Configure Jamf Compliance Editor and Jamf Pro for Compliance Reporting

Rev 20250505

Contents

Preface

The Jamf Compliance Editor (JCE) is a tool designed to simplify the implementation of the macOS Security Compliance Project (mSCP) within a Jamf Pro environment. It allows IT administrators to enforce security standards by generating configuration profiles, scripts, and compliance reports for managed macOS, iOS/iPadOS, and visionOS devices. This guide will cover configuring the Jamf Compliance Editor using CIS Level 2 for Mac Computers and iOS devices enrolled in Jamf Pro. While the mSCP is script and command line driven, this document will cover using JCE as a guide for mSCP. For additional information on using mSCP scripts in the command line, please refer to Apple's Mac Security Compliance training at

https://it-training.apple.com/tutorials/apt-compliance/

Jamf Compliance Editor Key Features

1. **Based on NIST's macOS Security Compliance Project (mSCP)**
   Supports multiple compliance standards for government and enterprise security. Leverages NIST's macOS Security Compliance Project. https://github.com/usnistgov/macos_security/wiki
2. **Graphical Interface (GUI) for Compliance Management**
   Eliminates the need to manually edit configuration files or use command-line operations.
3. **Customizable Compliance Selection**
   Administrators can select specific security benchmarks and rules that fit their organization's needs.
4. **Automated Profile and Script Generation**
   Generates configuration profiles and scripts for enforcing and remediating compliance violations.
5. **Compliance Reporting and Documentation**
   Produces reports for internal teams and auditors to verify compliance efforts.
6. **Integration with Jamf Pro**
   Directly uploads compliance profiles, scripts, and extension attributes to Jamf Pro.

Supported Compliance Standards
The NIST macOS Security Compliance Project (mSCP) currently supports the following security frameworks.

Government and Regulatory Standards

- NIST 800-53 (FISMA High/Moderate/Low)
- NIST 800-171 (Controlled Unclassified Information (CUI) Security)
- DISA STIG (U.S. Department of Defense Security Technical Implementation Guide)
- CMMC 2.0 (Cybersecurity Maturity Model Certification)
- CNSSI-1253 (Committee on National Security Systems Instructions)
- Indigo (Base/High) (German Federal Office for Information Security [BSI]) BSI is iOS only

Industry and Non-Governmental Security Standards

- CIS Benchmarks (macOS, iOS/iPadOS)
- CIS Critical Security Controls Version 8 (CIS Controls)

The mSCP project can be extended to support over 200 additional baselines developed by the Secure Controls Framework (SCF):
https://github.com/securecontrolsframework/securecontrolsframework/releases

A crosswalk mapping script—secure-framework-automapping.py—is available here:
https://github.com/boberito/mscp_scripts

This script requires the command-line version of mSCP and the dependencies outlined in the README. It can be used to generate baseline files aligned with various regulatory or compliance frameworks.

NOTE: While these baselines use the same controls evaluated by mSCP, they are not tested or validated by NIST. Additional due diligence is recommended.

Benefits for Organizations Using Jamf Pro

- Reduces complexity in implementing security standards.
- Automates compliance enforcement with minimal manual effort.
- Ensures regulatory alignment for organizations handling sensitive data.
- Streamlines auditing and reporting with built-in documentation tools.

Special thanks to the following individuals for making this guide possible:

- Allen Golbig
- Bob Gendler
- Jamie Richardson
- Nick Koval
- Tom Rice

Section 1: Creating an API Role in Jamf Pro

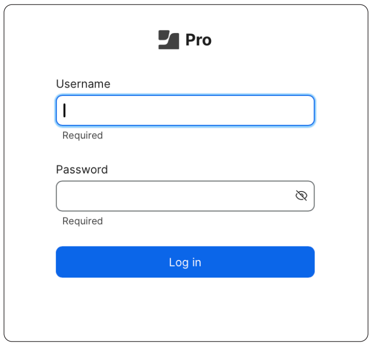
What You'll Need:
Learn what hardware, software, and information you'll need to complete the tutorials in this section.

Hardware and Software:
Requirements for following along with this section:

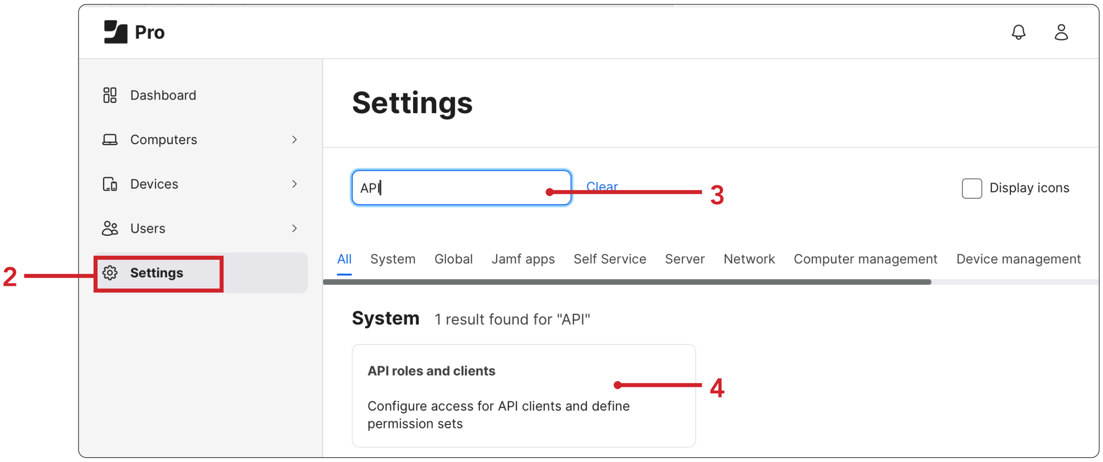
- A Jamf Pro server with administrative privileges to create or modify API roles and API Clients

In this section we create an API Role in Jamf Pro for use with the Jamf Compliance Editor application.

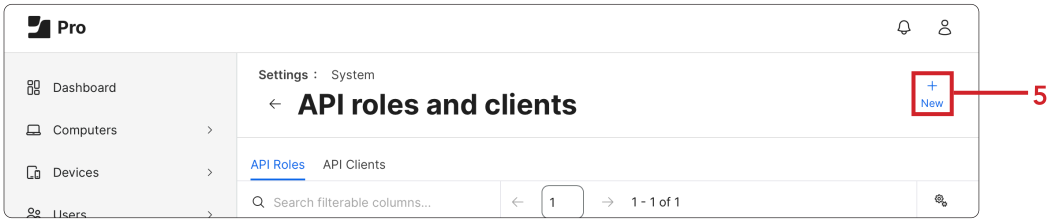
1. Log into your Jamf Pro Server with administrative privileges.



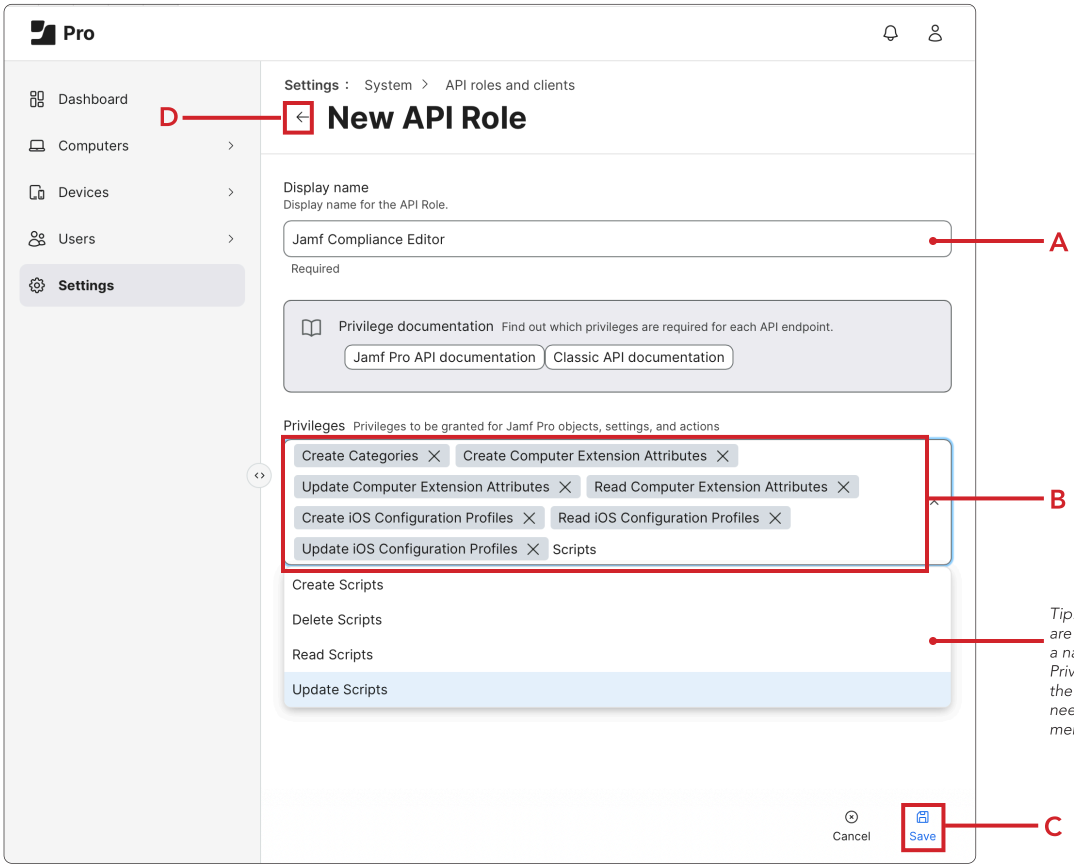
2. Click Settings.
3. Enter **API** in the search field.
4. Click on API roles and clients.



5. Click New.



6. Configure the following:
    A. Enter **Jamf Compliance Editor** for the Display Name.
    B. Enter and select the following under Privileges:
        - **Categories**: Create
        - **Computer Extension Attributes**: Create, Read, Update
        - **macOS Configuration Profiles**: Create, Read, Update
        - **iOS Configuration Profiles**: Create, Read, Update
        - **Scripts**: Create, Read, Update
    C. Click Save.
    D. Click Previous (←).



Settings : System > API roles and clients

New API Role

Display name
Display name for the API Role.

Jamf Compliance Editor

Required

Privilege documentation Find out which privileges are required for each API endpoint.

Jamf Pro API documentation | Classic API documentation

Privileges Privileges to be granted for Jamf Pro objects, settings, and actions

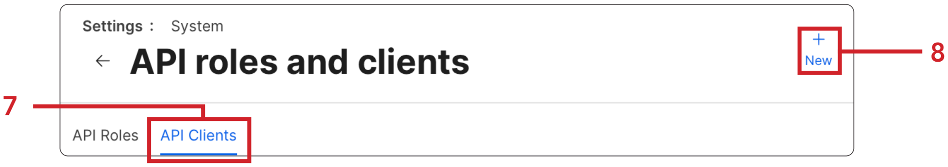
Create Categories ✕ | Create Computer Extension Attributes ✕ | Update Computer Extension Attributes ✕ | Read Computer Extension Attributes ✕ | Create iOS Configuration Profiles ✕ | Read iOS Configuration Profiles ✕ | Update iOS Configuration Profiles ✕ | Scripts

Create Scripts
Delete Scripts
Read Scripts
Update Scripts

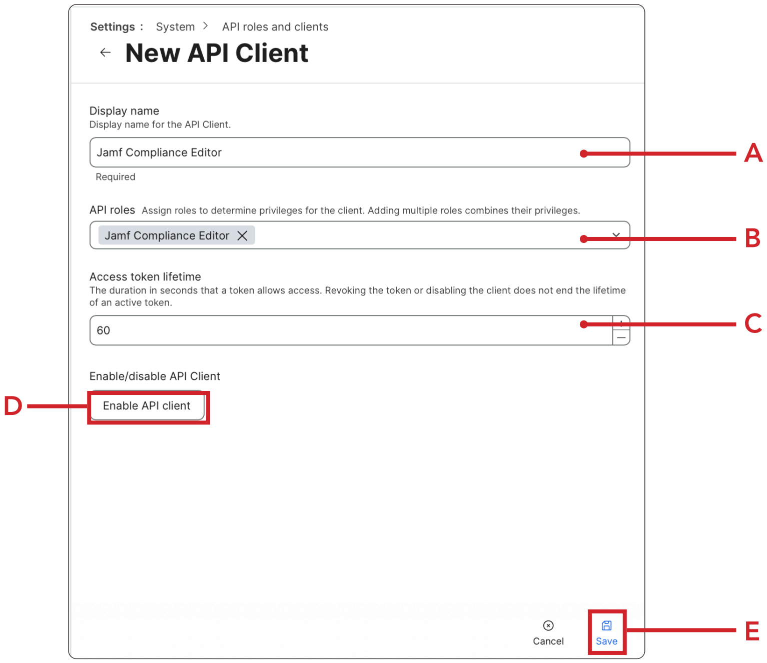
Tip: As you are entering a name of a Privliege, select the ones you need from the menu below.

7. Click API Clients.

8. Click New (+).



9. Configure the following:
   - A. Enter **Jamf Compliance Editor** for the Display Name.
   - B. Select **Jamf Compliance Editor** under API roles.
   - C. Access token lifetime: **60.**
   - D. Click enable API client.
   - E. Click Save.



Settings : System > API roles and clients

New API Client

Display name
Display name for the API Client.

Jamf Compliance Editor

Required

API roles Assign roles to determine privileges for the client. Adding multiple roles combines their privileges.

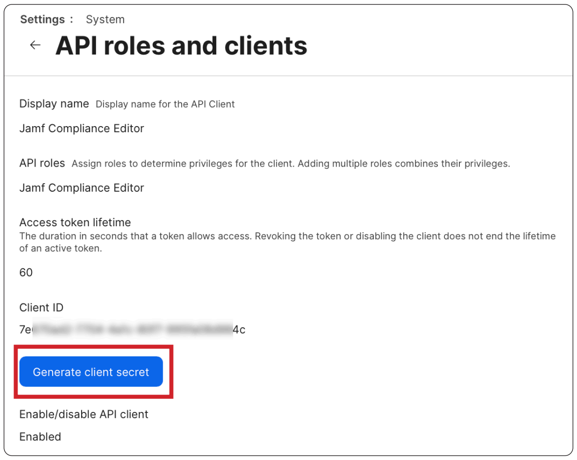
Jamf Compliance Editor

Access token lifetime
The duration in seconds that a token allows access. Revoking the token or disabling the client does not end the lifetime of an active token.

60

Enable/disable API Client

10. Click Generate client secret.



Settings : System

API roles and clients

Display name Display name for the API Client

Jamf Compliance Editor

API roles Assign roles to determine privileges for the client. Adding multiple roles combines their privileges.

Jamf Compliance Editor

Access token lifetime
The duration in seconds that a token allows access. Revoking the token or disabling the client does not end the lifetime of an active token.

60

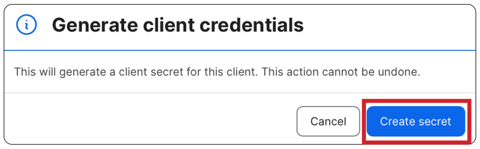
Client ID

7e[redacted]4c

Enable/disable API client

Enabled

11. Click Create secret.

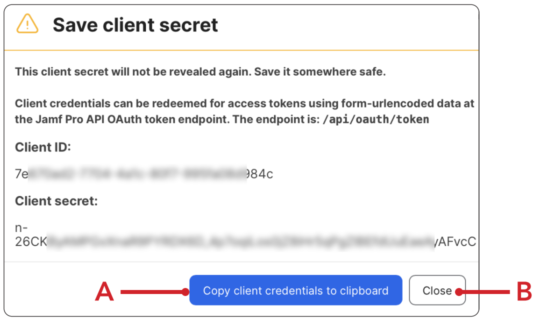


Generate client credentials

This will generate a client secret for this client. This action cannot be undone.

12. Perform the following:
    A. Click Copy client credentials to clipboard and paste into a text edit document. Save it to your Desktop with a name of your choosing.
    B. Click Close.

NOTE: We will need the Client ID and Client secret info in the next section of this guide.



Save client secret

This client secret will not be revealed again. Save it somewhere safe.

Client credentials can be redeemed for access tokens using form-urlencoded data at the Jamf Pro API OAuth token endpoint. The endpoint is: `/api/oauth/token`

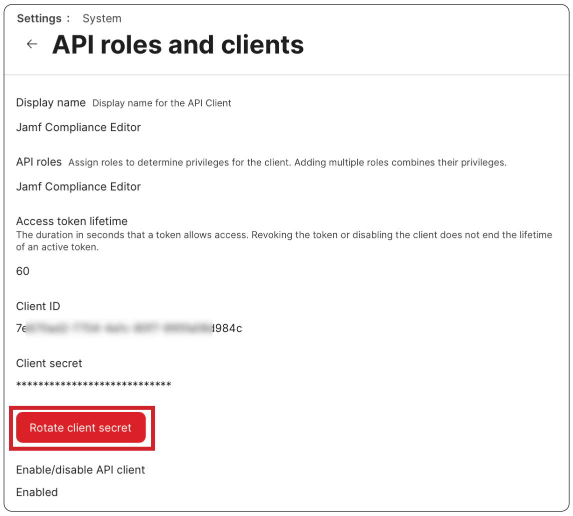
Client ID:

7e[redacted]984c

Client secret:

n-
26CK[redacted]AFvcC

13. Confirm you see the Rotate client secret button.



Settings : System

API roles and clients

Display name Display name for the API Client

Jamf Compliance Editor

API roles Assign roles to determine privileges for the client. Adding multiple roles combines their privileges.

Jamf Compliance Editor

Access token lifetime
The duration in seconds that a token allows access. Revoking the token or disabling the client does not end the lifetime of an active token.

60

Client ID

7e[redacted]984c

Client secret

****

Enable/disable API client

Enabled

This completes this section. In the next section, we will download and configure the Jamf Compliance Editor application.

Section 2: Configure the Jamf Compliance Editor Application.

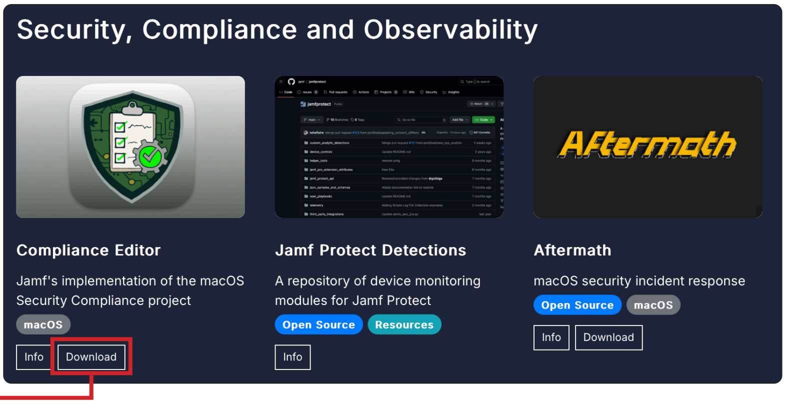
What You'll Need:
Learn what hardware, software, and information you'll need to complete the tutorials in this section.

Hardware and Software:
Requirements for following along with this section:

- Jamf Compliance Editor Application
- Jamf API Role Client ID and Secret
- A Jamf Pro server with administrative privileges

In this section we install and configure the Jamf Compliance Editor application to pre configure the Jamf Pro Server with the needed items for compliance.

1. Go to https://concepts.jamf.com.
2. Scroll down to the Security, Compliance and Observability section and click Download under Compliance Editor.



Security, Compliance and Observability

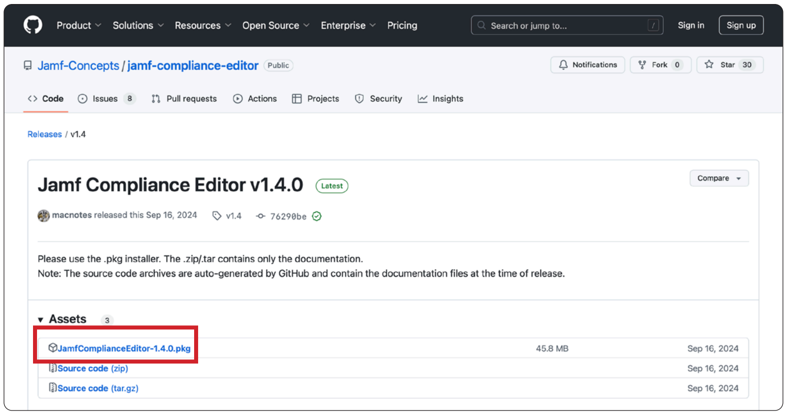
Compliance Editor
Jamf's implementation of the macOS Security Compliance project

Jamf Protect Detections
A repository of device monitoring modules for Jamf Protect

Aftermath
macOS security incident response

Click Download to receive Compliance Editor

3. Click JamfComplianceEditor-1.4.0.pkg.
   NOTE: 1.4.0 was the version at the time of this writing, your version number may be different.



Jamf-Concepts / jamf-compliance-editor

Releases / v1.4

Jamf Compliance Editor v1.4.0

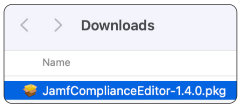
macnotes released this Sep 16, 2024 v1.4 76290be

Please use the .pkg installer. The .zip/.tar contains only the documentation.
Note: The source code archives are auto-generated by GitHub and contain the documentation files at the time of release.

Assets 3

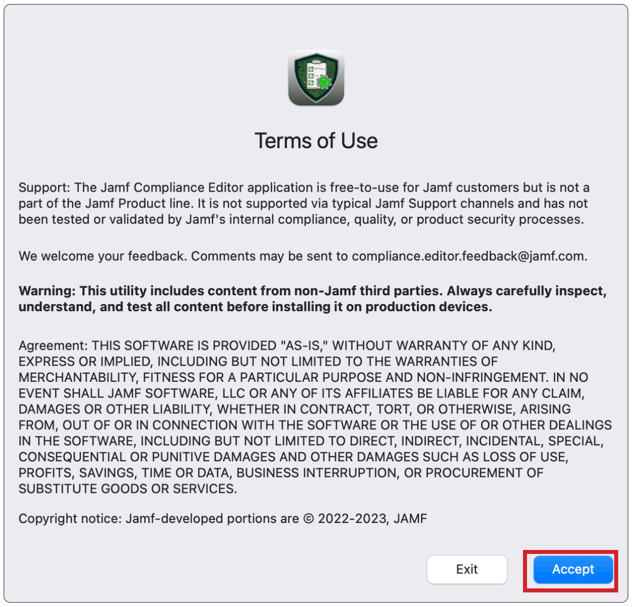
JamfComplianceEditor-1.4.0.pkg	45.8 MB	Sep 16, 2024
Source code (zip)		Sep 16, 2024
Source code (tar.gz)		Sep 16, 2024

4. Go to your Downloads folder and double-click to open JamfComplianceEditor-1.4.0.pkg and follow the default prompts to install it.



5. Open the Jamf Compliance Editor located in the Applications folder.

6. Read the Terms of Use then click Accept.



Terms of Use

Support: The Jamf Compliance Editor application is free-to-use for Jamf customers but is not a part of the Jamf Product line. It is not supported via typical Jamf Support channels and has not been tested or validated by Jamf's internal compliance, quality, or product security processes.

We welcome your feedback. Comments may be sent to compliance.editor.feedback@jamf.com.

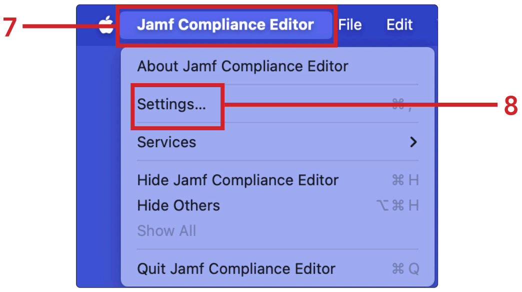
Warning: This utility includes content from non-Jamf third parties. Always carefully inspect, understand, and test all content before installing it on production devices.

Agreement: THIS SOFTWARE IS PROVIDED "AS-IS," WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. IN NO EVENT SHALL JAMF SOFTWARE, LLC OR ANY OF ITS AFFILIATES BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT, OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OF OR OTHER DEALINGS IN THE SOFTWARE, INCLUDING BUT NOT LIMITED TO DIRECT, INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR PUNITIVE DAMAGES AND OTHER DAMAGES SUCH AS LOSS OF USE, PROFITS, SAVINGS, TIME OR DATA, BUSINESS INTERRUPTION, OR PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES.

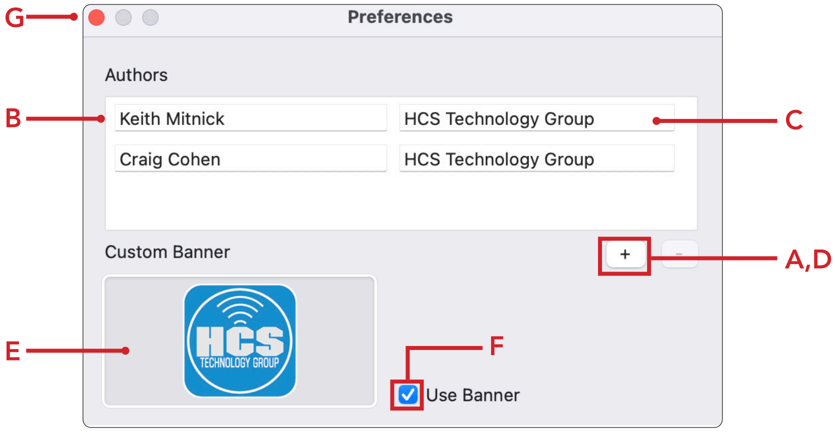
Copyright notice: Jamf-developed portions are © 2022-2023, JAMF

7. Click Jamf Compliance Editor menu.

8. Select Settings (⌘,).


7
Jamf Compliance Editor
File
Edit
About Jamf Compliance Editor
Settings... ⌘ ,
8
Services
Hide Jamf Compliance Editor ⌘ H
Hide Others ⌥ ⌘ H
Show All
Quit Jamf Compliance Editor ⌘ Q

9. Configure the following:
   A. Click Add (+)
   B. Enter your full name
   C. Enter your organization name
   D. If adding multiple authors like shown below, click Add (+)
   E. Drag a logo from your Mac filesystem to the Custom Banner field. Drag and drop from a webpage is not supported.
   F. Select the check box for Use Banner
   G. Close (⊗) the window.
   NOTE: The custom banner logo configured here will show up in the reports discussed later in this guide. The author information will only show up in a report if a baseline is manually altered to remove items from the baseline.



Preferences

Authors

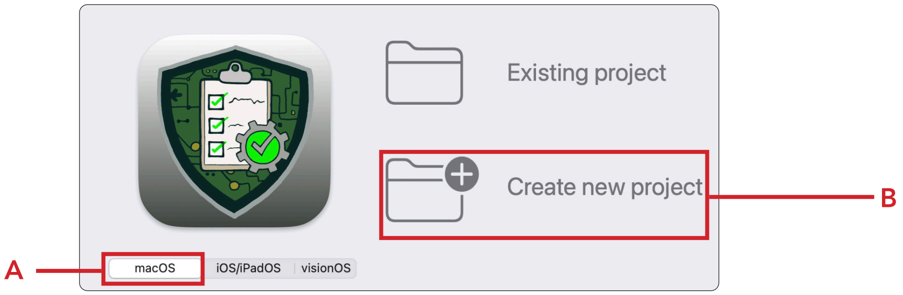
Keith Mitnick	HCS Technology Group
Craig Cohen	HCS Technology Group

Custom Banner

☑ Use Banner

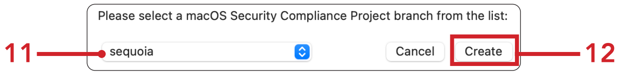
10. Configure the following:

   A. Select the device you’re looking to configure. macOS, iOS/iPadOS, visionOS - This guide will use macOS.
   B. Click Create new project.



11. Select your macOS version. I.E. Sequoia.

12. Click Create.

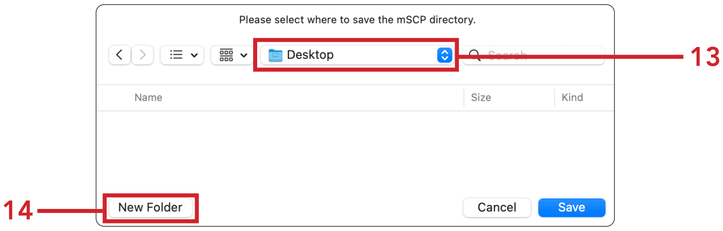


Please select a macOS Security Compliance Project branch from the list:

sequoia

13. Select the Desktop as the destination.

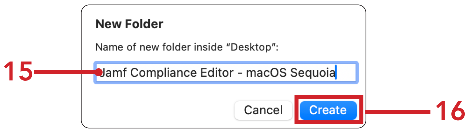
14. Click New Folder.



Please select where to save the mSCP directory.

