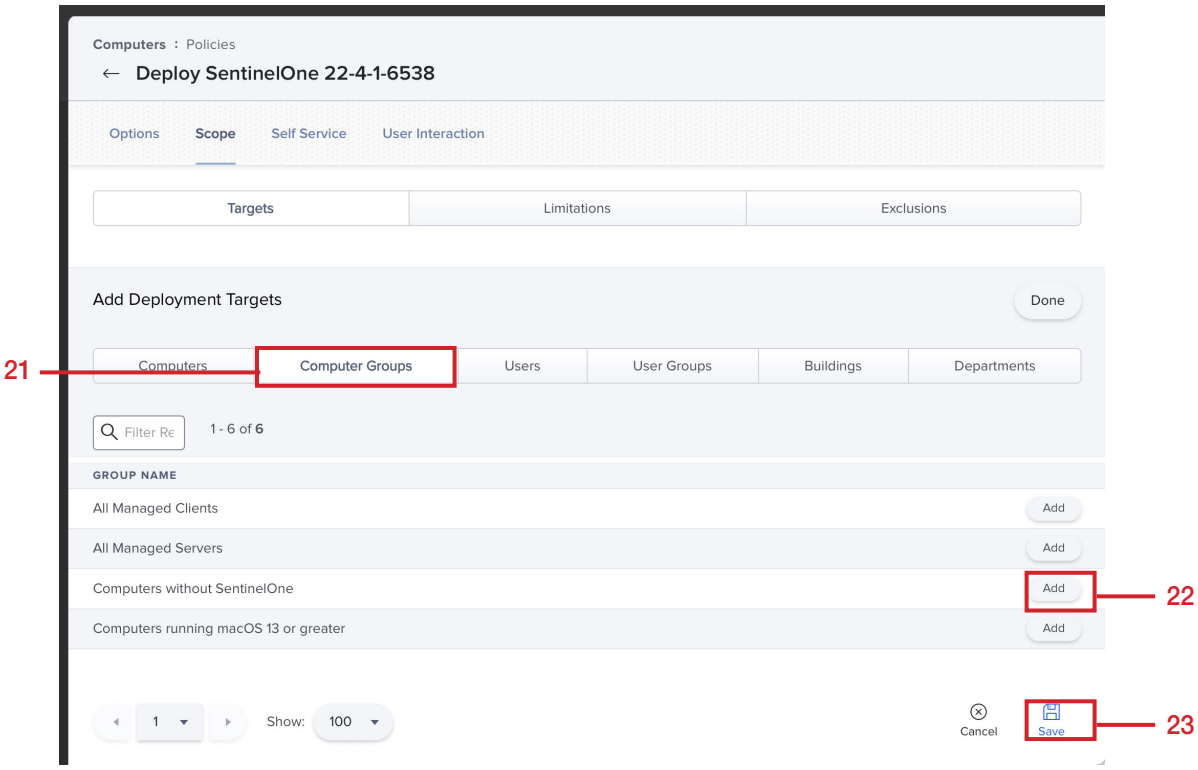
18. Confirm the checkbox for Update Inventory is selected.
19. Click Scope.



20. Click Add (+).



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



This completes this guide.