15. Enter **Jamf Compliance Editor - macOS Sequoia** for the name of the folder. (Change Sequoia to match whatever macOS version you selected in step 11.)

16. Click Create.



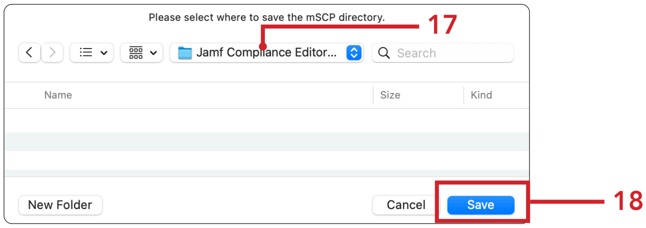
New Folder

Name of new folder inside "Desktop":

Jamf Compliance Editor - macOS Sequoia

17. Confirm the location matches what you created in the previous step.

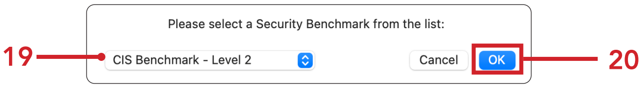
18. Click Save.



Please select where to save the mSCP directory.

19. Select a Benchmark. This guide will select CIS Benchmark - Level 2

20. Click OK.



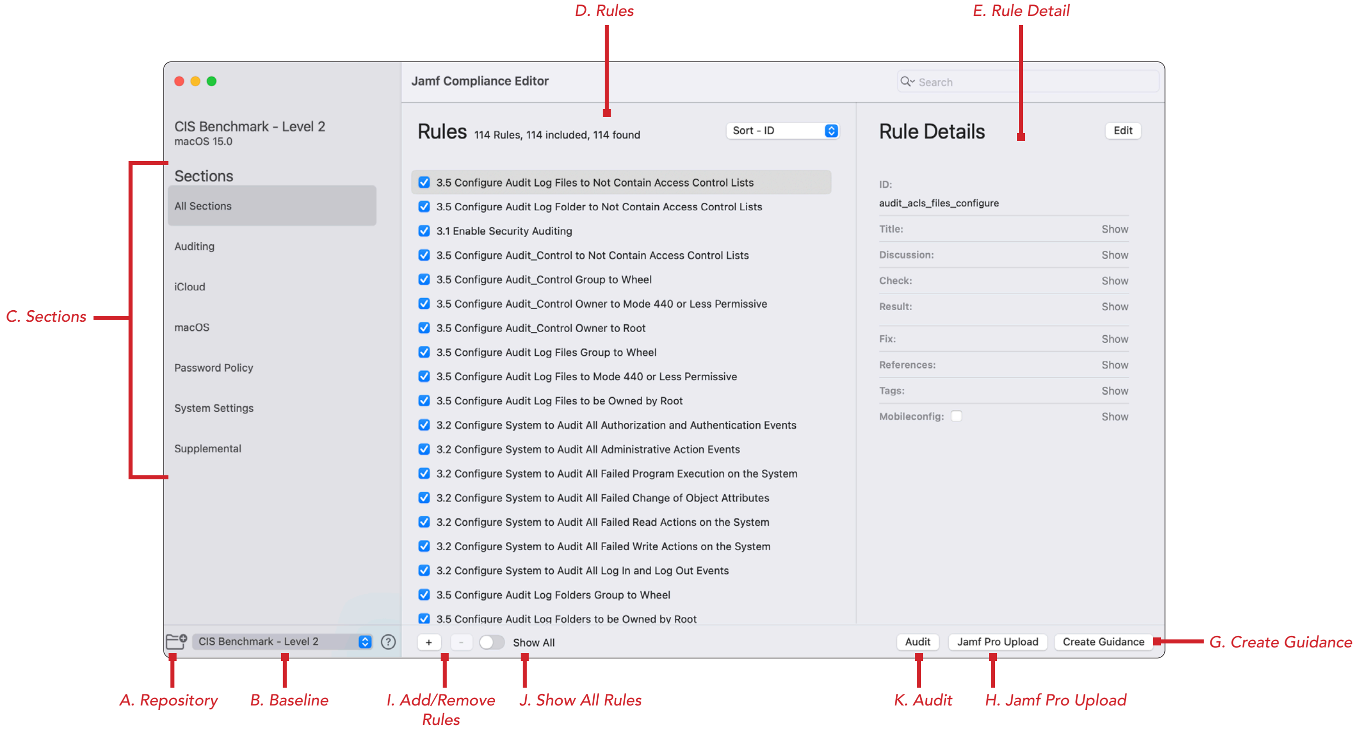
Please select a Security Benchmark from the list:

CIS Benchmark - Level 2

21. The Jamf Compliance Editor window is divided into the following areas:

A. Repository button - Used to select an existing repository or download a new one
B. Baseline popup menu - Switch between the baselines/benchmarks available
C. Sections - Displays all sections available from the selected baseline/benchmark
D. Rules - Displays rules from the selected Section
E. Rule Details - Allows editing of the various rule details including ODV values
F. Create Guidance - Generates output from mSCP plus files for Jamf Pro
G. Jamf Pro Upload - Uploads configuration profiles, compliance script, and
H. Extension Attributes to a Jamf Pro server (Button is greyed out until Create Guidance is completed)
I. Add/Remove Rules - Add/Remove custom rules
J. Show All Rules - Shows rules not in current baseline
K. Audit - Run audit against generated baseline (Button is greyed out until Create Guidance is completed)

22. Click the Create Guidance button.



D. Rules

E. Rule Detail

C. Sections

G. Create Guidance

A. Repository

B. Baseline

I. Add/Remove Rules

J. Show All Rules

K. Audit

H. Jamf Pro Upload

Jamf Compliance Editor

CIS Benchmark - Level 2
macOS 15.0

Sections
All Sections
Auditing
iCloud
macOS
Password Policy
System Settings
Supplemental

Rules 114 Rules, 114 included, 114 found   Sort - ID

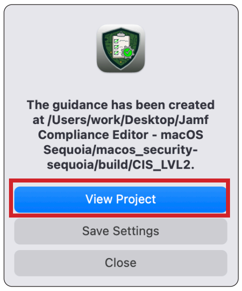
☑ 3.5 Configure Audit Log Files to Not Contain Access Control Lists
☑ 3.5 Configure Audit Log Folder to Not Contain Access Control Lists
☑ 3.1 Enable Security Auditing
☑ 3.5 Configure Audit_Control to Not Contain Access Control Lists
☑ 3.5 Configure Audit_Control Group to Wheel
☑ 3.5 Configure Audit_Control Owner to Mode 440 or Less Permissive
☑ 3.5 Configure Audit_Control Owner to Root
☑ 3.5 Configure Audit Log Files Group to Wheel
☑ 3.5 Configure Audit Log Files to Mode 440 or Less Permissive
☑ 3.5 Configure Audit Log Files to be Owned by Root
☑ 3.2 Configure System to Audit All Authorization and Authentication Events
☑ 3.2 Configure System to Audit All Administrative Action Events
☑ 3.2 Configure System to Audit All Failed Program Execution on the System
☑ 3.2 Configure System to Audit All Failed Change of Object Attributes
☑ 3.2 Configure System to Audit All Failed Read Actions on the System
☑ 3.2 Configure System to Audit All Failed Write Actions on the System
☑ 3.2 Configure System to Audit All Log In and Log Out Events
☑ 3.5 Configure Audit Log Folders Group to Wheel
☑ 3.5 Configure Audit Log Folders to be Owned by Root

Rule Details   Edit

ID:
audit_acls_files_configure

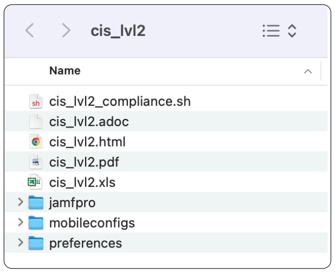
Title:	Show
Discussion:	Show
Check:	Show
Result:	Show
Fix:	Show
References:	Show
Tags:	Show
Mobileconfig: □	Show

23. Click View Project.



The guidance has been created at /Users/work/Desktop/Jamf Compliance Editor - macOS Sequoia/macos_security-sequoia/build/CIS_LVL2.

24. Confirm you see the the cis_lvl2 project files. These files contain everything that was configured when the Create Guidance button was clicked. The files are located in the project folder we created earlier in this guide. The path is:
~/Desktop/Jamf\ Compliance\ Editor\ -\ macOS\ Sequoia/macos_security-sequoia/build/cis_lvl2

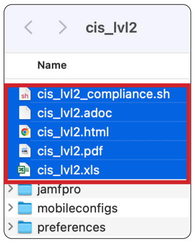

cis_lvl2

Name

- cis_lvl2_compliance.sh
- cis_lvl2.adoc
- cis_lvl2.html
- cis_lvl2.pdf
- cis_lvl2.xls
- jamfpro
- mobileconfigs
- preferences

25. The script, ***cis_lvl2_compliance.sh***, is used with a policy in Jamf Pro to make sure all the CIS Level 2 guidance is accurate on all Mac computers. If a rule was changed by the user, the script can set it back to the CIS Level 2 default setting.

26. The documents, ***cis_lvl2 - adoc, html, pdf, xls***, are documented reports in different file formats that contain everything that was configured when the guidance was created.


cis_lvl2

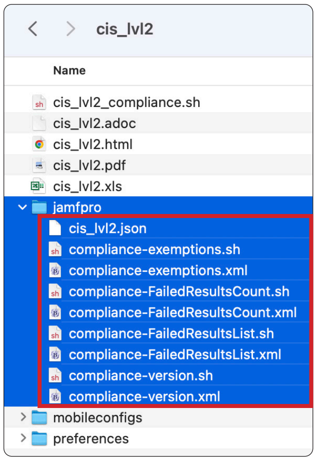
Name

- cis_lvl2_compliance.sh
- cis_lvl2.adoc
- cis_lvl2.html
- cis_lvl2.pdf
- cis_lvl2.xls
- jamfpro
- mobileconfigs
- preferences

27. The file, ***cis_lvl2.json***, is a custom settings schema that allows you to configure custom application settings. The file is used by the compliance script and the Extension Attributes to determine any exemption rules that a user in an organization has approval for. This ensures that the compliance checks succeed without the result count going up. It needs to be manually added to jamf pro and is discussed in detail in a later section of this guide.

28. The three scripts: ***compliance-exemptions.sh, compliance-FailedResultsCount.sh, compliance-FailedResultsList.sh***
are used when running a local Mac audit without using Jamf Pro.

29. The three xml files, ***compliance-exemptions.xml, compliance-FailedResultsCount.xml, compliance-FailedResultsList.xml***,
are imported into Jamf Pro and will create Extension Attributes for reporting.

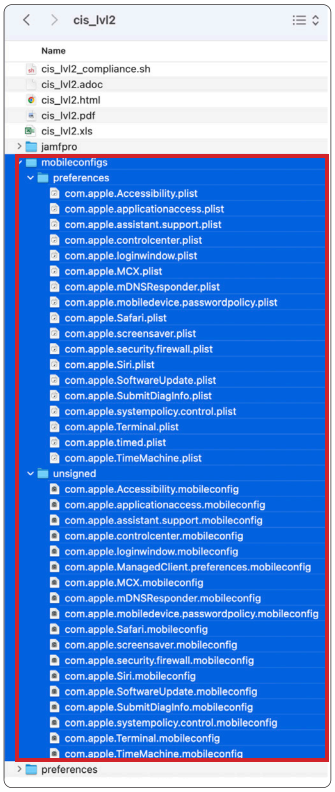

cis_lvl2

Name

- cis_lvl2_compliance.sh
- cis_lvl2.adoc
- cis_lvl2.html
- cis_lvl2.pdf
- cis_lvl2.xls
- jamfpro
  - cis_lvl2.json
  - compliance-exemptions.sh
  - compliance-exemptions.xml
  - compliance-FailedResultsCount.sh
  - compliance-FailedResultsCount.xml
  - compliance-FailedResultsList.sh
  - compliance-FailedResultsList.xml
  - compliance-version.sh
  - compliance-version.xml
- mobileconfigs
- preferences

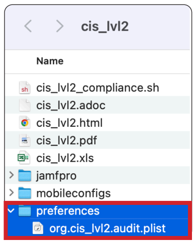
30. In the ***mobileconfigs*** folder, resides two folders named ***preferences*** and ***unsigned***.

   A. The preferences folder contains the plist files for all the settings that are configured for CIS Level 2. These are used when running a local Mac audit without using Jamf Pro.
   B. The unsigned folder contains all the mobileconfig files CIS Level 2. These get uploaded to the Jamf Pro server when the Jamf Pro Upload button is clicked.



```
cis_lvl2
Name
cis_lvl2_compliance.sh
cis_lvl2.adoc
cis_lvl2.html
cis_lvl2.pdf
cis_lvl2.xls
> jamfpro
v mobileconfigs
  v preferences
      com.apple.Accessibility.plist
      com.apple.applicationaccess.plist
      com.apple.assistant.support.plist
      com.apple.controlcenter.plist
      com.apple.loginwindow.plist
      com.apple.MCX.plist
      com.apple.mDNSResponder.plist
      com.apple.mobiledevice.passwordpolicy.plist
      com.apple.Safari.plist
      com.apple.screensaver.plist
      com.apple.security.firewall.plist
      com.apple.Siri.plist
      com.apple.SoftwareUpdate.plist
      com.apple.SubmitDiagInfo.plist
      com.apple.systempolicy.control.plist
      com.apple.Terminal.plist
      com.apple.timed.plist
      com.apple.TimeMachine.plist
  v unsigned
      com.apple.Accessibility.mobileconfig
      com.apple.applicationaccess.mobileconfig
      com.apple.assistant.support.mobileconfig
      com.apple.controlcenter.mobileconfig
      com.apple.loginwindow.mobileconfig
      com.apple.ManagedClient.preferences.mobileconfig
      com.apple.MCX.mobileconfig
      com.apple.mDNSResponder.mobileconfig
      com.apple.mobiledevice.passwordpolicy.mobileconfig
      com.apple.Safari.mobileconfig
      com.apple.screensaver.mobileconfig
      com.apple.security.firewall.mobileconfig
      com.apple.Siri.mobileconfig
      com.apple.SoftwareUpdate.mobileconfig
      com.apple.SubmitDiagInfo.mobileconfig
      com.apple.systempolicy.control.mobileconfig
      com.apple.Terminal.mobileconfig
      com.apple.TimeMachine.mobileconfig
> preferences
```

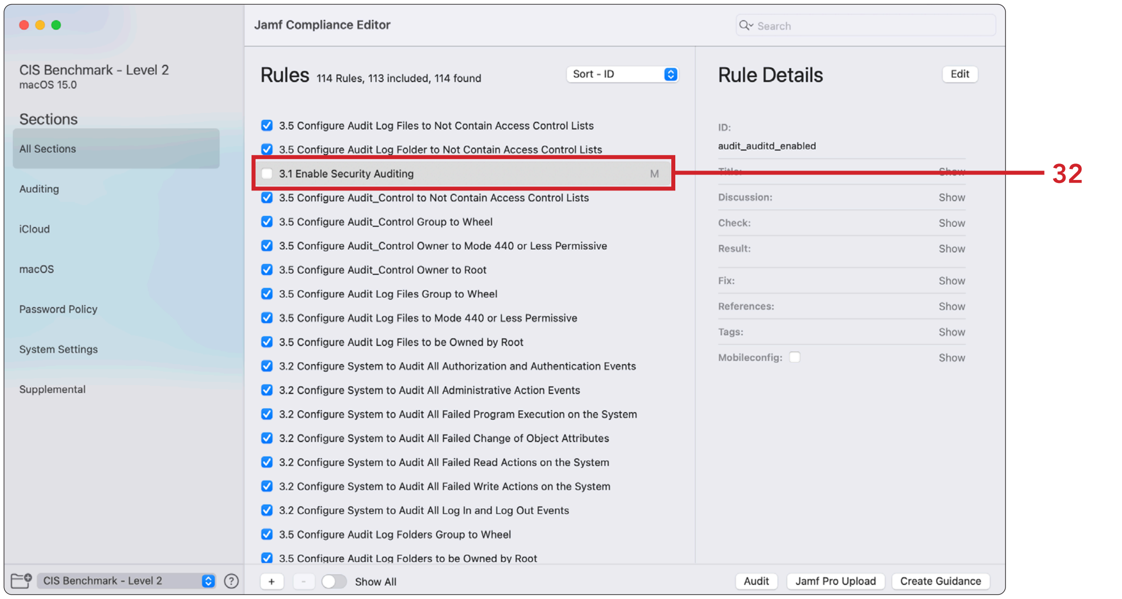
31. In the ***preferences*** folder, a file named ***org.cis_lvl2.audit.plist*** is used when running a local Mac audit without using Jamf Pro.



```
cis_lvl2
Name
cis_lvl2_compliance.sh
cis_lvl2.adoc
cis_lvl2.html
cis_lvl2.pdf
cis_lvl2.xls
> jamfpro
> mobileconfigs
v preferences
    org.cis_lvl2.audit.plist
```

32. Switch back to the Jamf Compliance Editor application. Disable rule 3.1 Enable Security Auditing. Confirm the rule shows the letter “M” to the right of the rule. This means the rule has been modified from the original CIS Level 2 benchmark.

33. Re-enable the 3.1 Enable Security Auditing.



☑ 3.5 Configure Audit Log Files to Not Contain Access Control Lists
☑ 3.5 Configure Audit Log Folder to Not Contain Access Control Lists
□ 3.1 Enable Security Auditing M
☑ 3.5 Configure Audit_Control to Not Contain Access Control Lists
☑ 3.5 Configure Audit_Control Group to Wheel
☑ 3.5 Configure Audit_Control Owner to Mode 440 or Less Permissive
☑ 3.5 Configure Audit_Control Owner to Root
☑ 3.5 Configure Audit Log Files Group to Wheel
☑ 3.5 Configure Audit Log Files to Mode 440 or Less Permissive
☑ 3.5 Configure Audit Log Files to be Owned by Root
☑ 3.2 Configure System to Audit All Authorization and Authentication Events
☑ 3.2 Configure System to Audit All Administrative Action Events
☑ 3.2 Configure System to Audit All Failed Program Execution on the System
☑ 3.2 Configure System to Audit All Failed Change of Object Attributes
☑ 3.2 Configure System to Audit All Failed Read Actions on the System
☑ 3.2 Configure System to Audit All Failed Write Actions on the System
☑ 3.2 Configure System to Audit All Log In and Log Out Events
☑ 3.5 Configure Audit Log Folders Group to Wheel
☑ 3.5 Configure Audit Log Folders to be Owned by Root

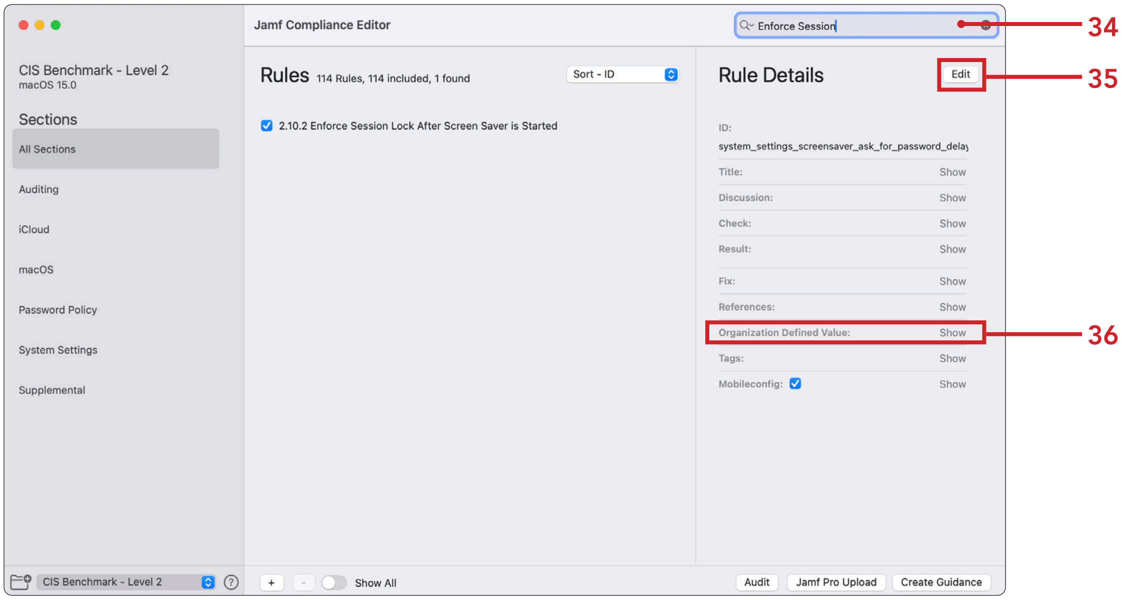
ID:
audit_auditd_enabled
Title: Show
Discussion: Show
Check: Show
Result: Show
Fix: Show
References: Show
Tags: Show
Mobileconfig: □ Show

CIS Benchmark - Level 2

34. In the search field, enter **Enforce Session**.

35. In the Rule Details section, click Edit.

36. Click Show for Organization Defined Value.



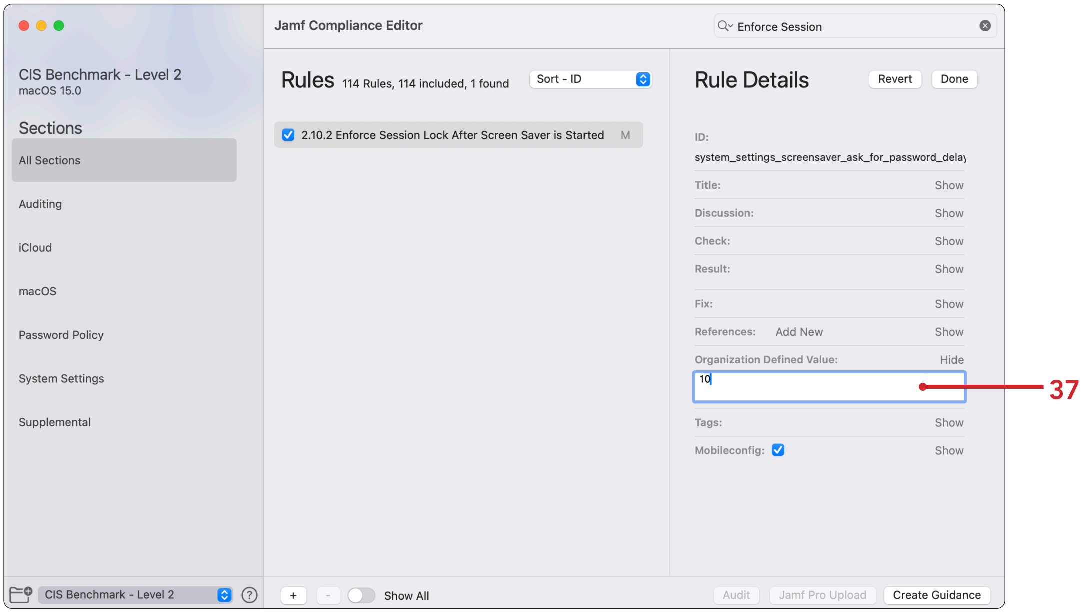
Enforce Session

☑ 2.10.2 Enforce Session Lock After Screen Saver is Started

ID:
system_settings_screensaver_ask_for_password_delay
Title: Show
Discussion: Show
Check: Show
Result: Show
Fix: Show
References: Show
Organization Defined Value: Show
Tags: Show
Mobileconfig: ☑ Show

CIS Benchmark - Level 2

37. In the Organization Defined Value field, change from 5 to 10.



CIS Benchmark - Level 2
macOS 15.0

Rules 114 Rules, 114 included, 1 found

☑ 2.10.2 Enforce Session Lock After Screen Saver is Started

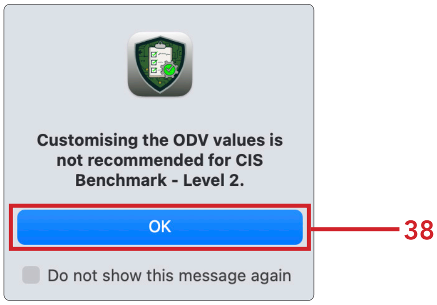
Rule Details

ID: system_settings_screensaver_ask_for_password_delay

Organization Defined Value: 10

Mobileconfig: ☑

38. Confirm a message that states modifying is not recommended. Click OK.



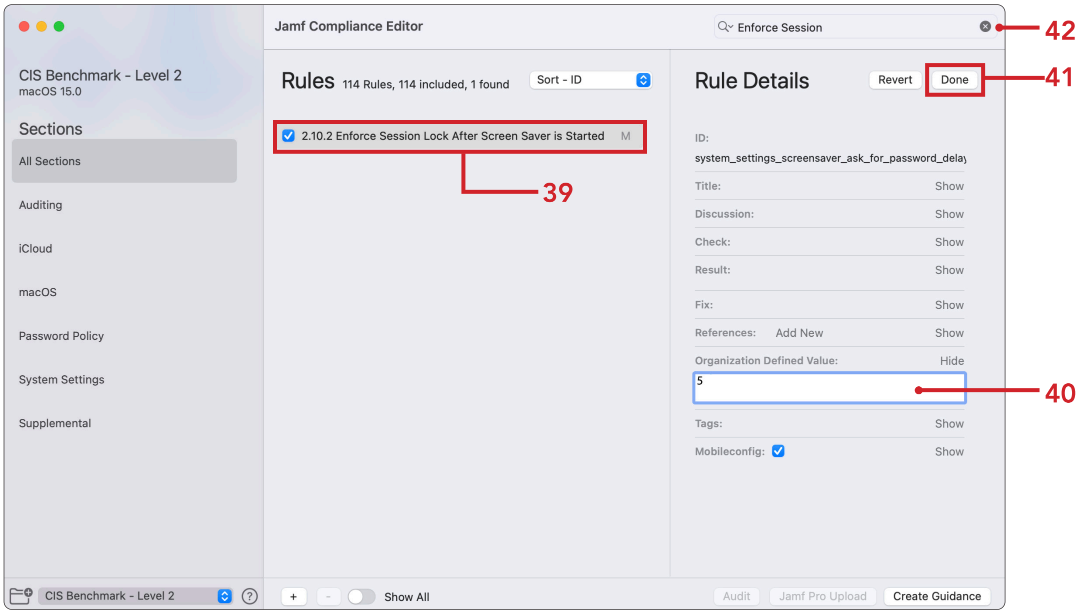
Customising the ODV values is not recommended for CIS Benchmark - Level 2.

39. In the rules section, Notice the letter “M” next to the Enforce Session rule. This means the rule has been modified.

40. In the Organization Defined Value field, change from 10 to 5 to keep things back to the default value.

41. Click Done

42. Remove (⊗) “Enforce Session” from the search field.
NOTE: This was to demonstrate that a rule does not have to be disabled to be modified in a benchmark.


Search: Enforce Session

CIS Benchmark - Level 2
macOS 15.0

Rules 114 Rules, 114 included, 1 found

☑ 2.10.2 Enforce Session Lock After Screen Saver is Started M

Rule Details

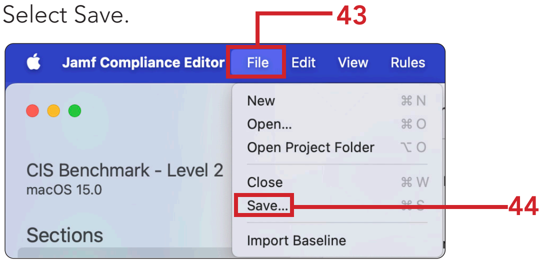
ID: system_settings_screensaver_ask_for_password_delay

Organization Defined Value: 5

Mobileconfig: ☑

43. Click File.

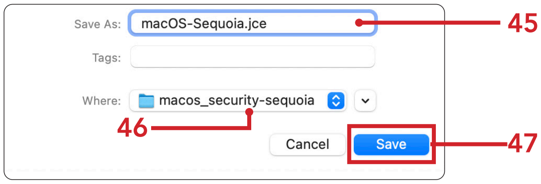
44. Select Save.



45. Enter **macOS-Sequoia.jce** for the File Name.

46. Save to a location of your choosing. This guide will save it to the existing project folder.

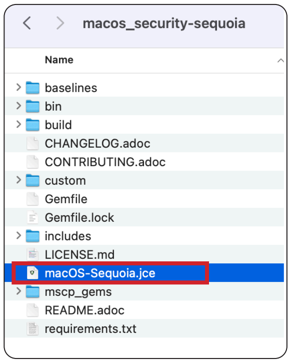
47. Click Save.


Save As: macOS-Sequoia.jce

Tags:

Where: macos_security-sequoia

48. Confirm the macOS-Sequoia.jce was created in the location you saved it in.

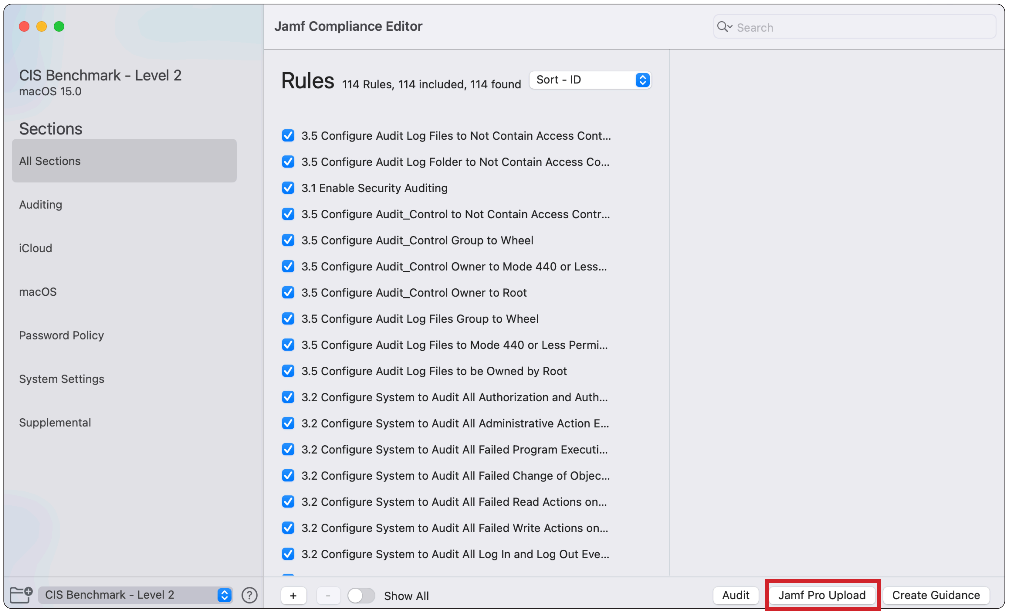


macos_security-sequoia

Name

- baselines
- bin
- build
- CHANGELOG.adoc
- CONTRIBUTING.adoc
- custom
- Gemfile
- Gemfile.lock
- includes
- LICENSE.md
- macOS-Sequoia.jce
- mscp_gems
- README.adoc
- requirements.txt

49. Click Jamf Pro Upload.



Jamf Compliance Editor

CIS Benchmark - Level 2
macOS 15.0

Sections

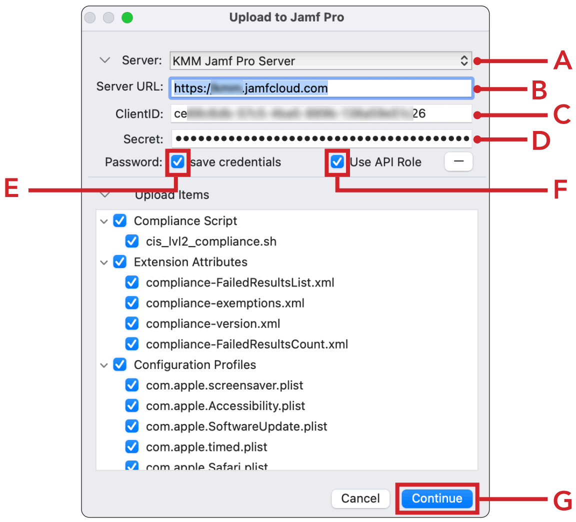
- All Sections
- Auditing
- iCloud
- macOS
- Password Policy
- System Settings
- Supplemental

Rules 114 Rules, 114 included, 114 found

Sort - ID

- ☑ 3.5 Configure Audit Log Files to Not Contain Access Cont...
- ☑ 3.5 Configure Audit Log Folder to Not Contain Access Co...
- ☑ 3.1 Enable Security Auditing
- ☑ 3.5 Configure Audit_Control to Not Contain Access Contr...
- ☑ 3.5 Configure Audit_Control Group to Wheel
- ☑ 3.5 Configure Audit_Control Owner to Mode 440 or Less...
- ☑ 3.5 Configure Audit_Control Owner to Root
- ☑ 3.5 Configure Audit Log Files Group to Wheel
- ☑ 3.5 Configure Audit Log Files to Mode 440 or Less Permi...
- ☑ 3.5 Configure Audit Log Files to be Owned by Root
- ☑ 3.2 Configure System to Audit All Authorization and Auth...
- ☑ 3.2 Configure System to Audit All Administrative Action E...
- ☑ 3.2 Configure System to Audit All Failed Program Executi...
- ☑ 3.2 Configure System to Audit All Failed Change of Objec...
- ☑ 3.2 Configure System to Audit All Failed Read Actions on...
- ☑ 3.2 Configure System to Audit All Failed Write Actions on...
- ☑ 3.2 Configure System to Audit All Log In and Log Out Eve...

50. Configure the following:
   A. Enter the name of your Jamf Pro server.
   B. Enter the URL of your Jamf Pro server.
   C. Enter the client ID we saved in section one of this guide.
   D. Enter the secret we saved in section one of this guide.
   E. Select the checkbox for save credentials.
   F. Select the checkbox or Use API Role.
   G. Click Continue (The button may say Add before it says Continue.)



Upload to Jamf Pro

Server: KMM Jamf Pro Server

Server URL: https://[redacted].jamfcloud.com

ClientID: ce[redacted]26

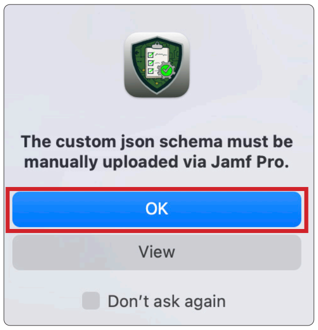
Secret: ••••••••••••••••••••••••••••••••••••••

Password: ☑ save credentials ☑ Use API Role

Upload Items

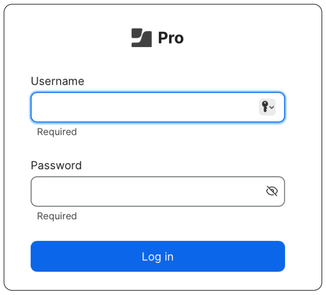
- ☑ Compliance Script
  - ☑ cis_lvl2_compliance.sh
- ☑ Extension Attributes
  - ☑ compliance-FailedResultsList.xml
  - ☑ compliance-exemptions.xml
  - ☑ compliance-version.xml
  - ☑ compliance-FailedResultsCount.xml
- ☑ Configuration Profiles
  - ☑ com.apple.screensaver.plist
  - ☑ com.apple.Accessibility.plist
  - ☑ com.apple.SoftwareUpdate.plist
  - ☑ com.apple.timed.plist
  - ☑ com.apple.Safari.plist

51. Click OK.



The custom json schema must be manually uploaded via Jamf Pro.

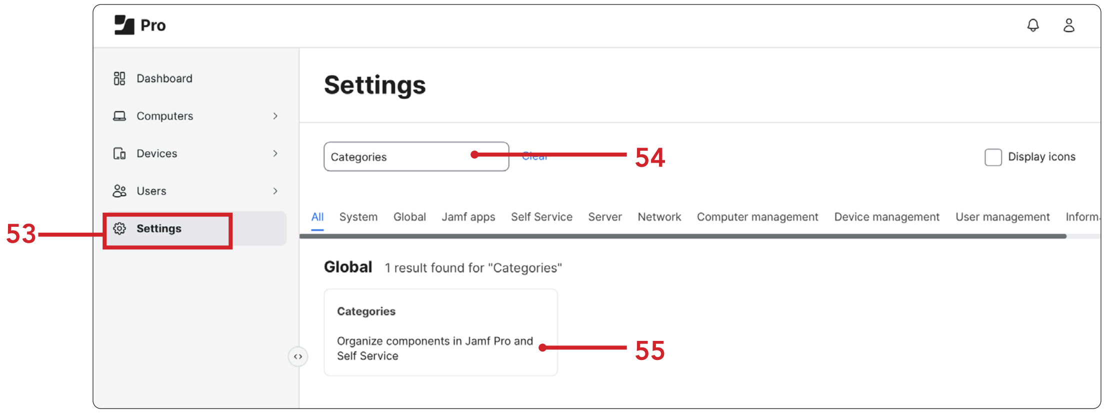
52. Let's confirm the category, configuration profiles, extension attributes and scripts were created by the JCE application, Switch back to your Jamf Pro server. If necessary, login with administrative privileges.



53. Select Settings.

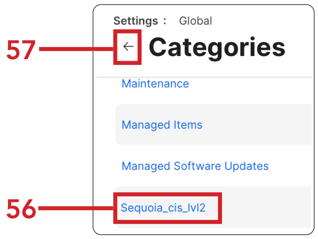
54. Enter categories in the search field.

55. Click Categories.



56. Confirm a category named Sequoia_cis_lvl2 was created.

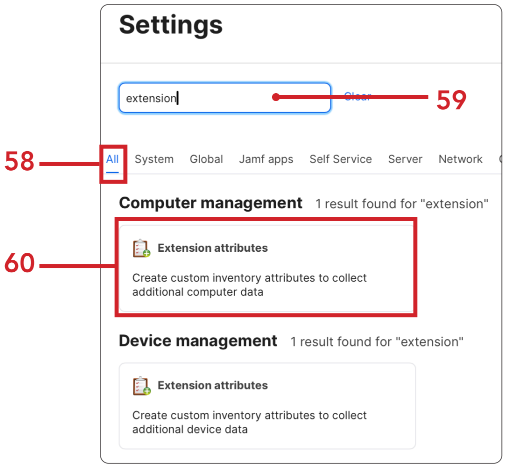
57. Click Previous (←).



58. Click All.

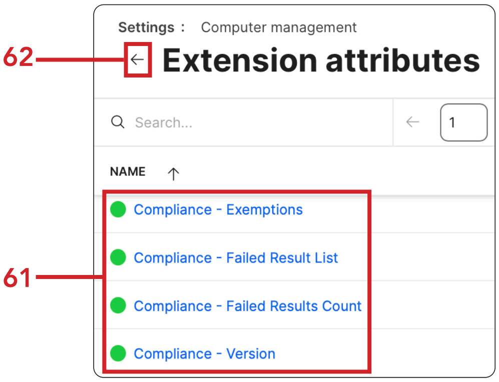
59. Enter extension in the search field.

60. Click Extension attributes under Computer management.


Settings
extension
Clear
All
System
Global
Jamf apps
Self Service
Server
Network
Computer management
1 result found for "extension"
Extension attributes
Create custom inventory attributes to collect additional computer data
Device management
1 result found for "extension"
Extension attributes
Create custom inventory attributes to collect additional device data
58
59
60

61.Confirm that four Extension Attributes that start with Compliance were created.

62.Click Previous (←).



Settings : Computer management

← Extension attributes

Search... ← 1

NAME ↑

● Compliance - Exemptions

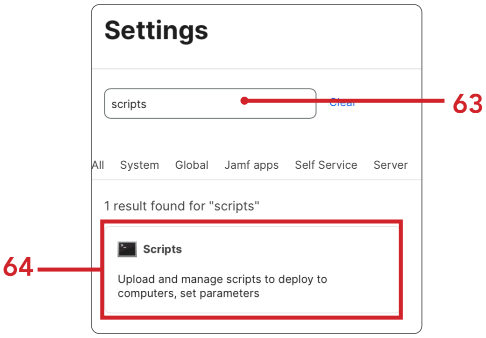
● Compliance - Failed Result List

● Compliance - Failed Results Count

● Compliance - Version

63.Enter scripts in the search field.

64.Click Scripts.



Settings

scripts

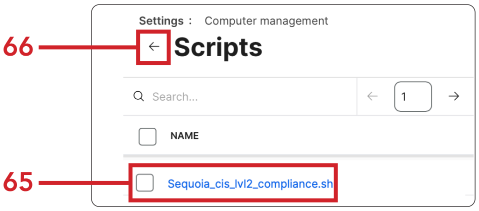
1 result found for "scripts"

Scripts

Upload and manage scripts to deploy to computers, set parameters

65.Confirm a script named Sequoia_cis_lvl2_compliance.sh was created.

66.Click Previous (←).



Settings : Computer management

← Scripts

Search... ← 1 →

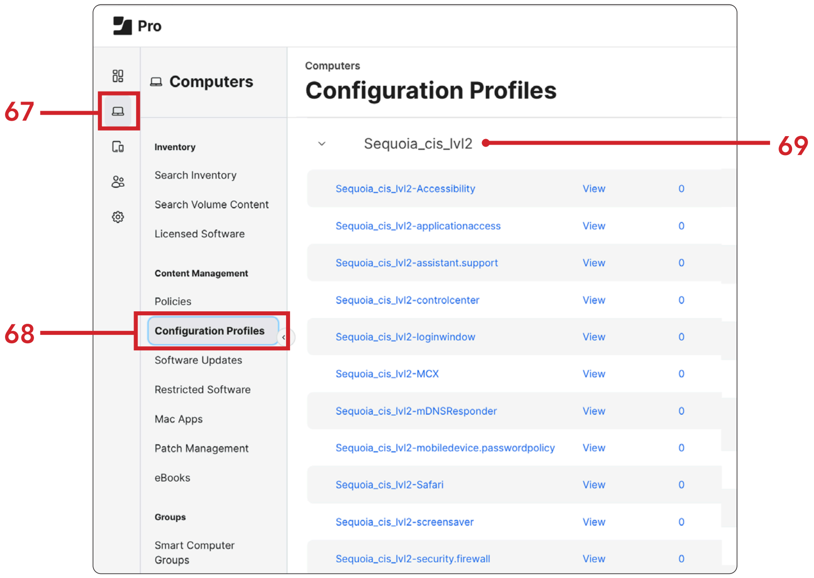
□ NAME

□ Sequoia_cis_lvl2_compliance.sh

67. Click Computers.

68. Click Configuration Profiles.

69. Confirm a category named Sequoia_cis_lvl2 was created with multiple configuration profiles listed.
NOTE: These configuration profiles have not been scoped to any Mac computers yet.



Computers

Configuration Profiles

Sequoia_cis_lvl2

Sequoia_cis_lvl2-Accessibility	View	0
Sequoia_cis_lvl2-applicationaccess	View	0
Sequoia_cis_lvl2-assistant.support	View	0
Sequoia_cis_lvl2-controlcenter	View	0
Sequoia_cis_lvl2-loginwindow	View	0
Sequoia_cis_lvl2-MCX	View	0
Sequoia_cis_lvl2-mDNSResponder	View	0
Sequoia_cis_lvl2-mobiledevice.passwordpolicy	View	0
Sequoia_cis_lvl2-Safari	View	0
Sequoia_cis_lvl2-screensaver	View	0
Sequoia_cis_lvl2-security.firewall	View	0

This completes this section. In the next section, we will create smart computer groups to use for scoping in Jamf Pro.

Section 3: Creating Smart Computer Groups

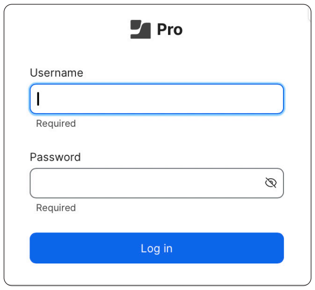
What You'll Need:
Learn what hardware, software, and information you'll need to complete the tutorials in this section.

Hardware and Software:
Requirements for following along with this section:

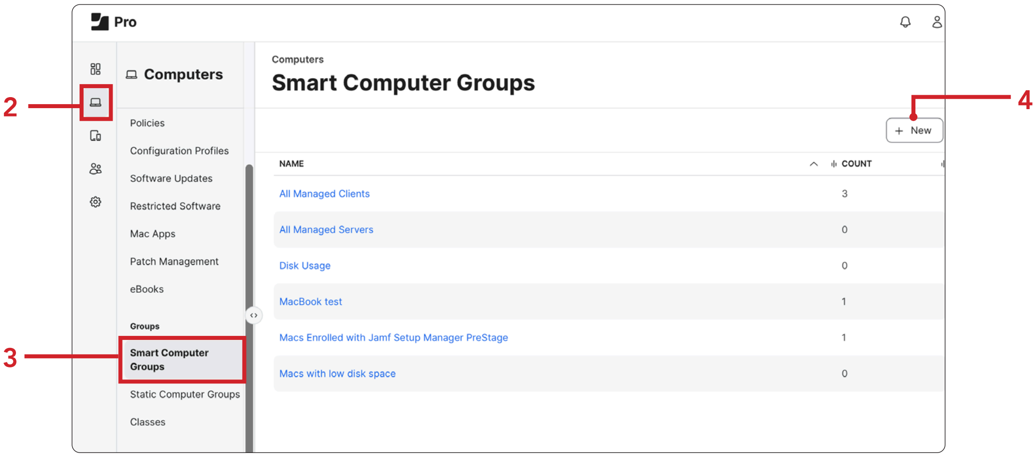
- A Jamf Pro server with administrative privileges

In this section we create three smart computer groups in Jamf Pro to use for scoping.

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



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

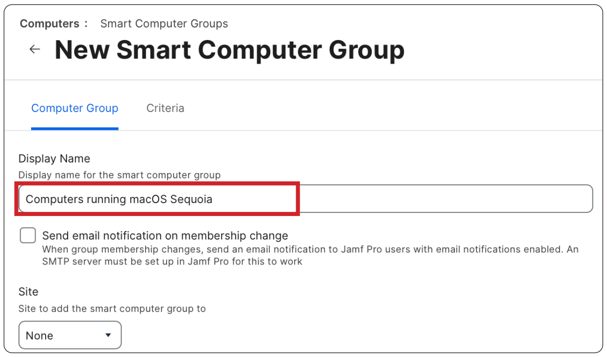


Computers

Smart Computer Groups

NAME	COUNT
All Managed Clients	3
All Managed Servers	0
Disk Usage	0
MacBook test	1
Macs Enrolled with Jamf Setup Manager PreStage	1
Macs with low disk space	0

5. Enter **Computers running macOS Sequoia** for the Display Name.
   NOTE: Change the macOS name to your needs.



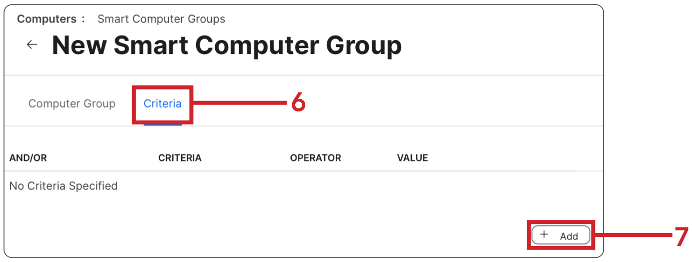
Display Name
Display name for the smart computer group
Computers running macOS Sequoia

☐ 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

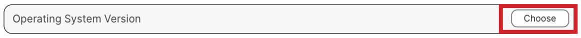
Site
Site to add the smart computer group to
None

6. Click Criteria.

7. Click Add (+).



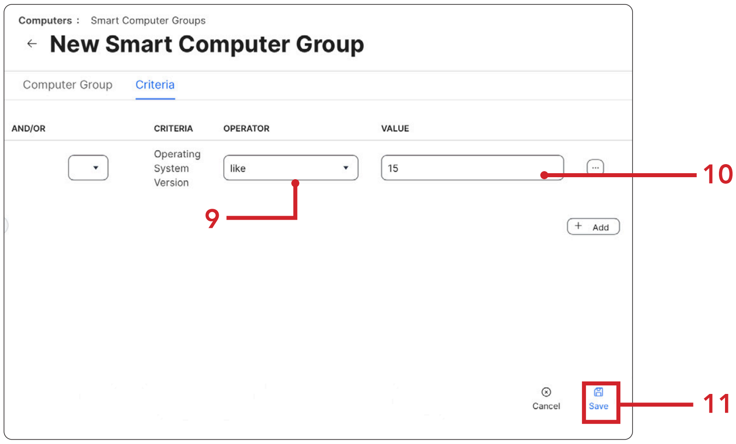
8. Scroll down to Operating System Version and click Choose.



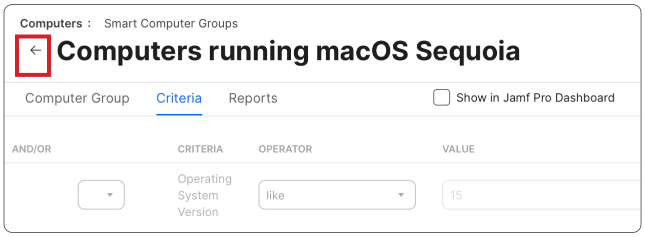
9. Set the Operator to **like.**

10. Enter the value to your needs. This guide will use **15.**

11. Click Save.

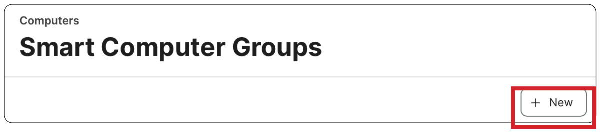


12. Click Previous (←).

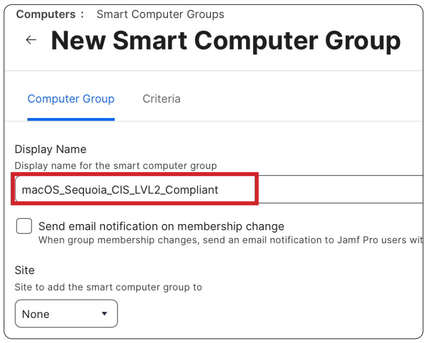


Computers : Smart Computer Groups
Computers running macOS Sequoia
Computer Group
Criteria
Reports
□ Show in Jamf Pro Dashboard
AND/OR
CRITERIA
OPERATOR
VALUE
Operating System Version
like
15

13. Click New (+).



14. Enter **macOS_Sequoia_CIS_LVL2_Compliant** for the Display Name. NOTE: Change the macOS name to your needs.



Computers : Smart Computer Groups

← New Smart Computer Group

Computer Group | Criteria

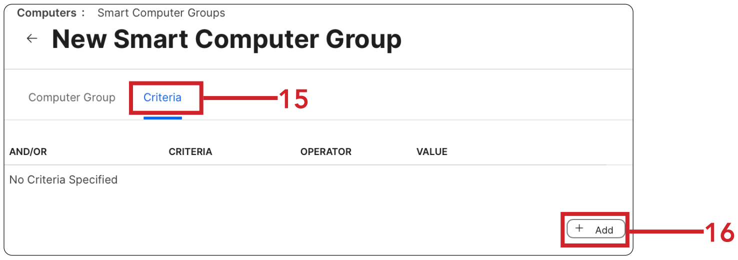
Display Name
Display name for the smart computer group
macOS_Sequoia_CIS_LVL2_Compliant

☐ Send email notification on membership change
When group membership changes, send an email notification to Jamf Pro users wit

Site
Site to add the smart computer group to
None ▾

15. Click Criteria.

16. Click Add (+).



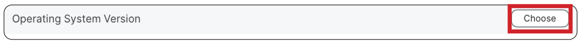
Computers : Smart Computer Groups

← New Smart Computer Group

Computer Group | Criteria

AND/OR	CRITERIA	OPERATOR	VALUE
No Criteria Specified			

17. Scroll down to Operating System and click Choose.

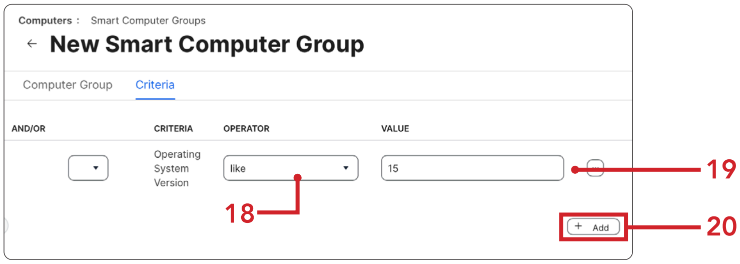


Operating System Version

18. Set the Operator to **like.**

19. Enter the value to your needs. This guide will use **15.**

20. Click Add (+).



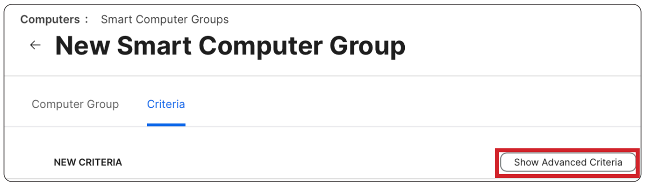
Computers : Smart Computer Groups

← New Smart Computer Group

Computer Group | Criteria

AND/OR	CRITERIA	OPERATOR	VALUE
▾	Operating System Version	like ▾	15

21. Click Show Advanced Criteria, if necessary.



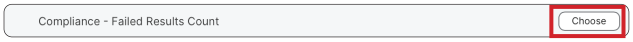
Computers : Smart Computer Groups

← New Smart Computer Group

Computer Group | Criteria

NEW CRITERIA

22. Scroll down to Compliance - Failed Results Count and click Choose.

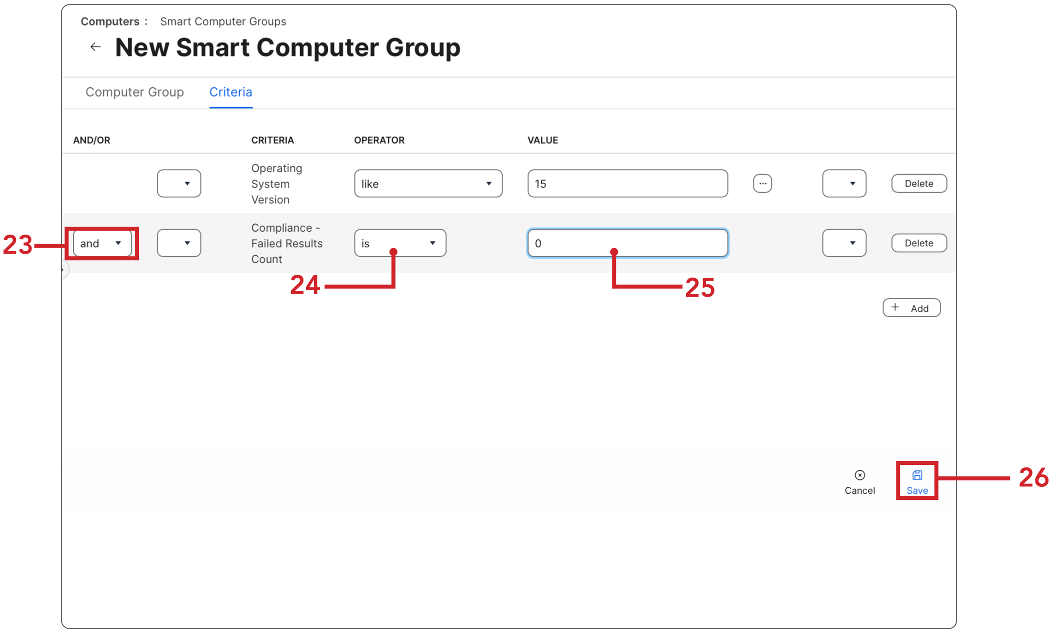


23. From the menu, select **and.**

24. Set the Operator to **is.**

25. Enter the Value: **0.**

26. Click Save.

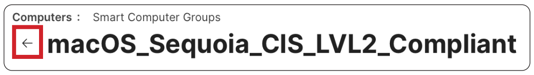

Computers : Smart Computer Groups

New Smart Computer Group

Computer Group | Criteria

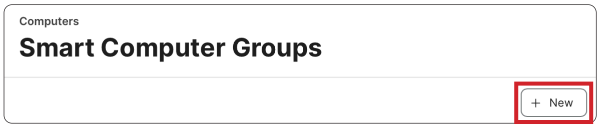
AND/OR		CRITERIA	OPERATOR	VALUE			
	▾	Operating System Version	like ▾	15	···	▾	Delete
and ▾	▾	Compliance - Failed Results Count	is ▾	0		▾	Delete

27. Click Previous (←).


Computers : Smart Computer Groups

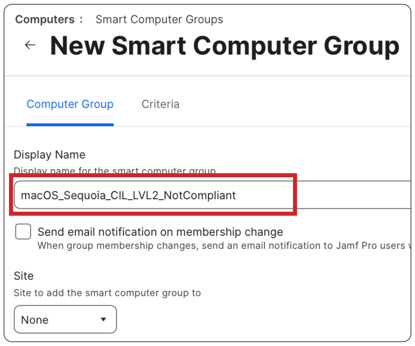
← macOS_Sequoia_CIS_LVL2_Compliant

28. Click New (+).


Computers

Smart Computer Groups

29. For the Display Name, enter: **macOS_Sequoia_CIL_LVL2_NotCompliant.**



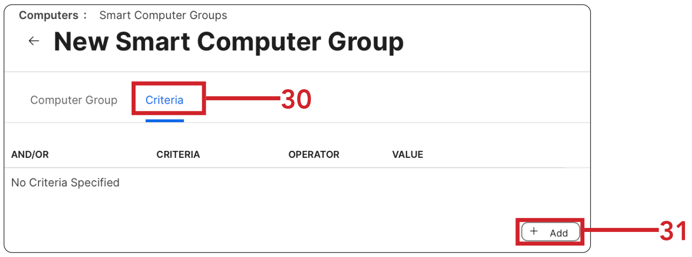
Display Name
Display name for the smart computer group
macOS_Sequoia_CIL_LVL2_NotCompliant

☐ Send email notification on membership change
When group membership changes, send an email notification to Jamf Pro users

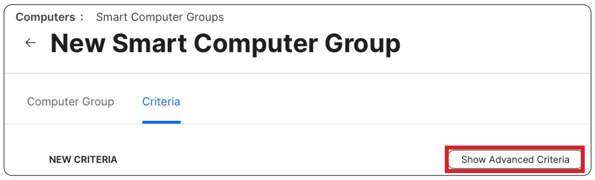
Site
Site to add the smart computer group to
None

30. Click Criteria.

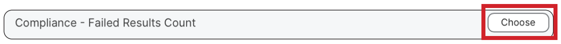
31. Click Add.



32. Click Show Advanced Criteria.



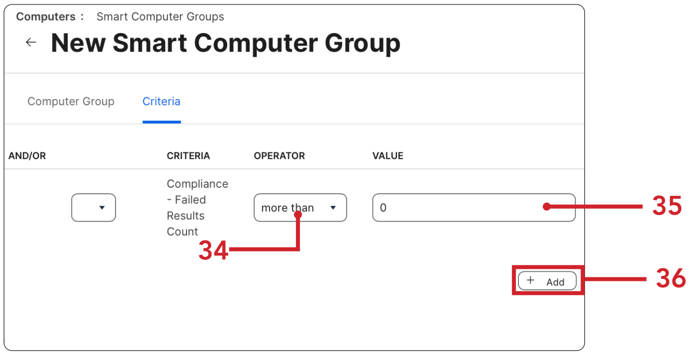
33. Scroll down to Compliance - Failed Results Count and click Choose.



34. For the Operator, select **more than.**

35. Enter **0** for the Value.

36. Click Add.



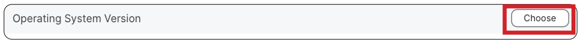
Computers : Smart Computer Groups

New Smart Computer Group

Computer Group | Criteria

AND/OR	CRITERIA	OPERATOR	VALUE
	Compliance - Failed Results Count	more than	0

37. Scroll down to Operating System and click Choose.



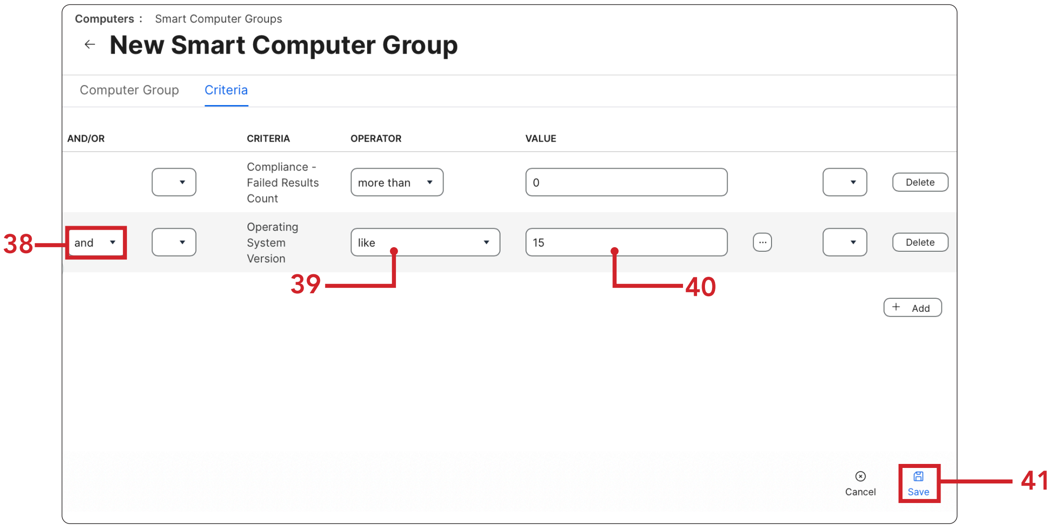
Operating System Version

38. From the menu, select **and.**

39. Set the Operator to **like.**

40. Enter **15** for the Value.

41. Click Save.



Computers : Smart Computer Groups

New Smart Computer Group

Computer Group | Criteria

AND/OR		CRITERIA	OPERATOR	VALUE
		Compliance - Failed Results Count	more than	0
and		Operating System Version	like	15

This completes this section. In the next section, we will create three policies in Jamf Pro.

Section 4: Creating Policies

What You'll Need:
Learn what hardware, software, and information you'll need to complete the tutorials in this section.

Hardware and Software:
Requirements for following along with this section:

- A Jamf Pro server with administrative privileges

In this section, we will create three Jamf Pro policies to execute the sequoia_cis_lvl2_compliance.sh script generated by Jamf Compliance Editor. This script supports several flags that control its behavior. The policies will use the following flags:

- `--check` Runs an audit only (no remediation).
- `--cfc` Runs an audit, applies remediation, then re-audits to verify compliance.
- `--reset` Clears results from the previous audit for the current baseline.

Policies to Create in Jamf Pro

Sequoia_CIS Level 2_Audit

- Script flag: `--check`
- Purpose: Performs a compliance audit only.

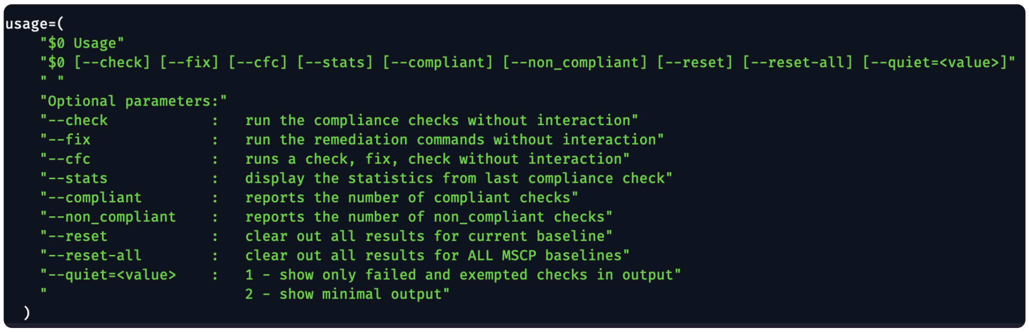
Sequoia_CIS Level 2_Remediation

- Script flag: `--cfc`
- Purpose: Performs audit, remediates failures, then verifies compliance.

Reset Baseline

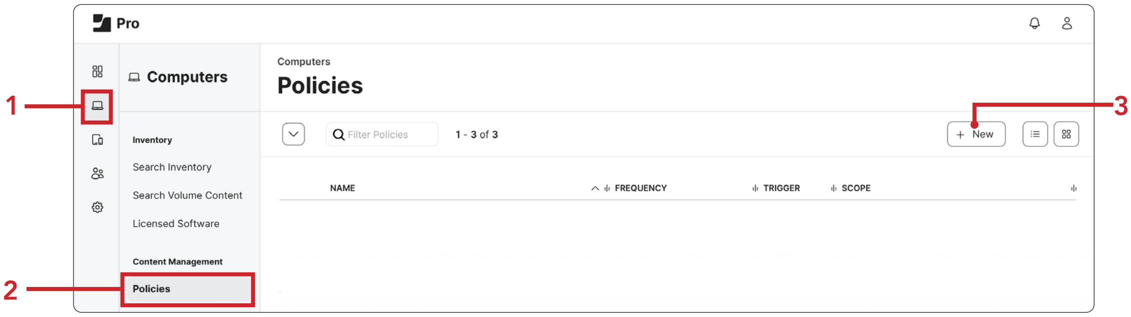
- Script flags: `--reset --check`
- Purpose: Clears previous results and runs a fresh audit.

For a listing of all the flags, have a look at the usage code block in the sequoia_cis_lvl2_compliance.sh

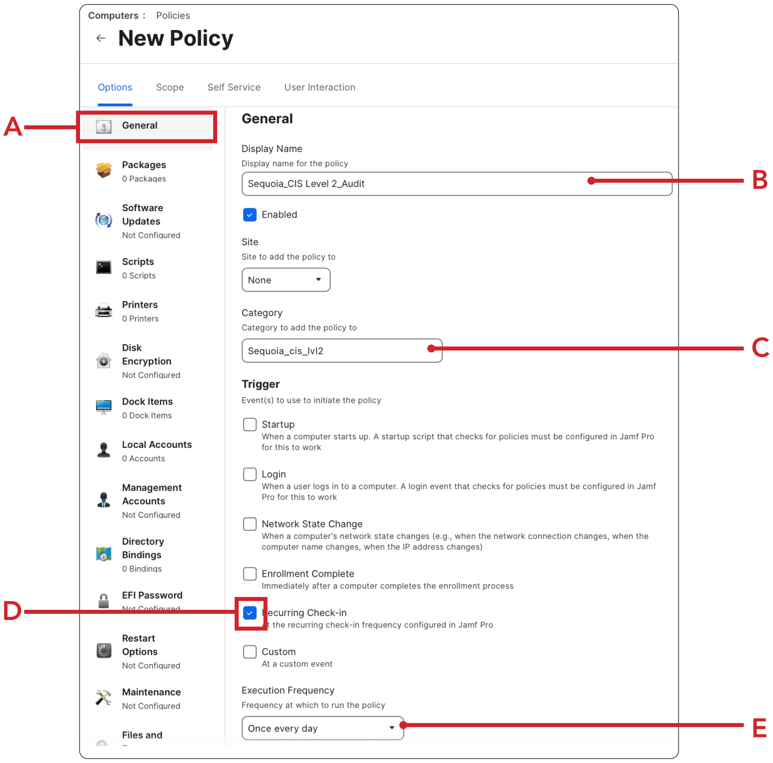


```
usage=(
    "$0 Usage"
    "$0 [--check] [--fix] [--cfc] [--stats] [--compliant] [--non_compliant] [--reset] [--reset-all] [--quiet=<value>]"
    " "
    "Optional parameters:"
    "--check            :   run the compliance checks without interaction"
    "--fix              :   run the remediation commands without interaction"
    "--cfc              :   runs a check, fix, check without interaction"
    "--stats            :   display the statistics from last compliance check"
    "--compliant        :   reports the number of compliant checks"
    "--non_compliant    :   reports the number of non_compliant checks"
    "--reset            :   clear out all results for current baseline"
    "--reset-all        :   clear out all results for ALL MSCP baselines"
    "--quiet=<value>    :   1 - show only failed and exempted checks in output"
    "                       2 - show minimal output"
  )
```

1. Click Computers.
2. Click Policies.
3. Click New.



4. Configure the following:
   A. Click General.
   B. For the Display Name, enter: **Sequoia_CIS Level 2_Audit.**
   C. Category: **Sequoia_CIS Level 2_Audit.**
   D. Set the Trigger: **Recurring Check-in.**
   E. Select an execution frequency of your choosing. This guide will choose **Once Every Day.**



General

Display Name
Display name for the policy
Sequoia_CIS Level 2_Audit

☑ Enabled

Site
Site to add the policy to
None

Category
Category to add the policy to
Sequoia_cis_lvl2

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 event 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

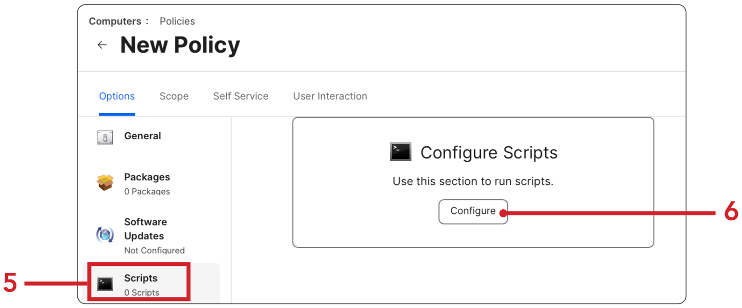
☑ Recurring Check-in
At the recurring check-in frequency configured in Jamf Pro

☐ Custom
At a custom event

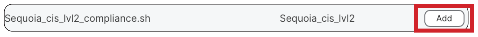
Execution Frequency
Frequency at which to run the policy
Once every day

5. Select Scripts.

6. Click Configure.

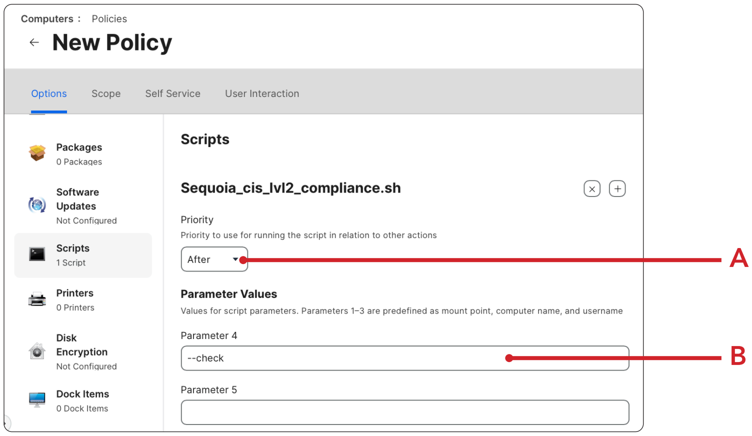


7. Find the sequoia_cis_lvl2_compliance.sh and click Add.



Sequoia_cis_lvl2_compliance.sh	Sequoia_cis_lvl2	Add

8. Configure the following:
    A. Set the Priority: **After**
    B. Parameter 4, enter: **--check**
        NOTE: A the --check flag runs a compliance check without user interaction.



Computers : Policies

← **New Policy**

Options | Scope | Self Service | User Interaction

Packages
0 Packages

Software Updates
Not Configured

Scripts
1 Script

Printers
0 Printers

Disk Encryption
Not Configured

Dock Items
0 Dock Items

Scripts

Sequoia_cis_lvl2_compliance.sh

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

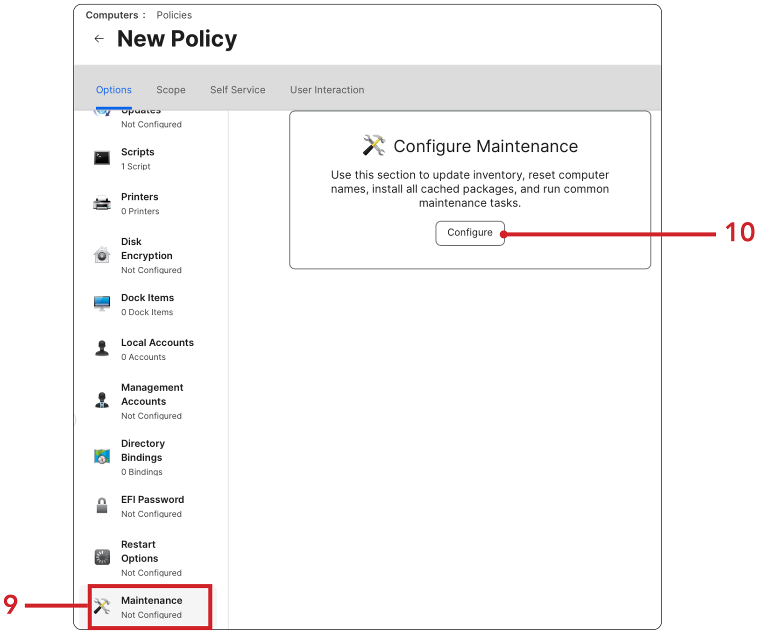
Parameter Values
Values for script parameters. Parameters 1–3 are predefined as mount point, computer name, and username

Parameter 4
--check

Parameter 5

9. Scroll down and click Maintenance.

10. Click Configure.



Computers : Policies

← **New Policy**

Options | Scope | Self Service | User Interaction

Updates
Not Configured

Scripts
1 Script

Printers
0 Printers

Disk Encryption
Not Configured

Dock Items
0 Dock Items

Local Accounts
0 Accounts

Management Accounts
Not Configured

Directory Bindings
0 Bindings

EFI Password
Not Configured

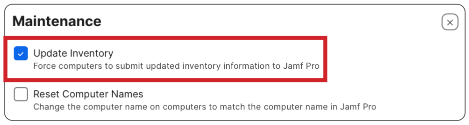
Restart Options
Not Configured

Maintenance
Not Configured

Configure Maintenance

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

11. Confirm the the checkbox is selected for Update Inventory.



Maintenance

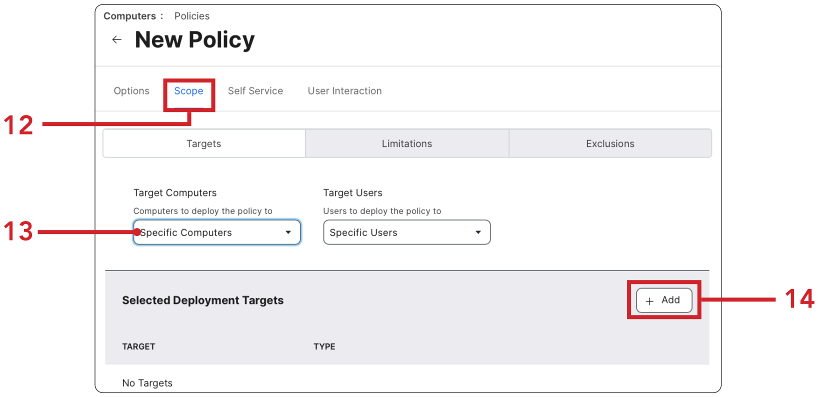
☑ Update Inventory
Force computers to submit updated inventory information to Jamf Pro

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

12. Click Scope.

13. Confirm Specific Computers is selected for Target Computers.

14. Click Add.



Target Computers
Computers to deploy the policy to
Specific Computers

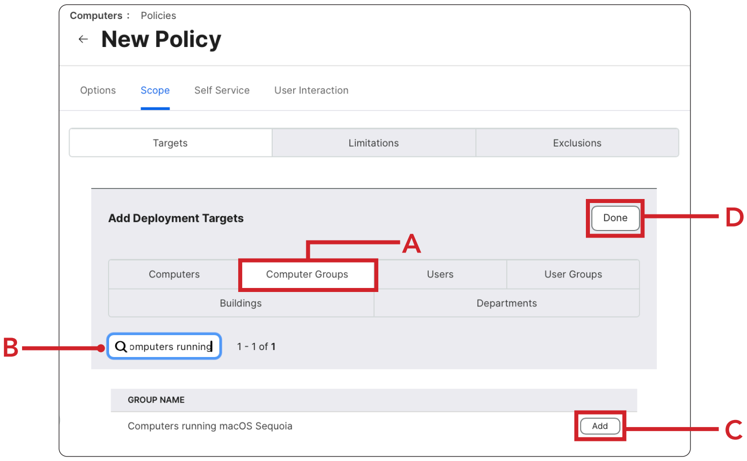
Target Users
Users to deploy the policy to
Specific Users

Selected Deployment Targets

No Targets

15. Perform the following:

A. Select Computer Groups.
B. In the search field, enter **computers running**.
C. Click Add for the group named Computers running macOS Sequoia.
D. Click Done.



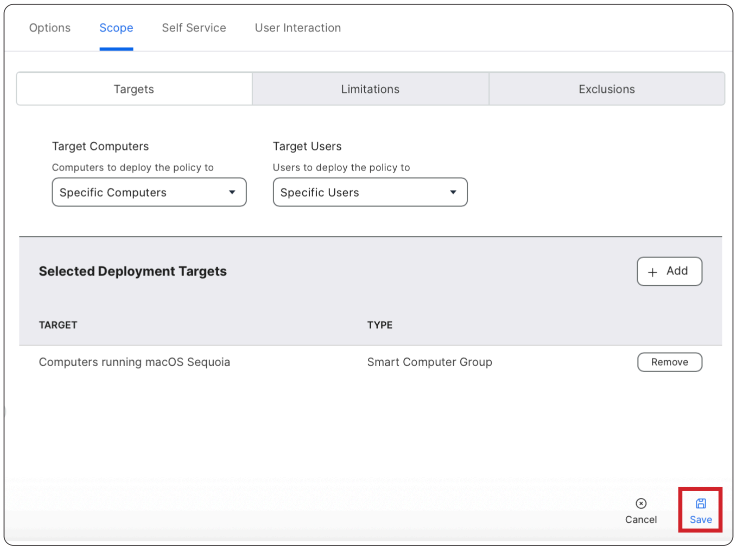
Add Deployment Targets

omputers running

1 - 1 of 1

Computers running macOS Sequoia

16. Click Save.



Options | Scope | Self Service | User Interaction

Targets | Limitations | Exclusions

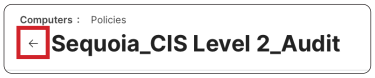
Target Computers
Computers to deploy the policy to
Specific Computers

Target Users
Users to deploy the policy to
Specific Users

Selected Deployment Targets

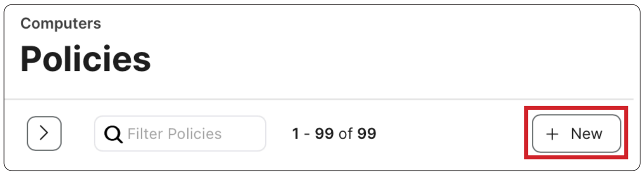
TARGET	TYPE
Computers running macOS Sequoia	Smart Computer Group

17. Click Previous (←).



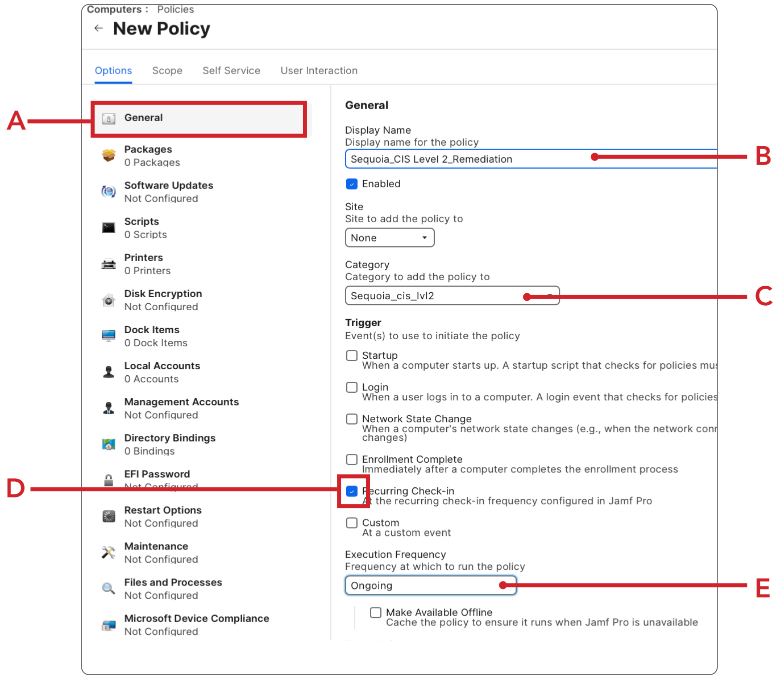
Computers : Policies
Sequoia_CIS Level 2_Audit

18. Click New (+).



Computers
Policies

19. Configure the following:
    A. Select General.
    B. Enter **Sequoia_CIS Level 2_Remediation** for the Display Name.
    C. Select **Sequoia_CIS Level 2_Audit** for the Category
    D. Select the checkbox for **Recurring Check-in.**
    E. Select **Ongoing** for Execution Frequency



General

Display Name
Display name for the policy
Sequoia_CIS Level 2_Remediation

☑ Enabled

Site
Site to add the policy to
None

Category
Category to add the policy to
Sequoia_cis_lvl2

Trigger
Event(s) to use to initiate the policy

☐ Startup
When a computer starts up. A startup script that checks for policies mu

☐ Login
When a user logs in to a computer. A login event that checks for policies

☐ Network State Change
When a computer's network state changes (e.g., when the network conn changes)

☐ Enrollment Complete
Immediately after a computer completes the enrollment process

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

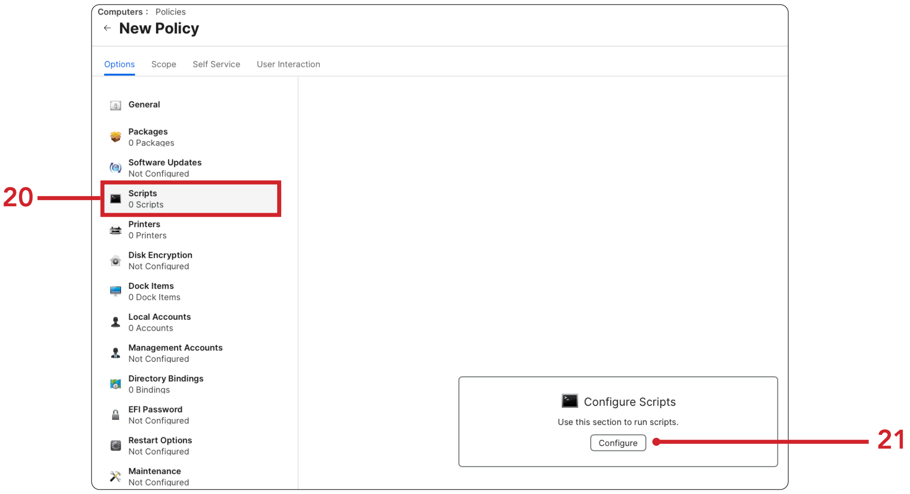
☐ Custom
At a custom event

Execution Frequency
Frequency at which to run the policy
Ongoing

☐ Make Available Offline
Cache the policy to ensure it runs when Jamf Pro is unavailable

20. Click Scripts.

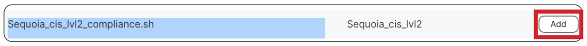
21. Click Configure.



Configure Scripts

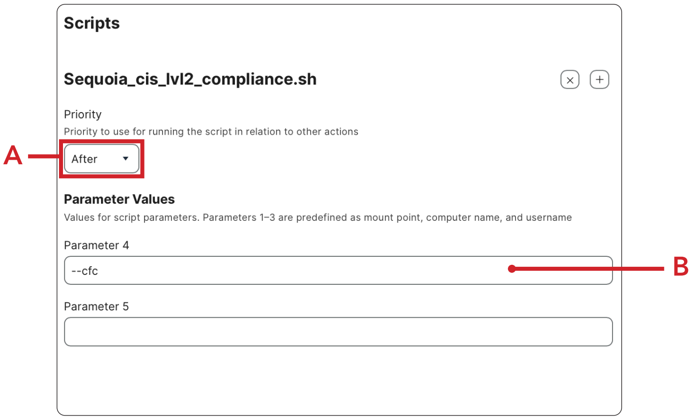
Use this section to run scripts.

22. Locate sequoia_cis_lvl2_compliance.sh and click Add.



Sequoia_cis_lvl2_compliance.sh Sequoia_cis_lvl2

23. Configure the following:
    A. Priority: **After.**
    B. Parameter 4: **--cfc.**
    NOTE: The --cfc flag runs a compliance check, fixes anything that is not compliant, then run another check. It does all of this without any user interaction and it part of the compliance script.



Scripts

Sequoia_cis_lvl2_compliance.sh

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

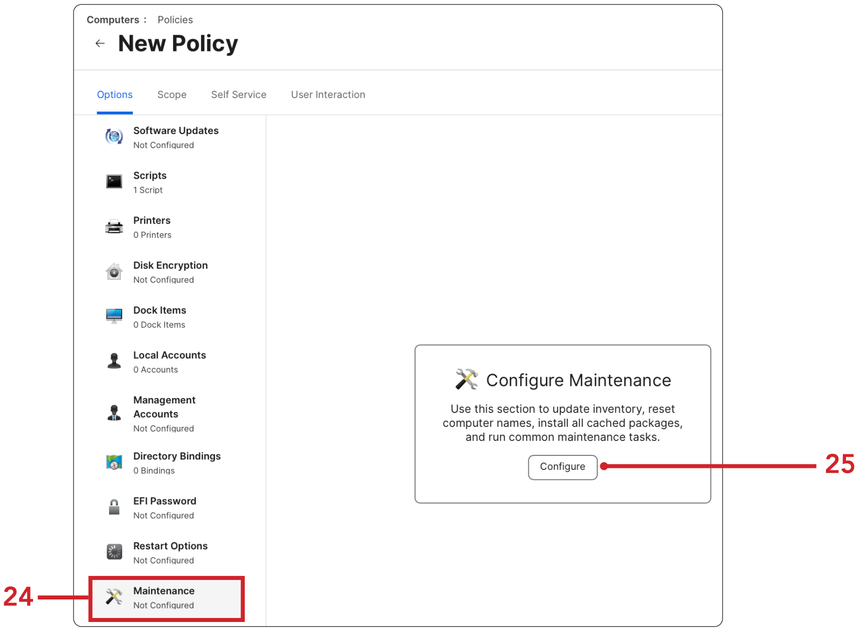
Parameter Values
Values for script parameters. Parameters 1–3 are predefined as mount point, computer name, and username

Parameter 4
--cfc

Parameter 5

24. Scroll down and select Maintenance.

25. Click Configure.



Software Updates
Not Configured

Scripts
1 Script

Printers
0 Printers

Disk Encryption
Not Configured

Dock Items
0 Dock Items

Local Accounts
0 Accounts

Management Accounts
Not Configured

Directory Bindings
0 Bindings

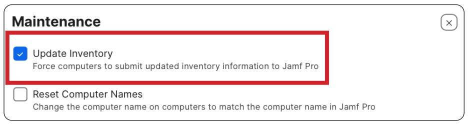
EFI Password
Not Configured

Restart Options
Not Configured

Maintenance
Not Configured

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

26. Confirm the checkbox is selected for Update Inventory.



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

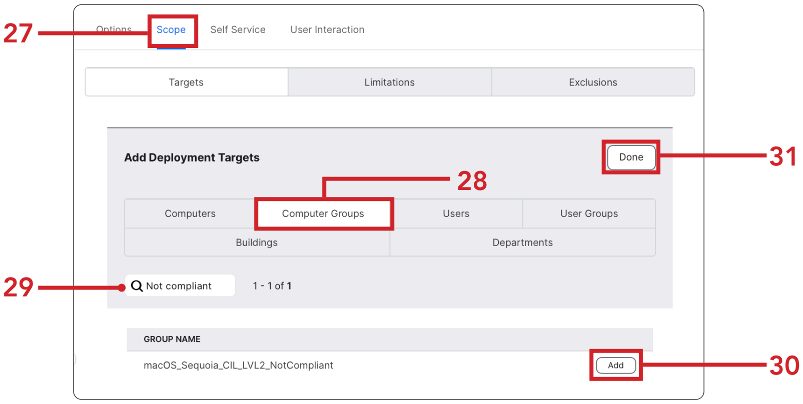
27. Click Scope.

28. Click Computer Groups.

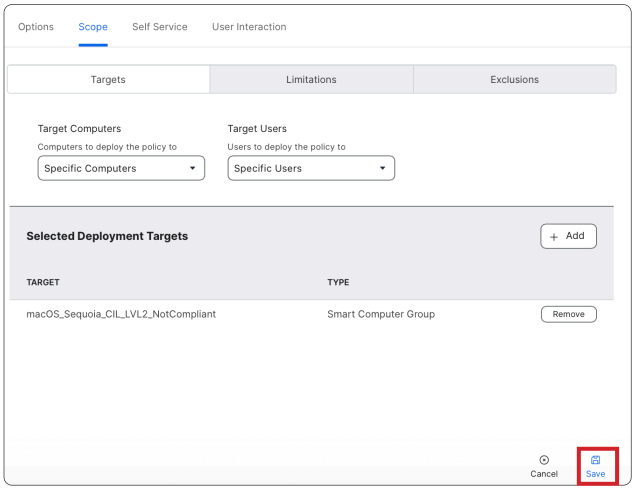
29. In the search field, enter: **not compliant**

30. Click Add for the group named: **macOS_Sequoia_CIL_LVL2_NotCompliant.**

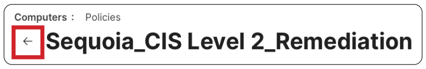
31. Click Done.



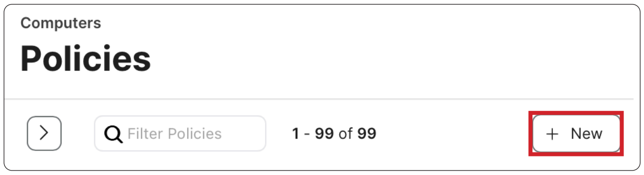
32. Click Save.



33. Click Previous (←).



34. Click New (+).


Computers

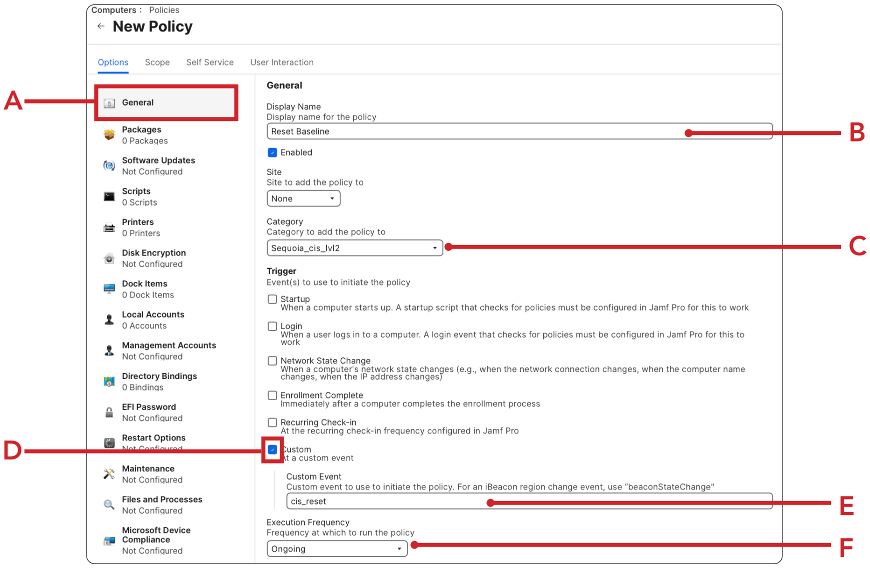
Policies

Filter Policies 1 - 99 of 99 + New

35. Configure the following:
   A. Select General.
   B. Enter **Reset Baseline** for the Display Name:
   C. Select **Sequoia_CIS Level 2_Audit** for the Category.
   D. Select the checkbox for **Custom** under Trigger.
   E. Enter **cis_reset** for Custom Event
   F. Select **Ongoing** for Execution Frequency

NOTE: This policy needs to be run manually either by offering it in Self Service or by running the command:

```
sudo jamf policy -event cis_reset
```



Computers : Policies

New Policy

Options Scope Self Service User Interaction

General

Packages 0 Packages

Software Updates Not Configured

Scripts 0 Scripts

Printers 0 Printers

Disk Encryption Not Configured

Dock Items 0 Dock Items

Local Accounts 0 Accounts

Management Accounts Not Configured

Directory Bindings 0 Bindings

EFI Password Not Configured

Restart Options Not Configured

Maintenance Not Configured

Files and Processes Not Configured

Microsoft Device Compliance Not Configured

General

Display Name
Display name for the policy
Reset Baseline

☑ Enabled

Site
Site to add the policy to
None

Category
Category to add the policy to
Sequoia_cis_lvl2

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 event 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

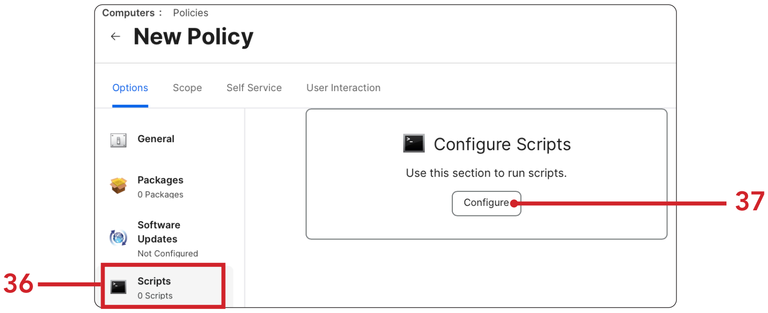
☑ Custom
At a custom event

Custom Event
Custom event to use to initiate the policy. For an iBeacon region change event, use "beaconStateChange"
cis_reset

Execution Frequency
Frequency at which to run the policy
Ongoing

36. Click Scripts.

37. Click Configure.



Computers : Policies

New Policy

Options Scope Self Service User Interaction

General

Packages 0 Packages

Software Updates Not Configured

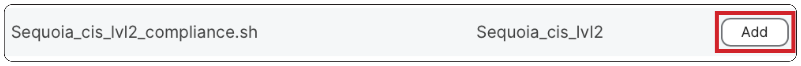
Scripts 0 Scripts

Configure Scripts

Use this section to run scripts.

Configure

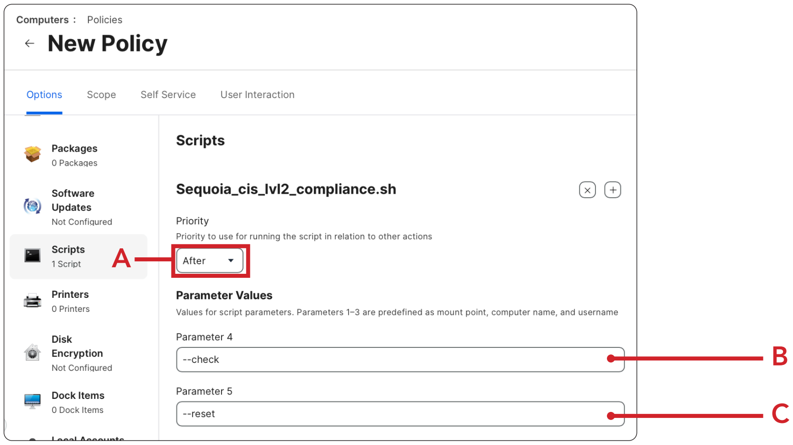
38. Find the sequoia_cis_lvl2_compliance.sh and click Add.



Sequoia_cis_lvl2_compliance.sh Sequoia_cis_lvl2

39. Configure the following:

A. Priority: After.
B. Parameter 4: **--check**.
C. Parameter 5: **--reset**.



Computers : Policies

New Policy

Options Scope Self Service User Interaction

Packages
0 Packages

Software Updates
Not Configured

Scripts
1 Script

Printers
0 Printers

Disk Encryption
Not Configured

Dock Items
0 Dock Items

Local Accounts

Scripts

Sequoia_cis_lvl2_compliance.sh

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

After

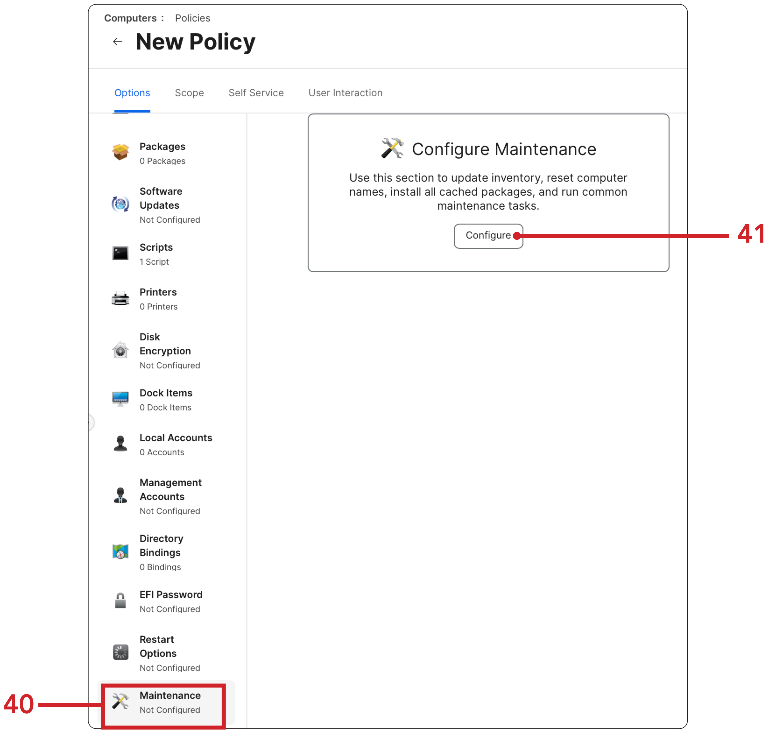
Parameter Values
Values for script parameters. Parameters 1–3 are predefined as mount point, computer name, and username

Parameter 4
--check

Parameter 5
--reset

40. Click Maintenance.

41. Click Configure.



Computers : Policies

New Policy

Options Scope Self Service User Interaction

Packages
0 Packages

Software Updates
Not Configured

Scripts
1 Script

Printers
0 Printers

Disk Encryption
Not Configured

Dock Items
0 Dock Items

Local Accounts
0 Accounts

Management Accounts
Not Configured

Directory Bindings
0 Bindings

EFI Password
Not Configured

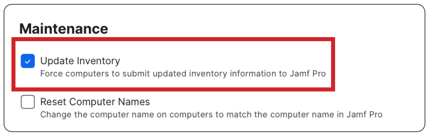
Restart Options
Not Configured

Maintenance
Not Configured

Configure Maintenance

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

42. Confirm the the checkbox is selected for Update Inventory.



Maintenance

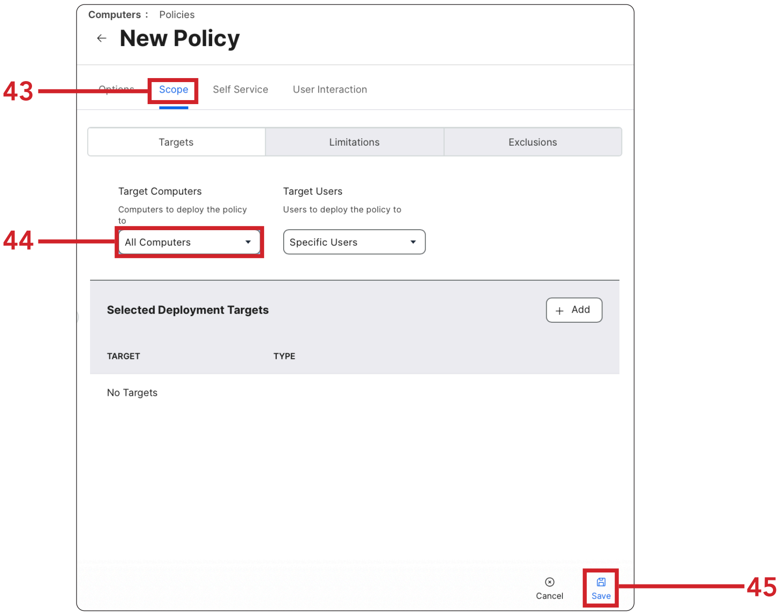
☑ Update Inventory
Force computers to submit updated inventory information to Jamf Pro

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

43. Click Scope.

44. Select "All Computers" for Target Computers.

45. Click Save.
NOTE: When testing your initial configuration you may make changes before settling a final baseline. During this time you might need to reset the plist which the EAs use to calculate compliance. We are scoping this to all computers just to be safe.



Computers : Policies

New Policy

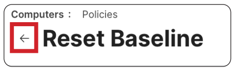
Target Computers
Computers to deploy the policy to
All Computers

Target Users
Users to deploy the policy to
Specific Users

Selected Deployment Targets

TARGET	TYPE
No Targets	

46. Click Previous (←).

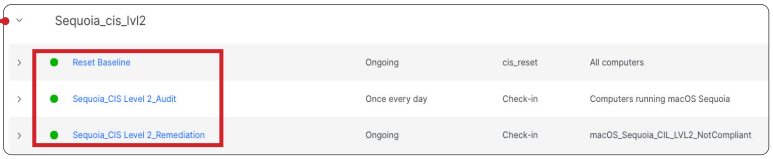


Computers : Policies

Reset Baseline

47. Go to the Sequoia_cis_lvl2 category.

48. Confirm all three policies have been created as shown below.



Expand the category to view the policies

Sequoia_cis_lvl2

● Reset Baseline	Ongoing	cis_reset	All computers
● Sequoia_CIS Level 2_Audit	Once every day	Check-in	Computers running macOS Sequoia
● Sequoia_CIS Level 2_Remediation	Ongoing	Check-in	macOS_Sequoia_CIL_LVL2_NotCompliant

This completes this section. In the next section, we will create a custom JSON schema to be used by the extension attributes and the scripts created earlier in this guide.

Section 5: Configure a JSON Schema

What You'll Need:
Learn what hardware, software, and information you'll need to complete the tutorials in this section.

Hardware and Software:
Requirements for following along with this section:

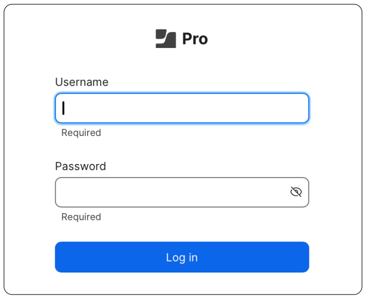
- A Jamf Pro server with administrative privileges

Jamf Compliance Editor (JCE) includes a feature that generates a JSON schema, allowing admins to manage exemptions without recreating or re-uploading the full compliance guidance. This schema can be used in a custom application settings configuration profile, which the compliance script and Extension Attributes read to apply approved rule exemptions—ensuring accurate compliance checks without inflating result counts.

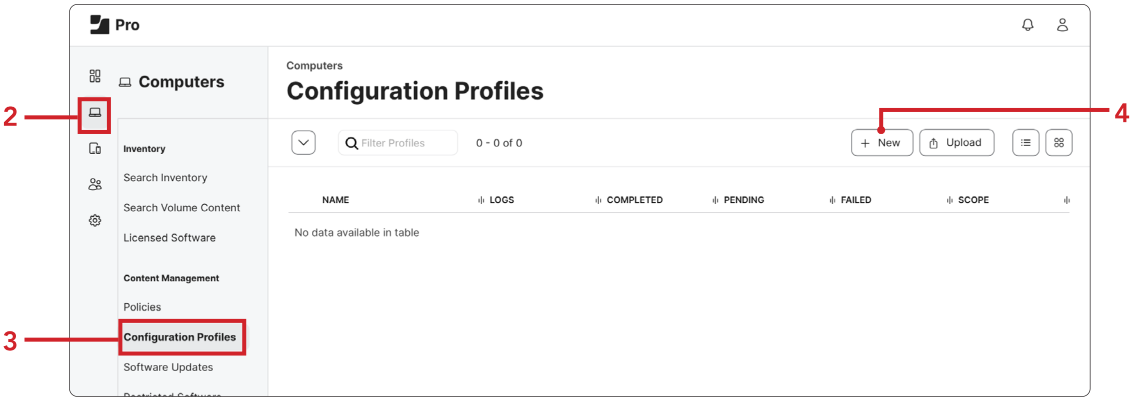
Earlier in the guide, we created an Extension Attribute called "Compliance – Failed Result List." When a JSON schema is used to manage exemptions, those exemptions will still appear in the "Compliance – Failed Result List."

In this section we will create a configuration profile using a custom JSON schema that defines exemptions for specific compliance rules.

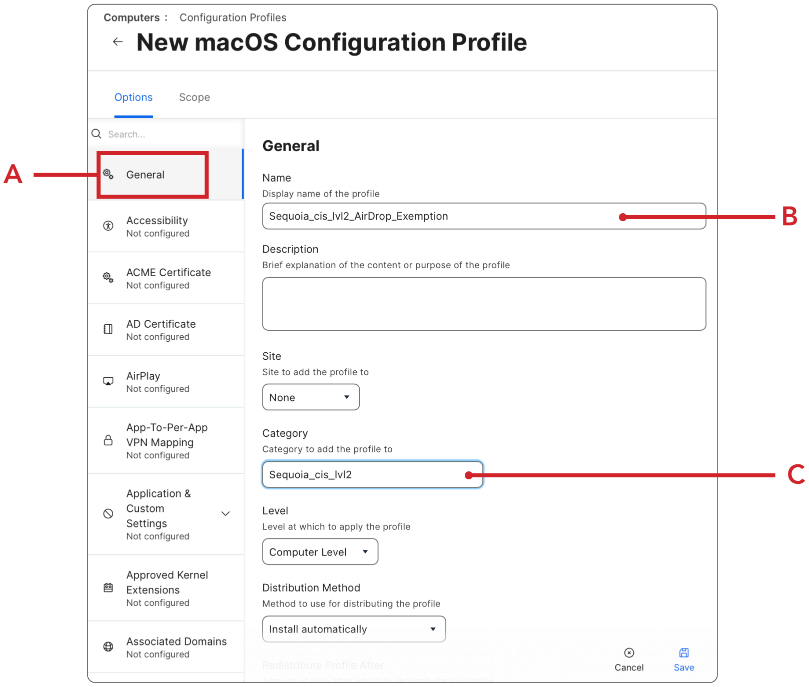
1. If necessary, Log into your Jamf Pro Server with administrative privileges.



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



5. Configure the following:
   A. Select the General Payload.
   B. Enter **Sequoia_cis_lvl2_AirDrop_Exemption** for the Name.
   C. Select **Sequoia_cis_lvl2** for the Category.



Computers : Configuration Profiles

← New macOS Configuration Profile

Options Scope

Search...

- General
- Accessibility — Not configured
- ACME Certificate — Not configured
- AD Certificate — Not configured
- AirPlay — Not configured
- App-To-Per-App VPN Mapping — Not configured
- Application & Custom Settings — Not configured
- Approved Kernel Extensions — Not configured
- Associated Domains — Not configured

General

Name
Display name of the profile
Sequoia_cis_lvl2_AirDrop_Exemption

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
Sequoia_cis_lvl2

Level
Level at which to apply the profile
Computer Level

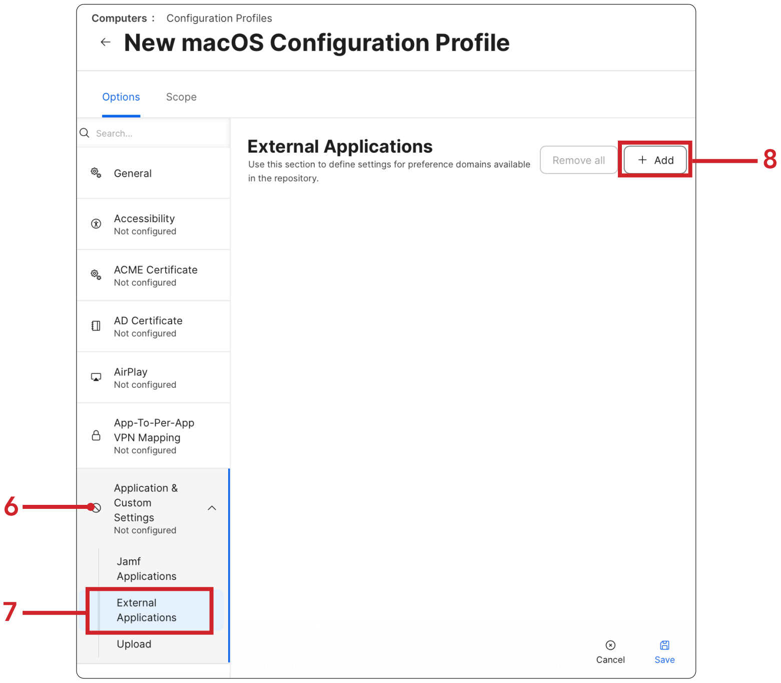
Distribution Method
Method to use for distributing the profile
Install automatically

Redistribute Profile After

6. Scroll down and select the Application & Custom Settings Payload.

7. Click External Applications.

8. Click Add (+).



Computers : Configuration Profiles

← New macOS Configuration Profile

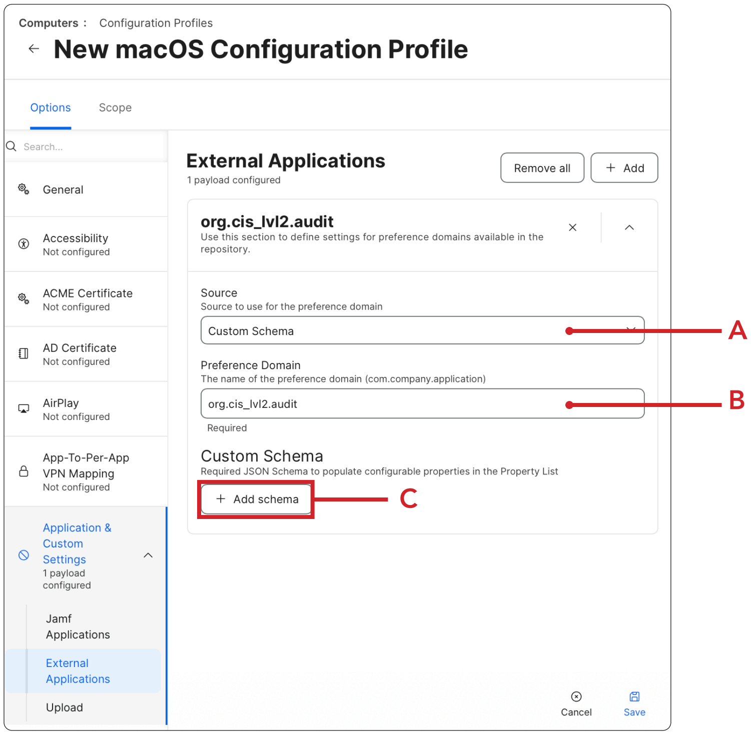
Options Scope

Search...

- General
- Accessibility — Not configured
- ACME Certificate — Not configured
- AD Certificate — Not configured
- AirPlay — Not configured
- App-To-Per-App VPN Mapping — Not configured
- Application & Custom Settings — Not configured
  - Jamf Applications
  - External Applications
  - Upload

External Applications
Use this section to define settings for preference domains available in the repository.

9. Configure the following:
    A. Source: Select **Custom Schema.**
    B. Preference Domain: enter **org.cis_lvl2.audit.**
    C. Click **Add schema.**



Computers : Configuration Profiles

New macOS Configuration Profile

Options Scope

Search...

General

Accessibility
Not configured

ACME Certificate
Not configured

AD Certificate
Not configured

AirPlay
Not configured

App-To-Per-App VPN Mapping
Not configured

Application & Custom Settings
1 payload configured

Jamf Applications

External Applications

Upload

External Applications
1 payload configured

Remove all | + Add

org.cis_lvl2.audit
Use this section to define settings for preference domains available in the repository.

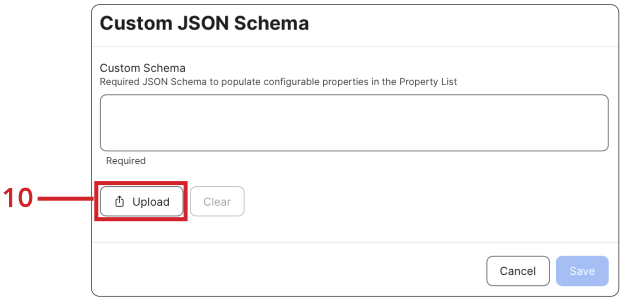
Source
Source to use for the preference domain
Custom Schema

Preference Domain
The name of the preference domain (com.company.application)
org.cis_lvl2.audit
Required

Custom Schema
Required JSON Schema to populate configurable properties in the Property List
+ Add schema

Cancel | Save

10.Click Upload.



Custom JSON Schema

Custom Schema
Required JSON Schema to populate configurable properties in the Property List

Required

Upload | Clear

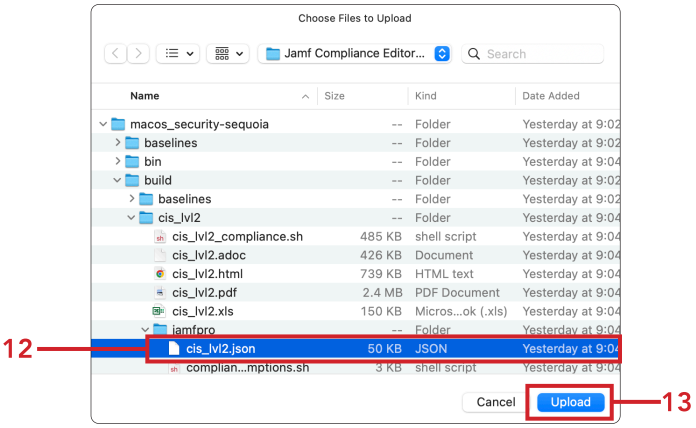
Cancel | Save

11. Navigate to: ~/Desktop/Jamf Compliance Editor - macOS Sequoia/macos_security-sequoia/build/cis_lvl2/jamfpro/

    NOTE: The **Jamf Compliance Editor - macOS Sequoia** folder was created on your Desktop in Section 2 of this guide.

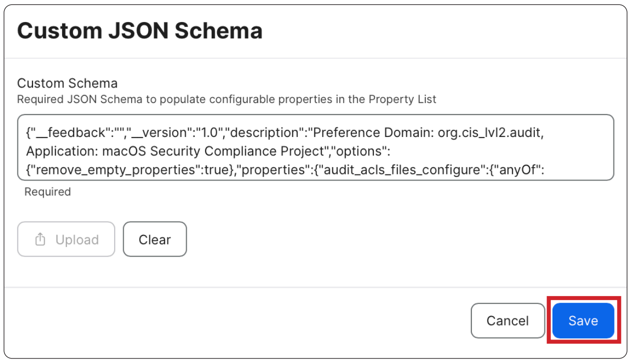
12. Select the **cis_lvl2.json** file.

13. Click Upload.



Name	Size	Kind	Date Added
macos_security-sequoia	--	Folder	Yesterday at 9:02
baselines	--	Folder	Yesterday at 9:02
bin	--	Folder	Yesterday at 9:04
build	--	Folder	Yesterday at 9:02
baselines	--	Folder	Yesterday at 9:02
cis_lvl2	--	Folder	Yesterday at 9:04
cis_lvl2_compliance.sh	485 KB	shell script	Yesterday at 9:04
cis_lvl2.adoc	426 KB	Document	Yesterday at 9:04
cis_lvl2.html	739 KB	HTML text	Yesterday at 9:04
cis_lvl2.pdf	2.4 MB	PDF Document	Yesterday at 9:04
cis_lvl2.xls	150 KB	Micros...ok (.xls)	Yesterday at 9:04
jamfpro	--	Folder	Yesterday at 9:04
cis_lvl2.json	50 KB	JSON	Yesterday at 9:04
complian...mptions.sh	3 KB	shell script	Yesterday at 9:04

14. Click Save.



Custom JSON Schema

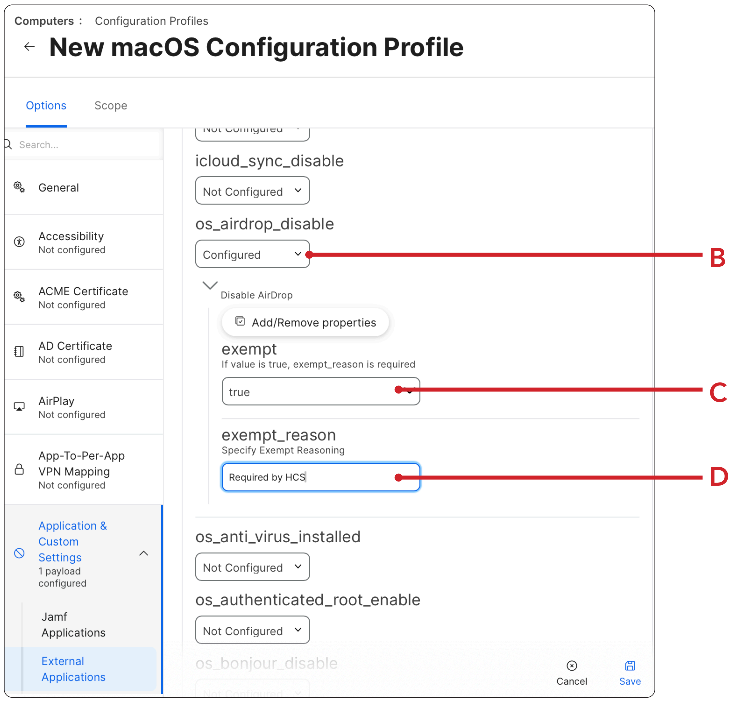
Custom Schema

Required JSON Schema to populate configurable properties in the Property List

{"__feedback":"","__version":"1.0","description":"Preference Domain: org.cis_lvl2.audit, Application: macOS Security Compliance Project","options":{"remove_empty_properties":true},"properties":{"audit_acls_files_configure":{"anyOf":

Required

15. Configure the following:
    A. Scroll down to os_airdrop_disable.
    B. Set it to **Configured.**
    C. Exempt: set to **true.**
    D. Exempt_reason: Enter a reason of your choosing. This guide will use **Required by HCS.**



Computers : Configuration Profiles

New macOS Configuration Profile

icloud_sync_disable: Not Configured

os_airdrop_disable: Configured

Disable AirDrop

exempt
If value is true, exempt_reason is required
true

exempt_reason
Specify Exempt Reasoning
Required by HCS

os_anti_virus_installed: Not Configured

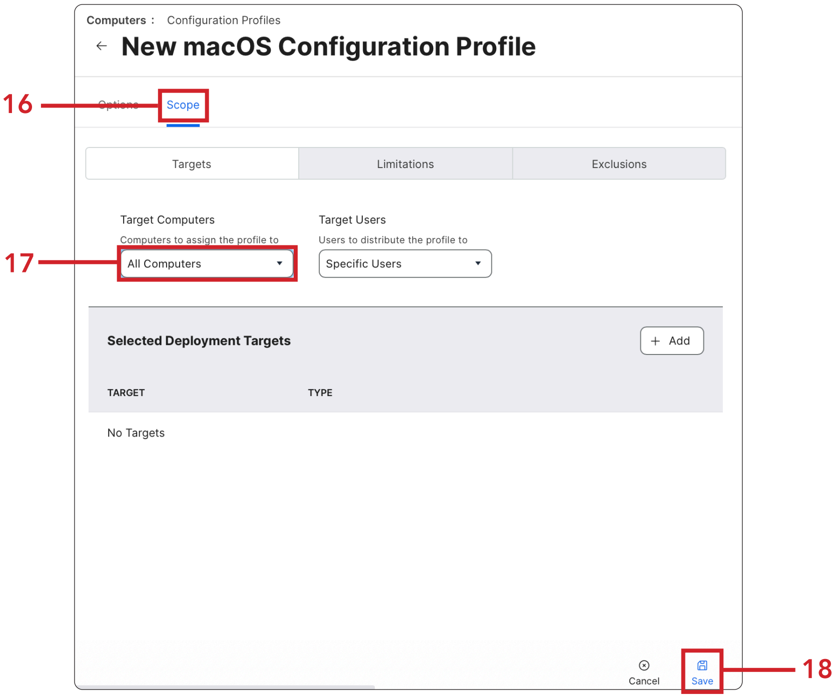
os_authenticated_root_enable: Not Configured

os_bonjour_disable

16.Click Scope.

17.Scope to your needs. This guide will scope to All Computers.

18. Click Save.


Computers : Configuration Profiles
New macOS Configuration Profile
16
Options
Scope
Targets
Limitations
Exclusions
Target Computers
Computers to assign the profile to
17
All Computers
Target Users
Users to distribute the profile to
Specific Users
Selected Deployment Targets
Add
TARGET
TYPE
No Targets
Cancel
Save
18

This completes this section. In the next section, we will scope the configuration profiles created by the Jamf Compliance Editor application.

Section 6: Scoping the JCE Computer Configuration Profiles

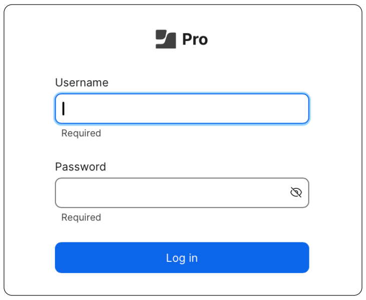
What You'll Need:
Learn what hardware, software, and information you'll need to complete the tutorials in this section.

Hardware and Software:
Requirements for following along with this section:

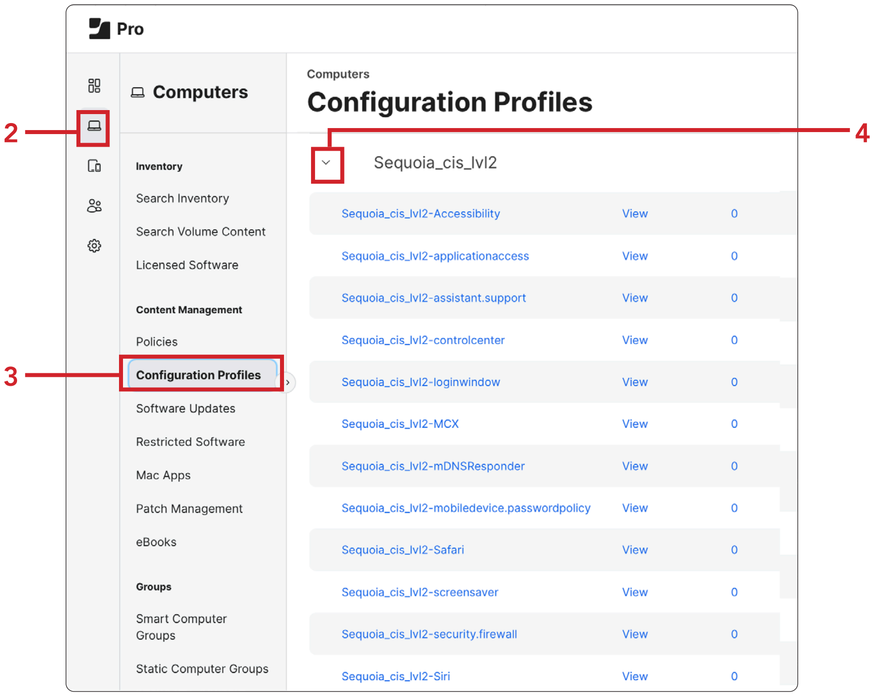
- A Jamf Pro server with administrative privileges

In this section, we'll create an Advanced Computer Search in Jamf Pro to generate reports. This allows administrators to identify which computers are compliant and which require remediation.

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

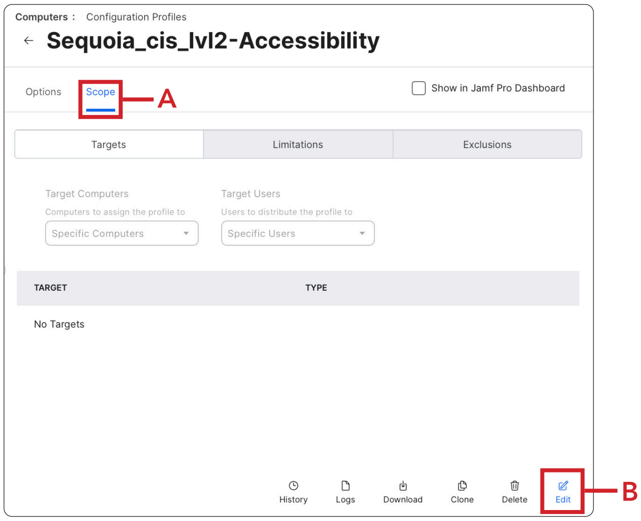


2. Click Computers.
3. Click Configuration Profiles.
4. Go to the Sequoia_cis_lvl2 category and expand the category to see all the computer configuration profiles that were created by the Jamf Compliance Editor application. Notice none of the computer configuration profiles are scoped. We need to scope all of them to the smart group named Computers running macOS Sequoia.



Sequoia_cis_lvl2-Accessibility	View	0
Sequoia_cis_lvl2-applicationaccess	View	0
Sequoia_cis_lvl2-assistant.support	View	0
Sequoia_cis_lvl2-controlcenter	View	0
Sequoia_cis_lvl2-loginwindow	View	0
Sequoia_cis_lvl2-MCX	View	0
Sequoia_cis_lvl2-mDNSResponder	View	0
Sequoia_cis_lvl2-mobiledevice.passwordpolicy	View	0
Sequoia_cis_lvl2-Safari	View	0
Sequoia_cis_lvl2-screensaver	View	0
Sequoia_cis_lvl2-security.firewall	View	0
Sequoia_cis_lvl2-Siri	View	0

5. Select the first computer configuration profile in the list. Perform the following:
    A. Click Scope.
    B. Click Edit.



Computers : Configuration Profiles

Sequoia_cis_lvl2-Accessibility

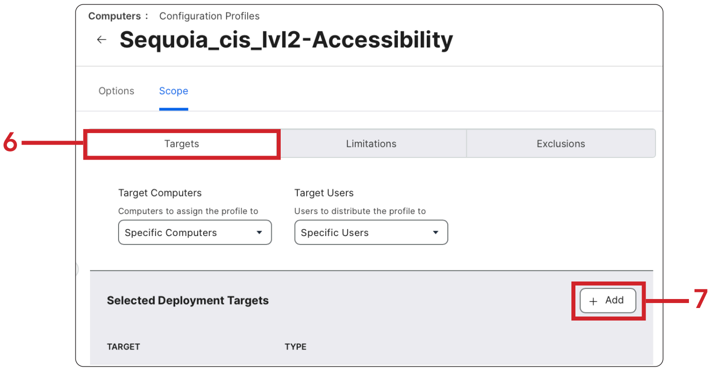
Target Computers — Computers to assign the profile to: Specific Computers

Target Users — Users to distribute the profile to: Specific Users

TARGET	TYPE
No Targets	

6. Click Targets.

7. Click Add.



Computers : Configuration Profiles

Sequoia_cis_lvl2-Accessibility

Target Computers — Computers to assign the profile to: Specific Computers

Target Users — Users to distribute the profile to: Specific Users

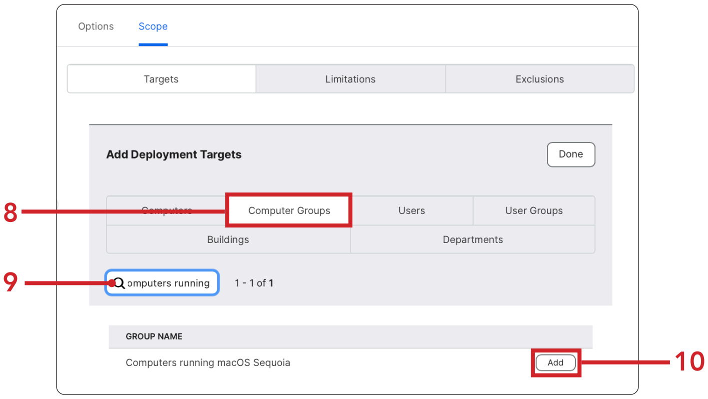
Selected Deployment Targets

TARGET	TYPE

8. Click **Computer Groups**.

9. In the search field, enter: **computers running.**

10. Click Add for the group named: **Computers running macOS Sequoia.**

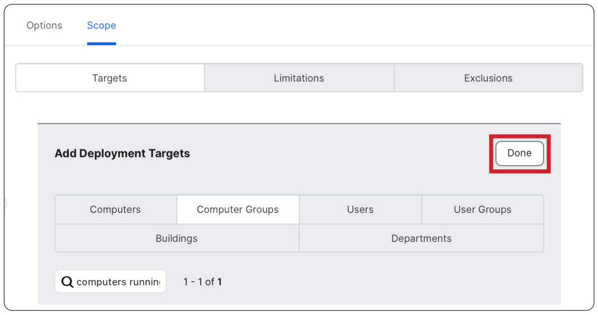


Add Deployment Targets

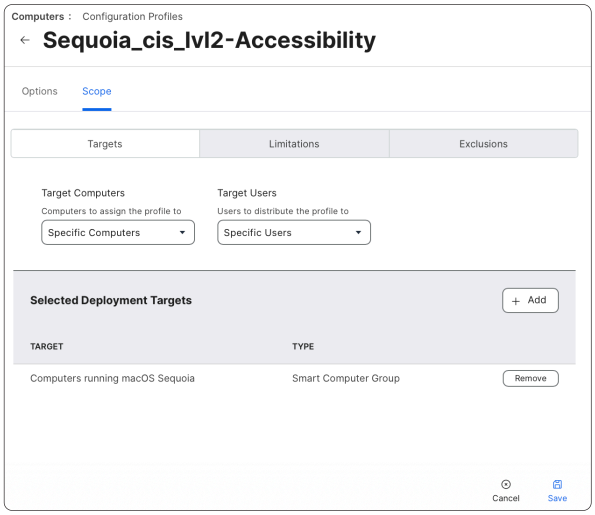
omputers running   1 - 1 of 1

GROUP NAME	
Computers running macOS Sequoia	Add

11. Click Done.



12. Click Save.


Computers : Configuration Profiles
Sequoia_cis_lvl2-Accessibility
Options
Scope
Targets
Limitations
Exclusions
Add
Remove
Cancel
Save

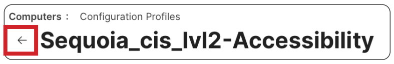
Target Computers
Computers to assign the profile to
Specific Computers

Target Users
Users to distribute the profile to
Specific Users

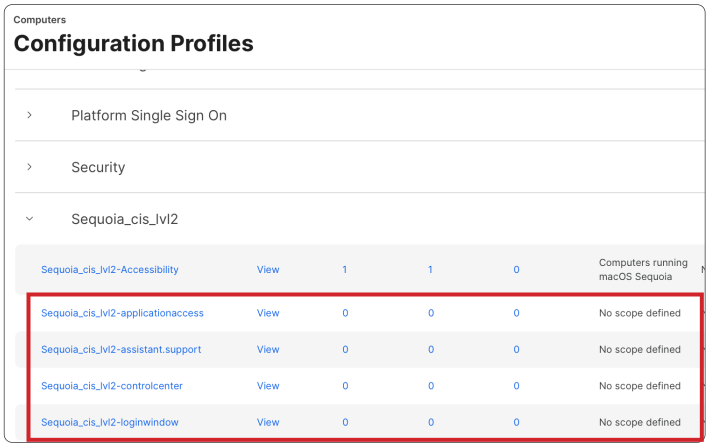
Selected Deployment Targets

TARGET	TYPE
Computers running macOS Sequoia	Smart Computer Group

13. Click Previous (←).


Computers : Configuration Profiles
Sequoia_cis_lvl2-Accessibility

14. Repeat steps 4 - 13 for the remaining computer configuration profiles. They should all be scoped to Computers running macOS Sequoia when done.



Sequoia_cis_lvl2-Accessibility	View	1	1	0	Computers running macOS Sequoia
Sequoia_cis_lvl2-applicationaccess	View	0	0	0	No scope defined
Sequoia_cis_lvl2-assistant.support	View	0	0	0	No scope defined
Sequoia_cis_lvl2-controlcenter	View	0	0	0	No scope defined
Sequoia_cis_lvl2-loginwindow	View	0	0	0	No scope defined

This completes this section. In the next section, we will create an Advanced Computer Search for reporting.

Section 7: Creating an Advanced computer Search

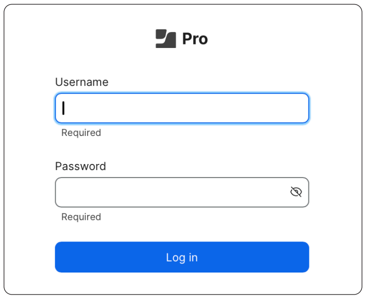
What You'll Need:
Learn what hardware, software, and information you'll need to complete the tutorials in this section.

Hardware and Software:
Requirements for following along with this section:

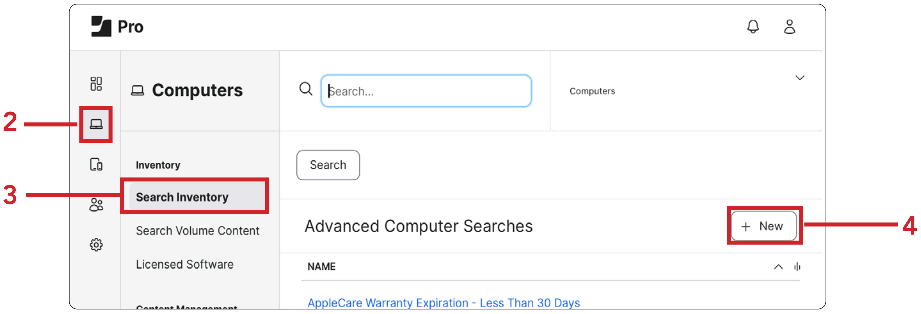
- A Jamf Pro server with administrative privileges

In this section we will create an Advanced Computer Search to run reports.

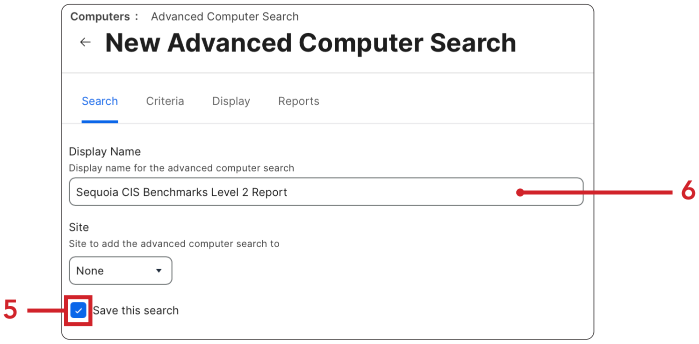
1. If necessary, Log into your Jamf Pro Server with administrative privileges.



2. Click Computers.
3. Click Search Inventory.
4. Click New.



5. Select the checkbox for Save this search.
6. Enter **Sequoia CIS Benchmarks Level 2** Report for the Display Name.


Computers : Advanced Computer Search
New Advanced Computer Search
Search
Criteria
Display
Reports
6
5

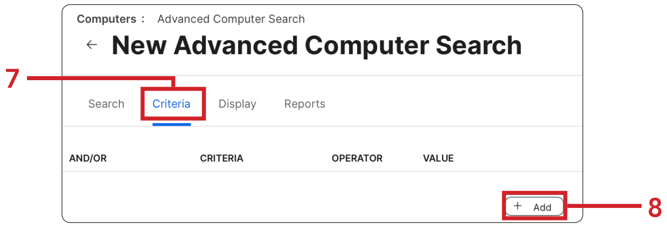
Display Name
Display name for the advanced computer search
Sequoia CIS Benchmarks Level 2 Report

Site
Site to add the advanced computer search to
None

☑ Save this search

7. Click Criteria.

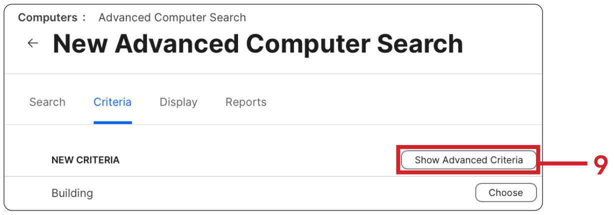
8. Click Add.



Computers : Advanced Computer Search

New Advanced Computer Search

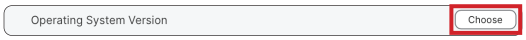
9. Click Show Advanced Criteria.



Computers : Advanced Computer Search

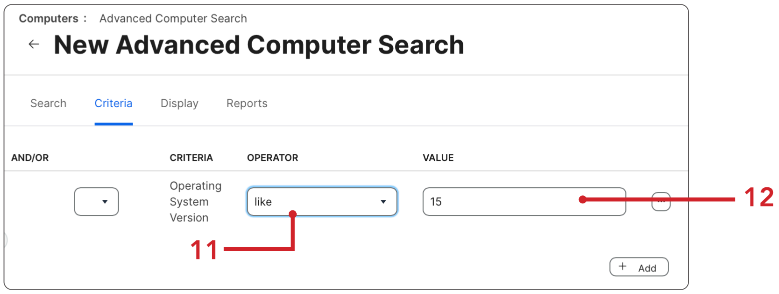
New Advanced Computer Search

10. Find Operating System Version and click Choose.



11. Select **like** for the Operator.

12. Enter **15** for the Value.



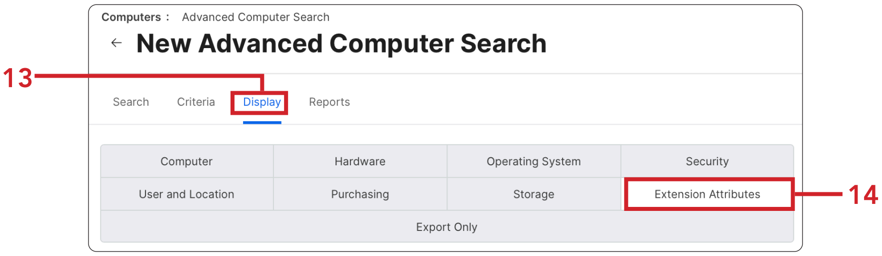
Computers : Advanced Computer Search

New Advanced Computer Search

AND/OR	CRITERIA	OPERATOR	VALUE
	Operating System Version	like	15

13. Click Display.

14. Click Extension Attributes.

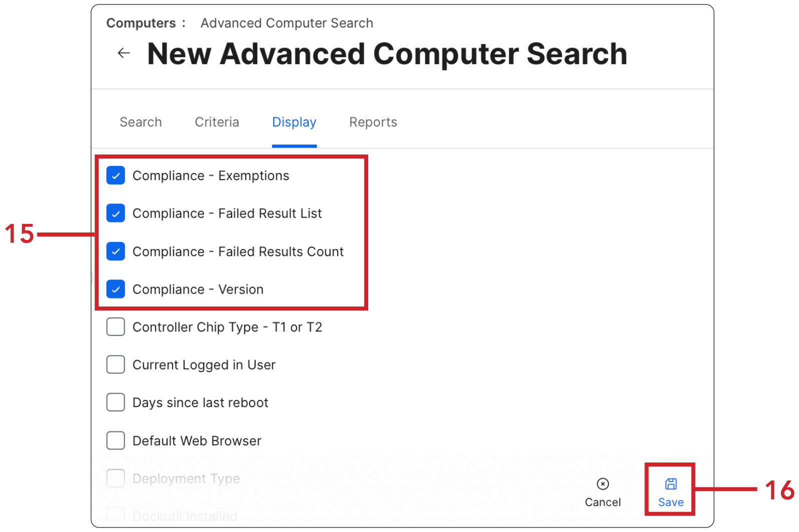


Computers : Advanced Computer Search

New Advanced Computer Search

15. Select the following extension attributes:
    - Compliance - Exemptions
    - Compliance - Failed Result List
    - Compliance - Failed Results Count
    - Compliance - Version

16. Click Save



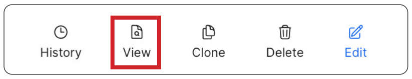
Computers : Advanced Computer Search

← **New Advanced Computer Search**

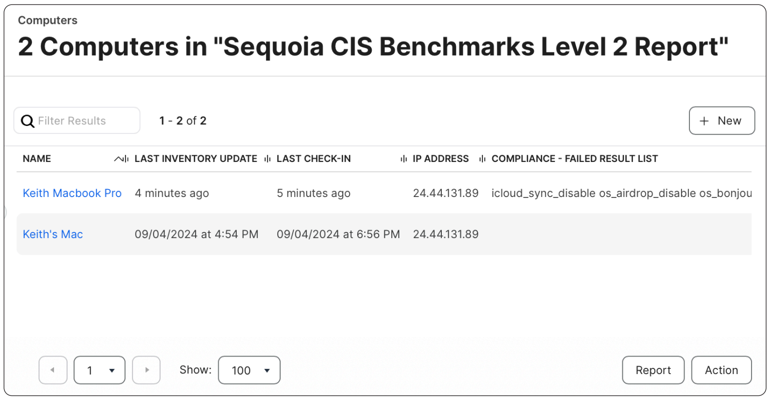
Search | Criteria | Display | Reports

☑ Compliance - Exemptions
☑ Compliance - Failed Result List
☑ Compliance - Failed Results Count
☑ Compliance - Version
□ Controller Chip Type - T1 or T2
□ Current Logged in User
□ Days since last reboot
□ Default Web Browser
□ Deployment Type
□ Dockutil Installed

17. Click View.



18. A list of complaint computers will be shown. You have the option of creating a report showing the compliance of the organizations computers by clicking the report button. A report can be exported in .csv, tsv, or xml formats.



Computers

2 Computers in "Sequoia CIS Benchmarks Level 2 Report"

Filter Results 1 - 2 of 2 + New

NAME	LAST INVENTORY UPDATE	LAST CHECK-IN	IP ADDRESS	COMPLIANCE - FAILED RESULT LIST
Keith Macbook Pro	4 minutes ago	5 minutes ago	24.44.131.89	icloud_sync_disable os_airdrop_disable os_bonjou
Keith's Mac	09/04/2024 at 4:54 PM	09/04/2024 at 6:56 PM	24.44.131.89	

This completes this section. In the next section, we will use the Jamf Compliance Editor to create a CIS Level 2 Baseline for iOS devices.

Section 8: Creating a Jamf Compliance Editor CIS Level 2 Baseline for iOS.

What You'll Need:
Learn what hardware, software, and information you'll need to complete the tutorials in this section.

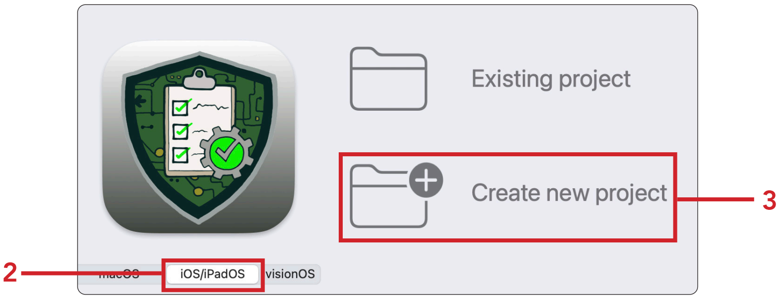
Hardware and Software:
Requirements for following along with this section:

- Jamf Compliance Editor Application
- A Jamf Pro server with administrative privileges

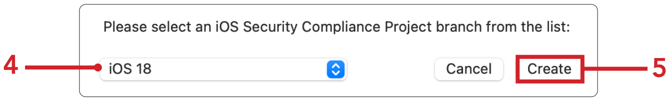
In this section we use the Jamf Compliance Editor application to create a Jamf Compliance Editor using the CIS level 2 benchmark.

1. Open the Jamf Compliance Editor located in the Applications folder.

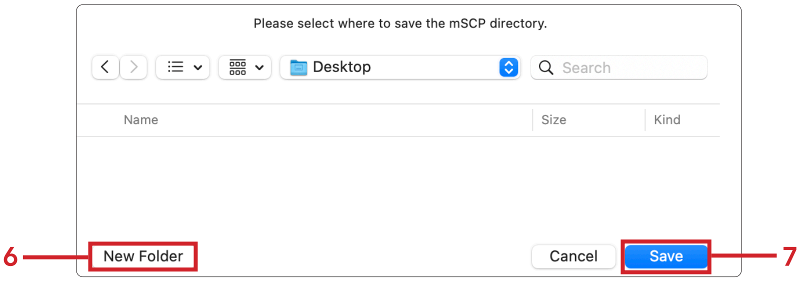
2. Click iOS/iPadOS.
3. Click Create new project



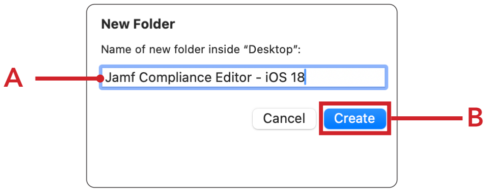
4. Select your iOS version. This guide will use iOS 18.
5. Click Create.


Please select an iOS Security Compliance Project branch from the list:

6. Navigate to the Desktop and click New Folder.
7. Click Save.


Please select where to save the mSCP directory.

8. Configure the following:
    A. Folder name Jamf Compliance Editor - iOS 18 (Change iOS 18 to match whatever version you selected in step 3)
    B. Click Create



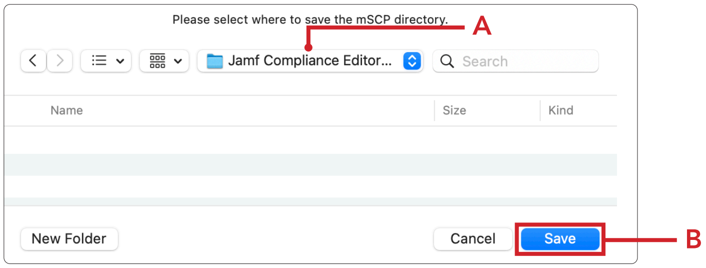
New Folder

Name of new folder inside "Desktop":

Jamf Compliance Editor - iOS 18

9. Confirm the save location matches what you created in the previous step.

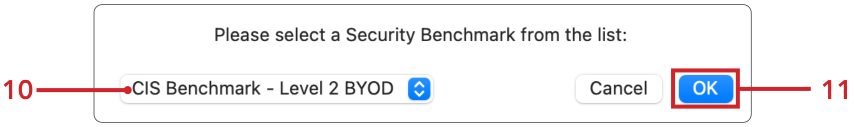
10. Click Save



Please select where to save the mSCP directory.

11. Select a Benchmark. This guide will select CIS Benchmark - Level 2 BYOD.

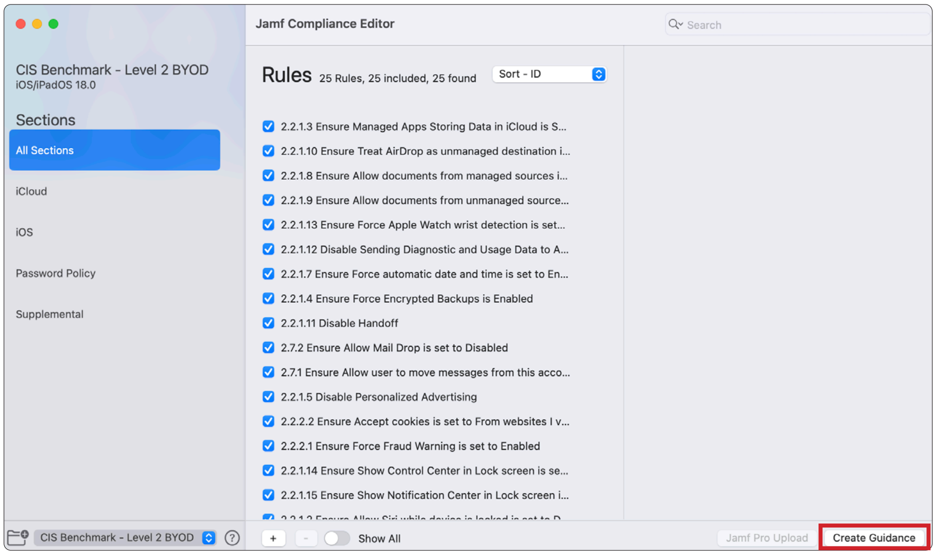
12. Click OK.



Please select a Security Benchmark from the list:

CIS Benchmark - Level 2 BYOD

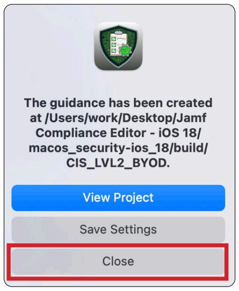
13. Click Create Guidance.



Rules 25 Rules, 25 included, 25 found

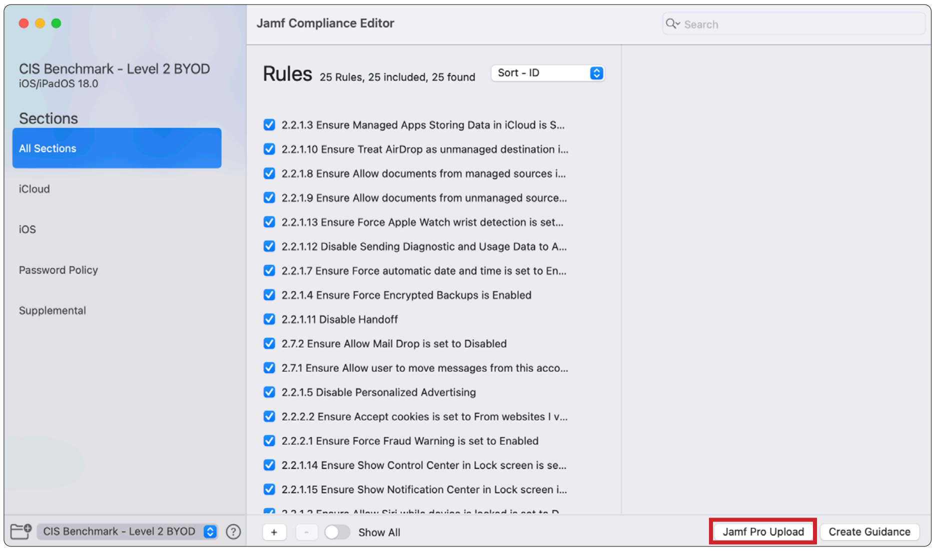
- ☑ 2.2.1.3 Ensure Managed Apps Storing Data in iCloud is S...
- ☑ 2.2.1.10 Ensure Treat AirDrop as unmanaged destination i...
- ☑ 2.2.1.8 Ensure Allow documents from managed sources i...
- ☑ 2.2.1.9 Ensure Allow documents from unmanaged source...
- ☑ 2.2.1.13 Ensure Force Apple Watch wrist detection is set...
- ☑ 2.2.1.12 Disable Sending Diagnostic and Usage Data to A...
- ☑ 2.2.1.7 Ensure Force automatic date and time is set to En...
- ☑ 2.2.1.4 Ensure Force Encrypted Backups is Enabled
- ☑ 2.2.1.11 Disable Handoff
- ☑ 2.7.2 Ensure Allow Mail Drop is set to Disabled
- ☑ 2.7.1 Ensure Allow user to move messages from this acco...
- ☑ 2.2.1.5 Disable Personalized Advertising
- ☑ 2.2.2.2 Ensure Accept cookies is set to From websites I v...
- ☑ 2.2.2.1 Ensure Force Fraud Warning is set to Enabled
- ☑ 2.2.1.14 Ensure Show Control Center in Lock screen is se...
- ☑ 2.2.1.15 Ensure Show Notification Center in Lock screen i...
- ☑ 2.2.1.2 Ensure Allow Siri while device is locked is set to D...

14. At the message below, click Close.



The guidance has been created at /Users/work/Desktop/Jamf Compliance Editor - iOS 18/macos_security-ios_18/build/CIS_LVL2_BYOD.

15. Click Jamf Pro Upload. This will upload all the Rules in the list. If you don't want the full rule set, you can deselect the rules you don't want before uploading to Jamf Pro.



Rules 25 Rules, 25 included, 25 found

☑ 2.2.1.3 Ensure Managed Apps Storing Data in iCloud is S...
☑ 2.2.1.10 Ensure Treat AirDrop as unmanaged destination i...
☑ 2.2.1.8 Ensure Allow documents from managed sources i...
☑ 2.2.1.9 Ensure Allow documents from unmanaged source...
☑ 2.2.1.13 Ensure Force Apple Watch wrist detection is set...
☑ 2.2.1.12 Disable Sending Diagnostic and Usage Data to A...
☑ 2.2.1.7 Ensure Force automatic date and time is set to En...
☑ 2.2.1.4 Ensure Force Encrypted Backups is Enabled
☑ 2.2.1.11 Disable Handoff
☑ 2.7.2 Ensure Allow Mail Drop is set to Disabled
☑ 2.7.1 Ensure Allow user to move messages from this acco...
☑ 2.2.1.5 Disable Personalized Advertising
☑ 2.2.2.2 Ensure Accept cookies is set to From websites I v...
☑ 2.2.2.1 Ensure Force Fraud Warning is set to Enabled
☑ 2.2.1.14 Ensure Show Control Center in Lock screen is se...
☑ 2.2.1.15 Ensure Show Notification Center in Lock screen i...
☑ 2.2.1.2 Ensure Allow Siri while device is locked is set to D...

16. Enter the name of your Jamf Pro server.

17. Enter the URL of your Jamf Pro server.

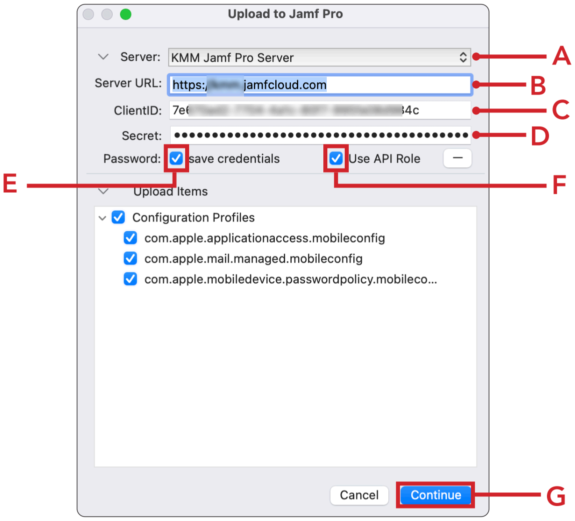
18. Enter the client ID we saved in section one of this guide.

19. Enter the secret we saved in section one of this guide.

20. Enable save credentials.

21. Select the checkbox for Use API Role.

22. Click Continue.



Upload to Jamf Pro

Server: KMM Jamf Pro Server

Server URL: https://[redacted].jamfcloud.com

ClientID: 7e[redacted]4c

Secret: ••

Password: ☑ save credentials ☑ Use API Role

Upload Items

- ☑ Configuration Profiles
  - ☑ com.apple.applicationaccess.mobileconfig
  - ☑ com.apple.mail.managed.mobileconfig
  - ☑ com.apple.mobiledevice.passwordpolicy.mobileco...

23. Quit the Jamf Compliance Editor app.

This completes this section. In the next section, we will create a smart device group for iOS devices using Account Driven Enrollment.

Section 9: Creating a Smart Device Group for iOS Devices using Account Driven Enrollment.

What You'll Need:
Learn what hardware, software, and information you'll need to complete the tutorials in this section.

Hardware and Software:
Requirements for following along with this section:

- A Jamf Pro server with administrative privileges

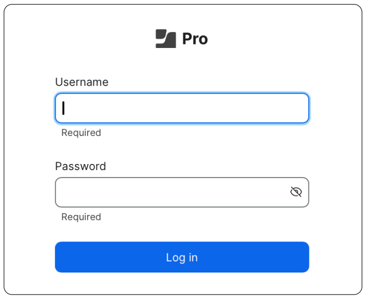
In this section we will create a Smart Device Group for iOS Devices using Account Driven Enrollment. We will use iPadOS 18.3 with CIS Benchmark Level 2 for Account Driven user enrollment as our example for this section. The process is the same for other versions of iOS/ iPadOS/visionOS using different baselines and benchmarks.

Remediation/Scripts for iOS/iPadOS/visionOS:

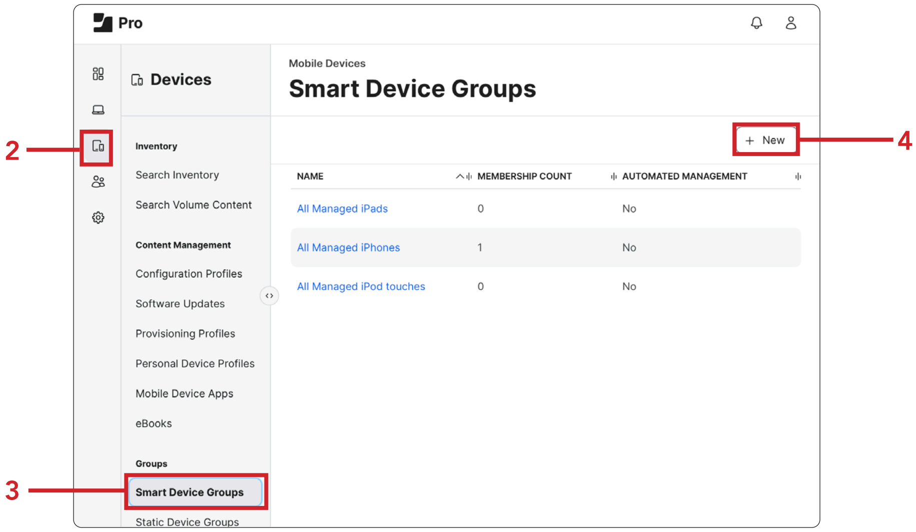
The ability to audit or remediate does not exist for iOS/iPadOS/visionOS. Once the configuration profile has been validated as deployed by the MDM server it is

considered compliant. There are no scripts that can audit or remediate an iOS/iPadOS/ visionOS device, nor are Jamf Pro Extension Attributes available.

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

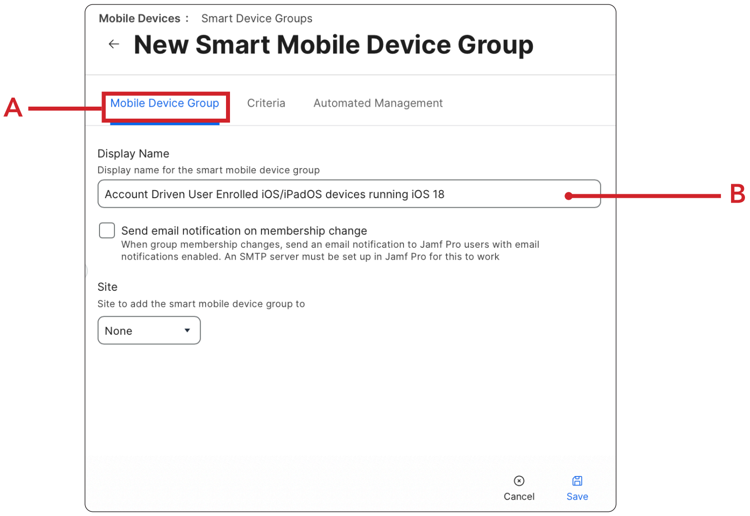


2. Click Devices.
3. Click Smart Device Groups.
4. Click New.



NAME	MEMBERSHIP COUNT	AUTOMATED MANAGEMENT
All Managed iPads	0	No
All Managed iPhones	1	No
All Managed iPod touches	0	No

5. Configure the following:
   A. Click Mobile Device Group.
   B. Enter **Account Driven User Enrolled iOS/iPadOS devices running iOS 18** for the Display Name.



Mobile Devices : Smart Device Groups

New Smart Mobile Device Group

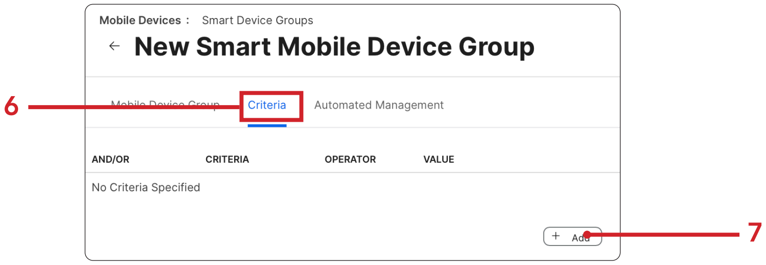
Display Name
Display name for the smart mobile device group
Account Driven User Enrolled iOS/iPadOS devices running iOS 18

□ 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

Site
Site to add the smart mobile device group to
None

6. Click Criteria.

7. Click Add.

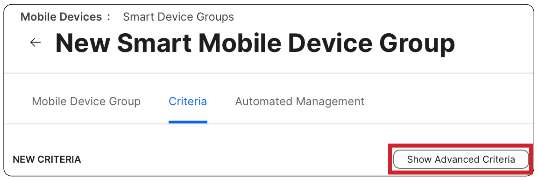


Mobile Devices : Smart Device Groups

New Smart Mobile Device Group

AND/OR	CRITERIA	OPERATOR	VALUE
No Criteria Specified			

8. Click Show Advanced Criteria.

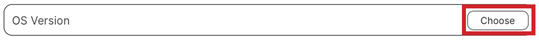


Mobile Devices : Smart Device Groups

New Smart Mobile Device Group

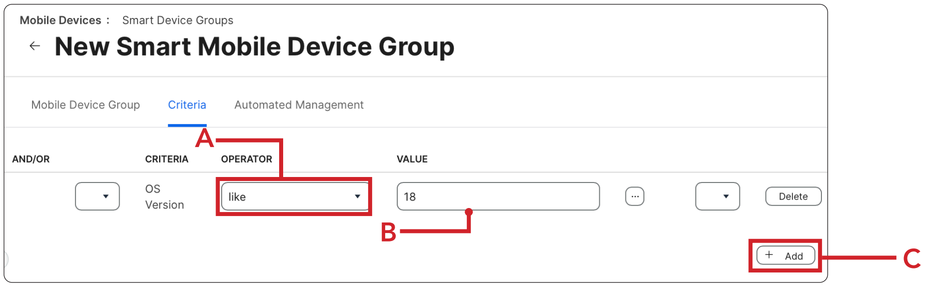
NEW CRITERIA

9. Scroll down to OS Version and click Choose.

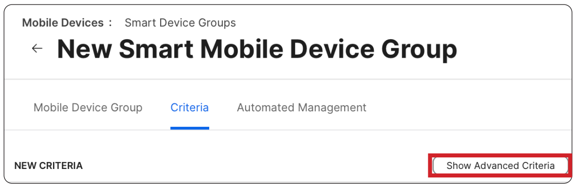


OS Version

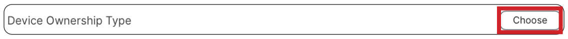
10. Configure the following:
    A. Select **like** for the Operator.
    B. Enter **18** for the Value
    C. Click Add



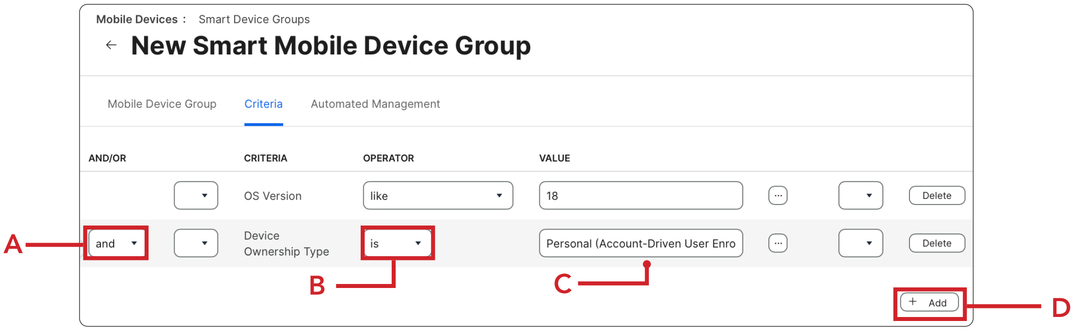
11. Click Show Advanced Criteria.



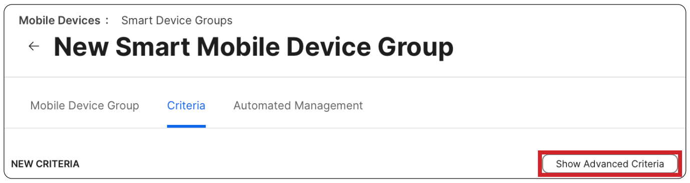
12. Select Device Ownership Type and click Choose.



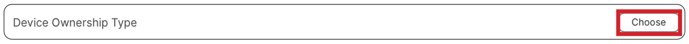
13. Configure the following:
    A. From the menu select **and**
    B. Select **is** for the Operator.
    C. Enter **Personal (Account-Driven User Enrollment)** for the Value.
    D. Click Add



14. Click Show Advanced Criteria.

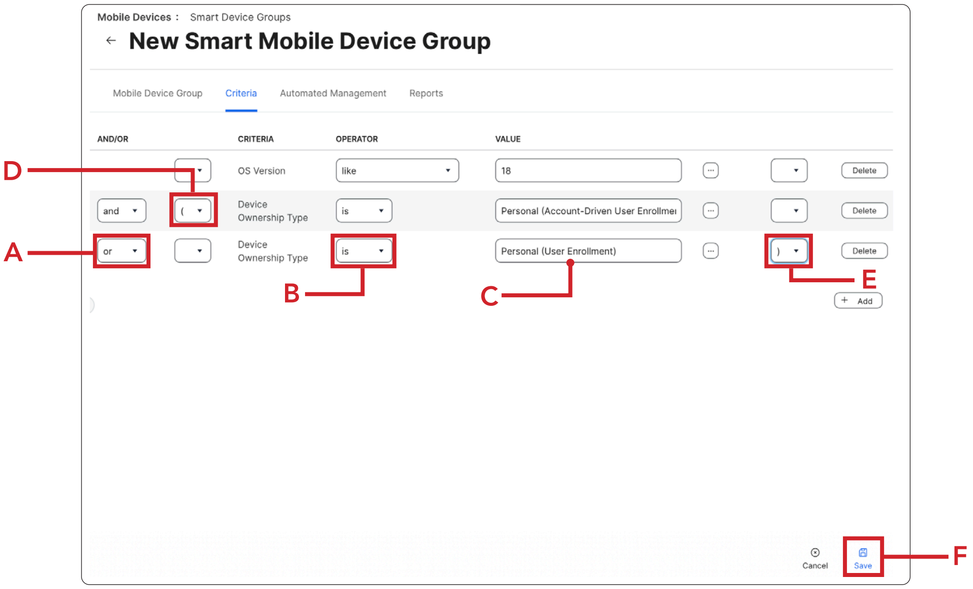


15. Select Device Ownership Type and click Choose.



Device Ownership Type

16. Configure the following:
    A. From the menu select **or**
    B. Select **is** for the Operator.
    C. Enter **Personal (User Enrollment)** for the Value.
    D. From the menu to the right of and, Select an open parentheses { **(** }.
    E. From the menu to the left Delete, select a closed parentheses { **)** }.
    F. Click Save

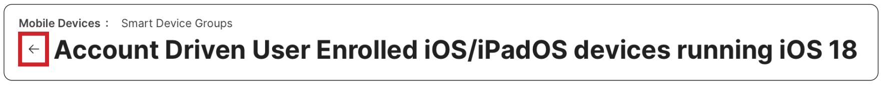


Mobile Devices : Smart Device Groups

New Smart Mobile Device Group

AND/OR		CRITERIA	OPERATOR	VALUE			
		OS Version	like	18	···		Delete
and	(	Device Ownership Type	is	Personal (Account-Driven User Enrollmer	···		Delete
or		Device Ownership Type	is	Personal (User Enrollment)	···	)	Delete

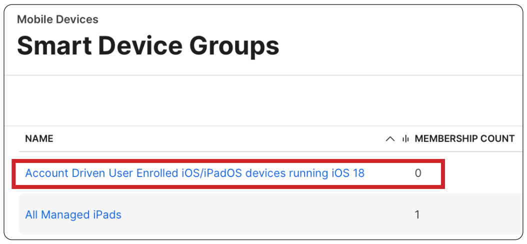
17.Click Previous (←).



Mobile Devices : Smart Device Groups

Account Driven User Enrolled iOS/iPadOS devices running iOS 18

18.Confirm Account Driven User Enrolled iOS/iPadOS devices running iOS 18 is shown in the list.



Mobile Devices

Smart Device Groups

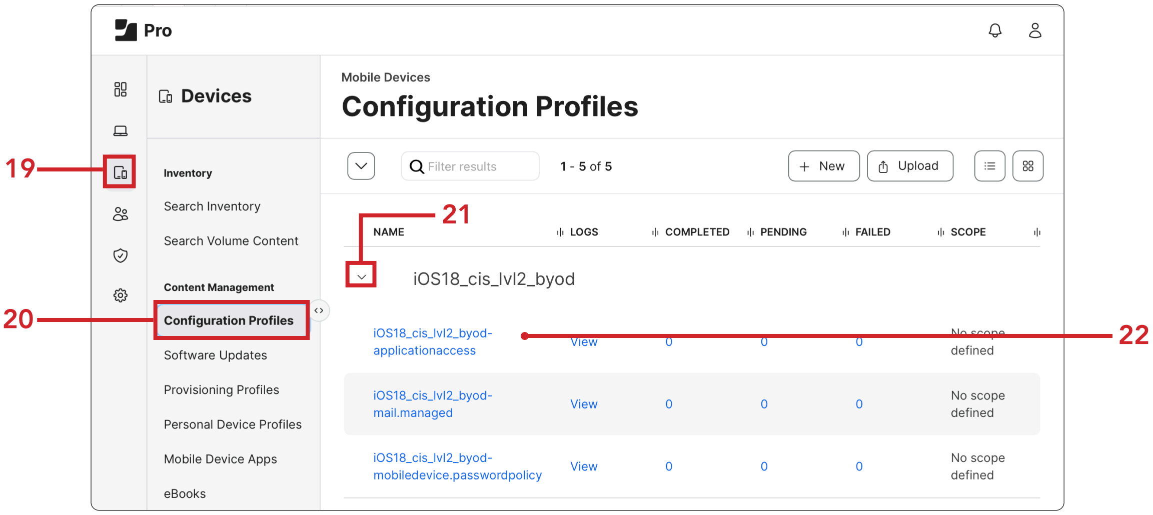
NAME	MEMBERSHIP COUNT
Account Driven User Enrolled iOS/iPadOS devices running iOS 18	0
All Managed iPads	1

19. Click Devices.

20. Click Configuration Profiles.

21. Go to **iOS18_cis_lvl2_byod** category and expand the category to see all the computer configuration profiles that were created by the Jamf Compliance Editor app.

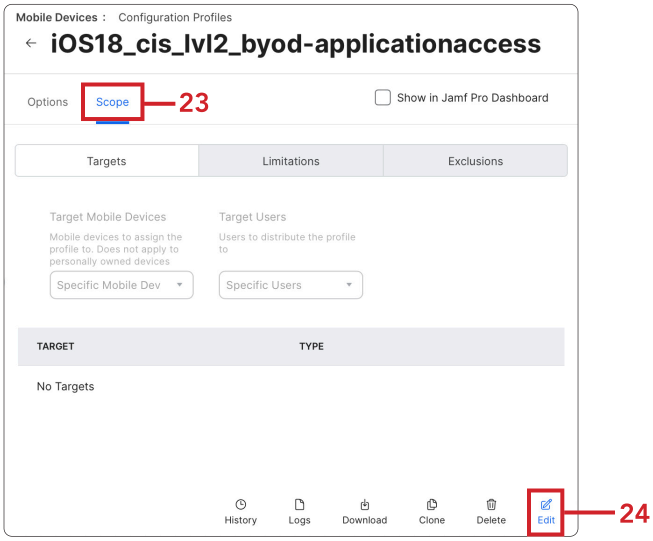
22. Select the first configuration profile in the list.



NAME	LOGS	COMPLETED	PENDING	FAILED	SCOPE
iOS18_cis_lvl2_byod					
iOS18_cis_lvl2_byod-applicationaccess	View	0	0	0	No scope defined
iOS18_cis_lvl2_byod-mail.managed	View	0	0	0	No scope defined
iOS18_cis_lvl2_byod-mobiledevice.passwordpolicy	View	0	0	0	No scope defined

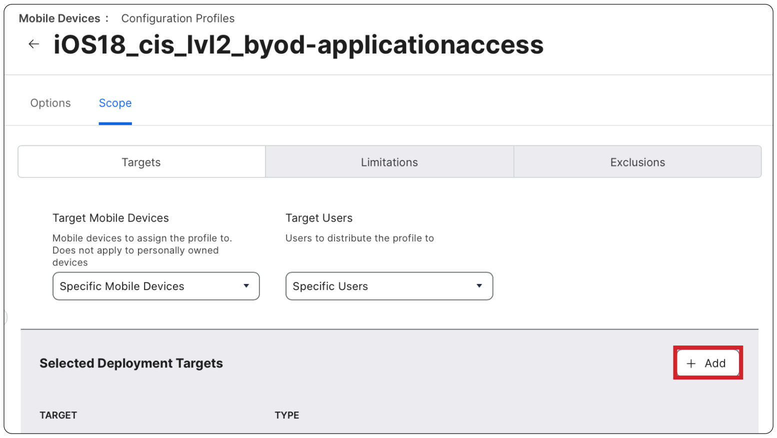
23. Select Scope.

24. Click Edit.


Mobile Devices : Configuration Profiles
iOS18_cis_lvl2_byod-applicationaccess
Options
Scope
23
Show in Jamf Pro Dashboard
Targets
Limitations
Exclusions
Target Mobile Devices
Mobile devices to assign the profile to. Does not apply to personally owned devices
Specific Mobile Dev
Target Users
Users to distribute the profile to
Specific Users
History
Logs
Download
Clone
Delete
Edit
24

TARGET	TYPE
No Targets	

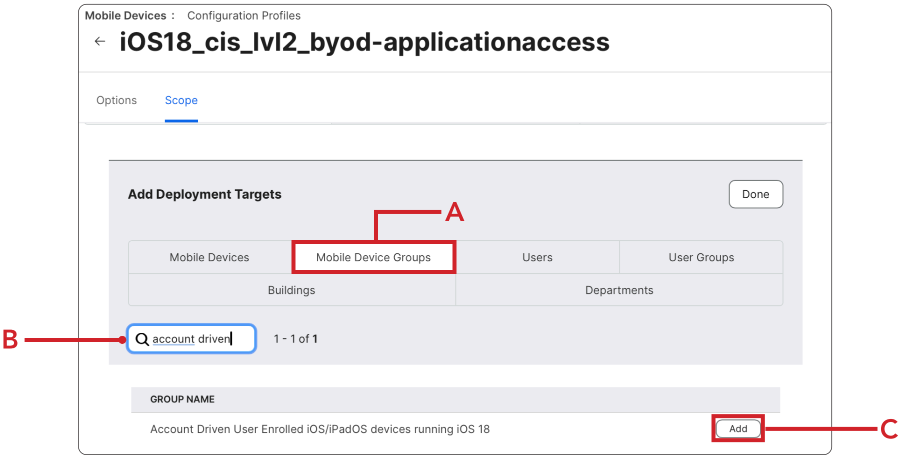
25. Click Add.


Mobile Devices : Configuration Profiles
iOS18_cis_lvl2_byod-applicationaccess
Options
Scope
Targets
Limitations
Exclusions
Selected Deployment Targets
+ Add
TARGET
TYPE

Target Mobile Devices
Mobile devices to assign the profile to. Does not apply to personally owned devices
Specific Mobile Devices

Target Users
Users to distribute the profile to
Specific Users

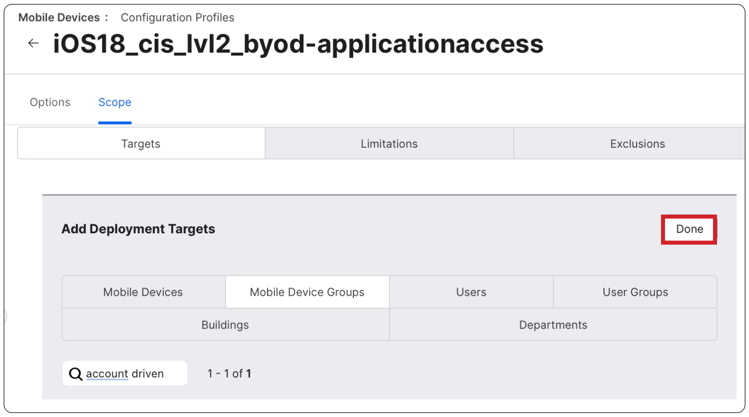
26. Perform the following:
    A. Select Mobile Device Groups
    B. In the search field enter: account driven
    C. Click add next to Account Driven User Enrolled iOS/iPadOS devices running iOS 18



account driven
1 - 1 of 1

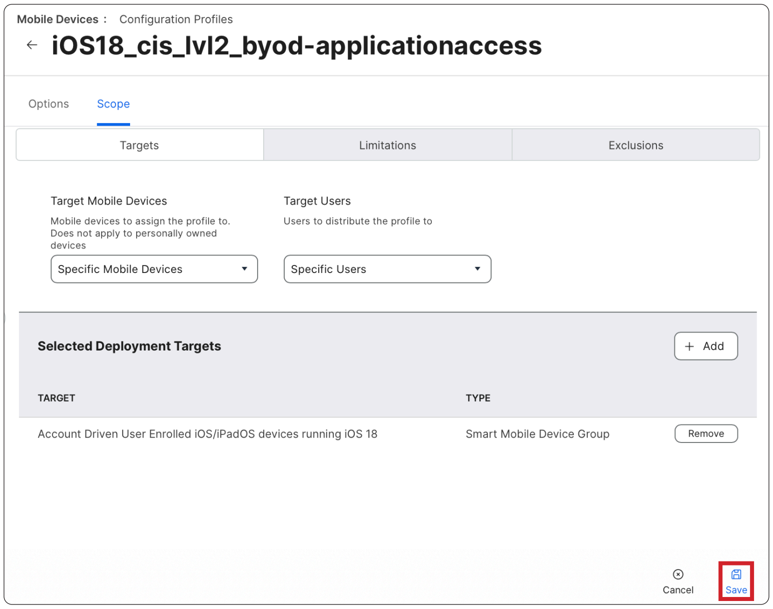
GROUP NAME	
Account Driven User Enrolled iOS/iPadOS devices running iOS 18	Add

27. Click Done.



account driven
1 - 1 of 1

28. Click Save.



Mobile Devices : Configuration Profiles

← iOS18_cis_lvl2_byod-applicationaccess

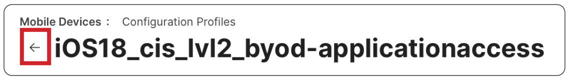
Target Mobile Devices
Mobile devices to assign the profile to. Does not apply to personally owned devices
Specific Mobile Devices

Target Users
Users to distribute the profile to
Specific Users

Selected Deployment Targets

TARGET	TYPE	
Account Driven User Enrolled iOS/iPadOS devices running iOS 18	Smart Mobile Device Group	Remove

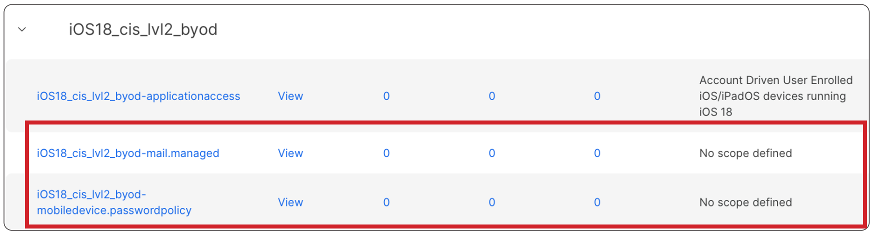
29. Click Previous (←).



Mobile Devices : Configuration Profiles

← iOS18_cis_lvl2_byod-applicationaccess

30. Scope the remaining two configuration profiles to the mobile device group named Account Driven User Enrolled iOS/iPadOS devices running iOS 18.



iOS18_cis_lvl2_byod

iOS18_cis_lvl2_byod-applicationaccess	View	0	0	0	Account Driven User Enrolled iOS/iPadOS devices running iOS 18
iOS18_cis_lvl2_byod-mail.managed	View	0	0	0	No scope defined
iOS18_cis_lvl2_byod-mobiledevice.passwordpolicy	View	0	0	0	No scope defined

This completes this section. In the next section, we use the Jamf Compliance Editor - macOS Sequoia project we created in section two of this guide using the CIS Benchmark - Level 2 to audit a local Mac computer..

Section 10: Run a local Mac Computer Audit

What You'll Need

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

Hardware and Software

Requirements for following along with this section:

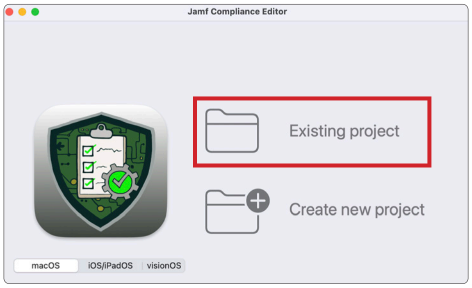
- A Mac computer with administrative privileges
- Jamf Compliance Editor Application
- The Jamf Compliance Editor - macOS Sequoia project we created in section two of this guide.

In this section, we use the Jamf Compliance Editor - macOS Sequoia project we created in section two of this guide using the CIS Benchmark - Level 2 to audit a local Mac computer.

1. If necessary, Open Jamf Compliance Editor.

Jamf Compliance Editor

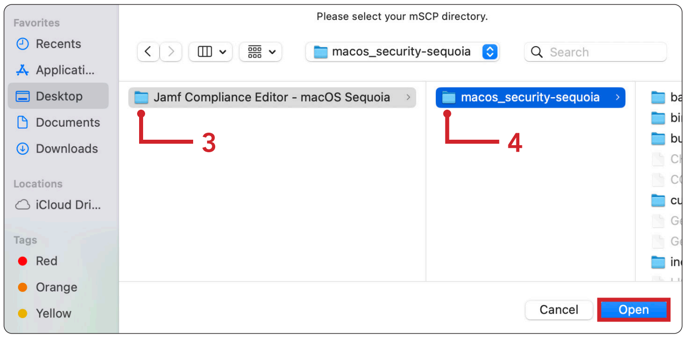
2. Click Existing project.



3. Select the Jamf Compliance Editor - macOS Sequoia folder located on your Desktop.

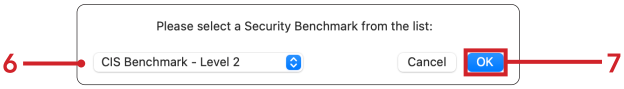
4. Select the macos_security-sequoia folder.

5. Click Open.


Please select your mSCP directory.

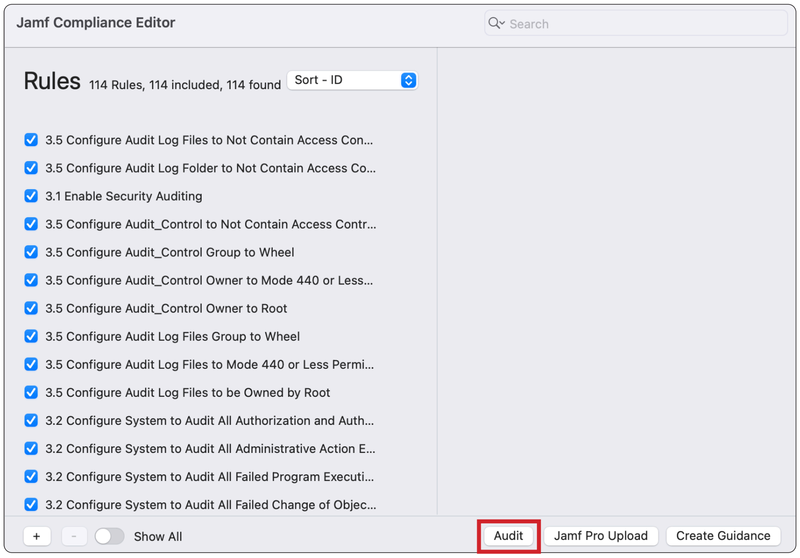
6. Select CIS Benchmark - Level 2.

7. Click OK.


Please select a Security Benchmark from the list:

CIS Benchmark - Level 2

8. Click the Audit button.



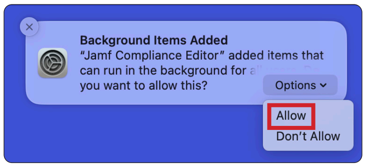
Jamf Compliance Editor

Search

Rules 114 Rules, 114 included, 114 found Sort - ID

- ☑ 3.5 Configure Audit Log Files to Not Contain Access Con...
- ☑ 3.5 Configure Audit Log Folder to Not Contain Access Co...
- ☑ 3.1 Enable Security Auditing
- ☑ 3.5 Configure Audit_Control to Not Contain Access Contr...
- ☑ 3.5 Configure Audit_Control Group to Wheel
- ☑ 3.5 Configure Audit_Control Owner to Mode 440 or Less...
- ☑ 3.5 Configure Audit_Control Owner to Root
- ☑ 3.5 Configure Audit Log Files Group to Wheel
- ☑ 3.5 Configure Audit Log Files to Mode 440 or Less Permi...
- ☑ 3.5 Configure Audit Log Files to be Owned by Root
- ☑ 3.2 Configure System to Audit All Authorization and Auth...
- ☑ 3.2 Configure System to Audit All Administrative Action E...
- ☑ 3.2 Configure System to Audit All Failed Program Executi...
- ☑ 3.2 Configure System to Audit All Failed Change of Objec...

9. If prompted with the message below, select Allow.
NOTE if you did not see notification, you can enable the background item for Jamf Compliance Editor here: System Settings > General > Login Items & Extensions > Allow in Background.

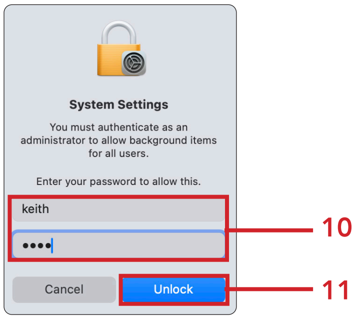


Background Items Added

"Jamf Compliance Editor" added items that can run in the background for a... you want to allow this?

10. Enter your administrator credentials.

11. Click Unlock.



System Settings

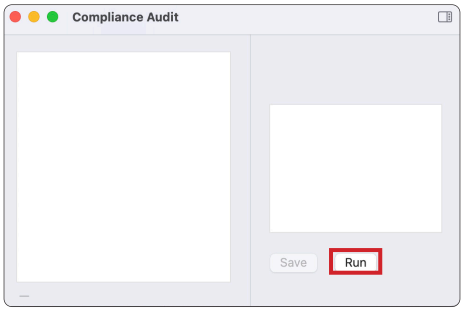
You must authenticate as an administrator to allow background items for all users.

Enter your password to allow this.

keith

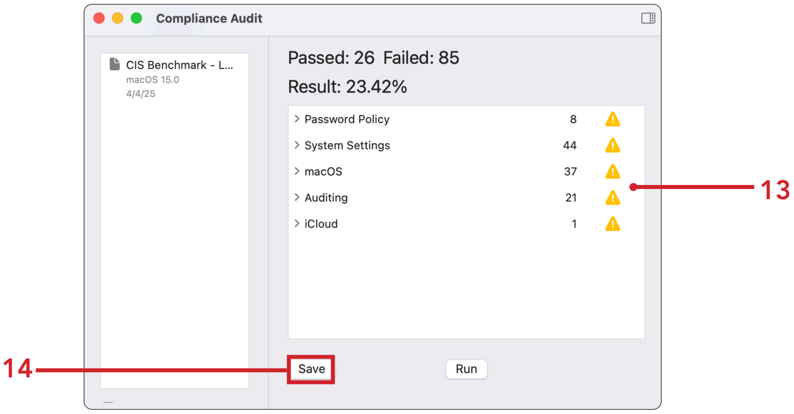
••••

12. Click Run.



13. Confirm the output of the CIS Benchmark - Level 2 local audit is shown below.

14. Click Save.
    NOTE: The results show in the image below were run on a NON compliant Mac computer to demonstrate what you would see if issue were found.



Compliance Audit

CIS Benchmark - L...
macOS 15.0
4/4/25

Passed: 26 Failed: 85

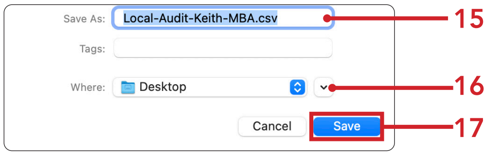
Result: 23.42%

› Password Policy	8	⚠
› System Settings	44	⚠
› macOS	37	⚠
› Auditing	21	⚠
› iCloud	1	⚠

15. Enter **Local-Audit-Keith-MBA.csv** (replace Keith with your name.)

16. Select Desktop as the destination.

17. Click Save



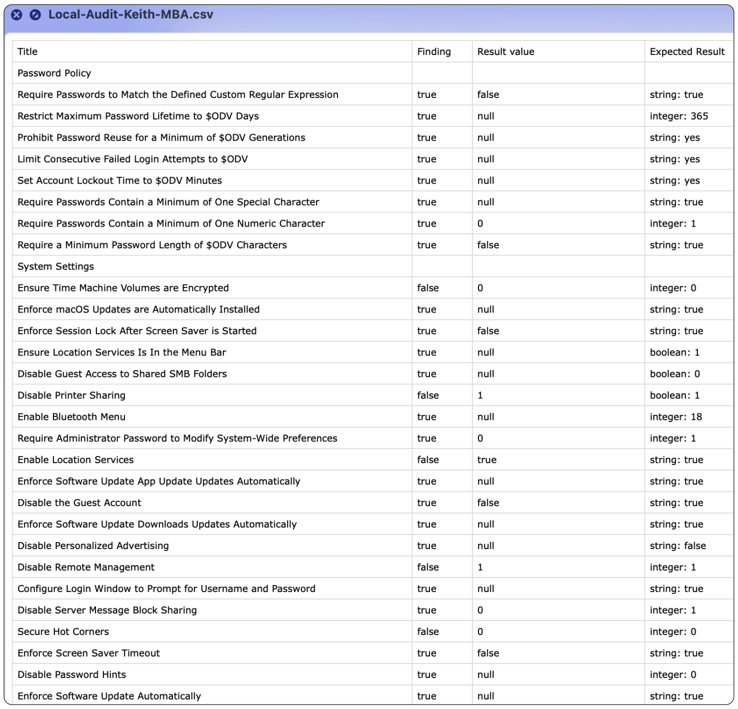
Save As: Local-Audit-Keith-MBA.csv

Tags:

Where: Desktop

18. Open the csv file that was saved to your desktop.

19. The file contains a full report of all the items that passed and failed the local audit using the CIS Benchmark - Level 2.



Local-Audit-Keith-MBA.csv

Title	Finding	Result value	Expected Result
Password Policy			
Require Passwords to Match the Defined Custom Regular Expression	true	false	string: true
Restrict Maximum Password Lifetime to $ODV Days	true	null	integer: 365
Prohibit Password Reuse for a Minimum of $ODV Generations	true	null	string: yes
Limit Consecutive Failed Login Attempts to $ODV	true	null	string: yes
Set Account Lockout Time to $ODV Minutes	true	null	string: yes
Require Passwords Contain a Minimum of One Special Character	true	null	string: true
Require Passwords Contain a Minimum of One Numeric Character	true	0	integer: 1
Require a Minimum Password Length of $ODV Characters	true	false	string: true
System Settings			
Ensure Time Machine Volumes are Encrypted	false	0	integer: 0
Enforce macOS Updates are Automatically Installed	true	null	string: true
Enforce Session Lock After Screen Saver is Started	true	false	string: true
Ensure Location Services Is In the Menu Bar	true	null	boolean: 1
Disable Guest Access to Shared SMB Folders	true	null	boolean: 0
Disable Printer Sharing	false	1	boolean: 1
Enable Bluetooth Menu	true	null	integer: 18
Require Administrator Password to Modify System-Wide Preferences	true	0	integer: 1
Enable Location Services	false	true	string: true
Enforce Software Update App Update Updates Automatically	true	null	string: true
Disable the Guest Account	true	false	string: true
Enforce Software Update Downloads Updates Automatically	true	null	string: true
Disable Personalized Advertising	true	null	string: false
Disable Remote Management	false	1	integer: 1
Configure Login Window to Prompt for Username and Password	true	null	string: true
Disable Server Message Block Sharing	true	0	integer: 1
Secure Hot Corners	false	0	integer: 0
Enforce Screen Saver Timeout	true	false	string: true
Disable Password Hints	true	null	integer: 0
Enforce Software Update Automatically	true	null	string: true

This completes this section. In the next section, we will modify the CIS Benchmark - Level 2 to create a risk based benchmark and report with custom author names.

Section 11: Risk based benchmarks and reports

What You'll Need

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

Hardware and Software

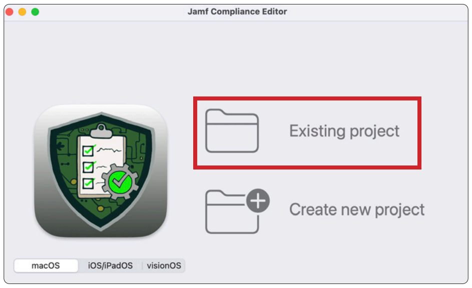
Requirements for following along with this section:

- A Mac computer with administrative privileges
- Jamf Compliance Editor Application
- The Jamf Compliance Editor - macOS Sequoia project we created in section two of this guide.

In this section we modify the Jamf Compliance Editor - macOS Sequoia project we created in section two of this guide using the CIS Benchmark - Level 2 to create a risk based benchmark. Modifying CIS benchmarks becomes risk-based when changes are informed by specific risk evaluations, ensuring that controls are tailored to mitigate key threats effectively while maintaining operational balance.

1. If necessary, Open Jamf Compliance Editor.

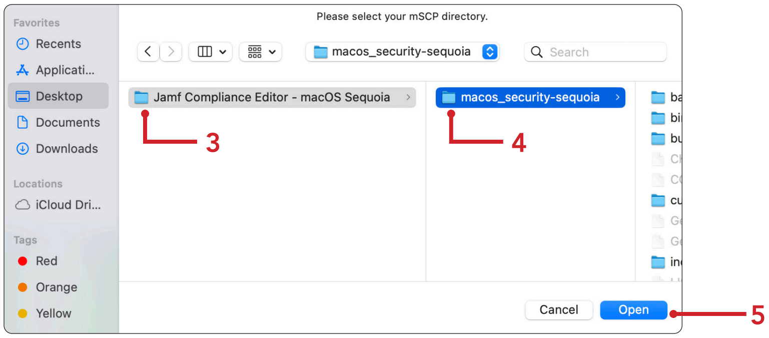
2. Select Existing project.



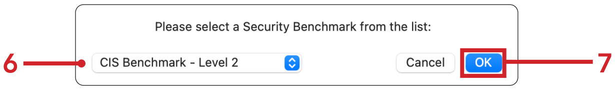
3. Select the Jamf Compliance Editor - macOS Sequoia folder located on your Desktop

4. Select the macos_security-sequoia folder

5. Click Open


Please select your mSCP directory.

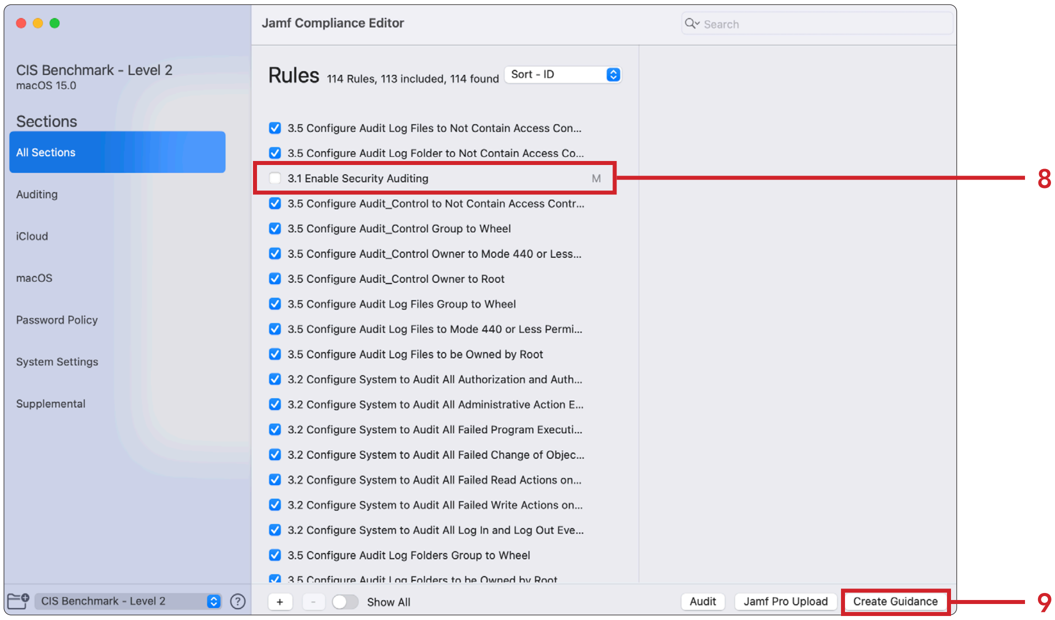
6. Select CIS Benchmark - Level 2.
7. Click OK.



Please select a Security Benchmark from the list:

CIS Benchmark - Level 2

8. Deselect the checkbox for 3.1 Enable Security Auditing. Confirm an "M" to the right of 3.1 Enable Security Auditing. This means the baseline was modified
9. Click Create Guidance



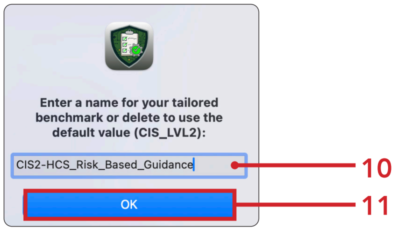
CIS Benchmark - Level 2
macOS 15.0

Rules 114 Rules, 113 included, 114 found

Sort - ID

☑ 3.5 Configure Audit Log Files to Not Contain Access Con...
☑ 3.5 Configure Audit Log Folder to Not Contain Access Co...
☐ 3.1 Enable Security Auditing M
☑ 3.5 Configure Audit_Control to Not Contain Access Contr...
☑ 3.5 Configure Audit_Control Group to Wheel
☑ 3.5 Configure Audit_Control Owner to Mode 440 or Less...
☑ 3.5 Configure Audit_Control Owner to Root
☑ 3.5 Configure Audit Log Files Group to Wheel
☑ 3.5 Configure Audit Log Files to Mode 440 or Less Permi...
☑ 3.5 Configure Audit Log Files to be Owned by Root
☑ 3.2 Configure System to Audit All Authorization and Auth...
☑ 3.2 Configure System to Audit All Administrative Action E...
☑ 3.2 Configure System to Audit All Failed Program Executi...
☑ 3.2 Configure System to Audit All Failed Change of Objec...
☑ 3.2 Configure System to Audit All Failed Read Actions on...
☑ 3.2 Configure System to Audit All Failed Write Actions on...
☑ 3.2 Configure System to Audit All Log In and Log Out Eve...
☑ 3.5 Configure Audit Log Folders Group to Wheel
☑ 3.5 Configure Audit Log Folders to be Owned by Root

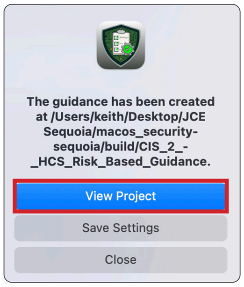
10. Enter a name for the benchmark. This guide will use **CIS2-HCS_Risk_Based_Guidance**. NOTE: If you use spaces, JCE will rename it with underscores and dashes.
11. Click OK.



Enter a name for your tailored benchmark or delete to use the default value (CIS_LVL2):

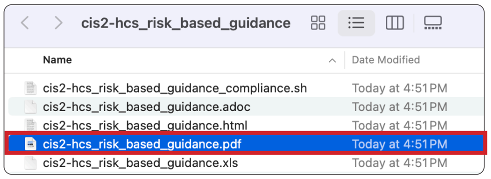
CIS2-HCS_Risk_Based_Guidance

12. Click View Project.



The guidance has been created at /Users/keith/Desktop/JCE Sequoia/macos_security-sequoia/build/CIS_2_-_HCS_Risk_Based_Guidance.

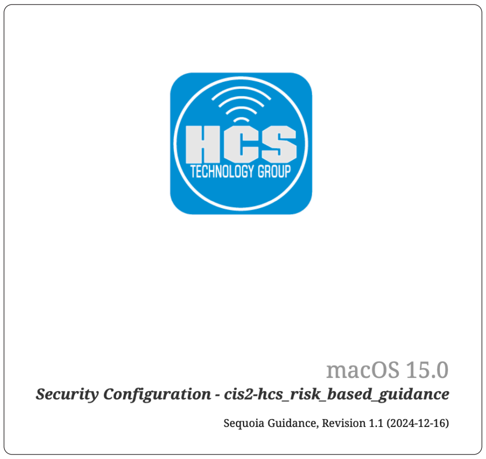
13. Open the file named cis2-hcs_risk_based_guidance.pdf. NOTE: You filename will be different.



cis2-hcs_risk_based_guidance

Name	Date Modified
cis2-hcs_risk_based_guidance_compliance.sh	Today at 4:51 PM
cis2-hcs_risk_based_guidance.adoc	Today at 4:51 PM
cis2-hcs_risk_based_guidance.html	Today at 4:51 PM
cis2-hcs_risk_based_guidance.pdf	Today at 4:51 PM
cis2-hcs_risk_based_guidance.xls	Today at 4:51 PM

14. The report will have your organizations logo on the cover page.

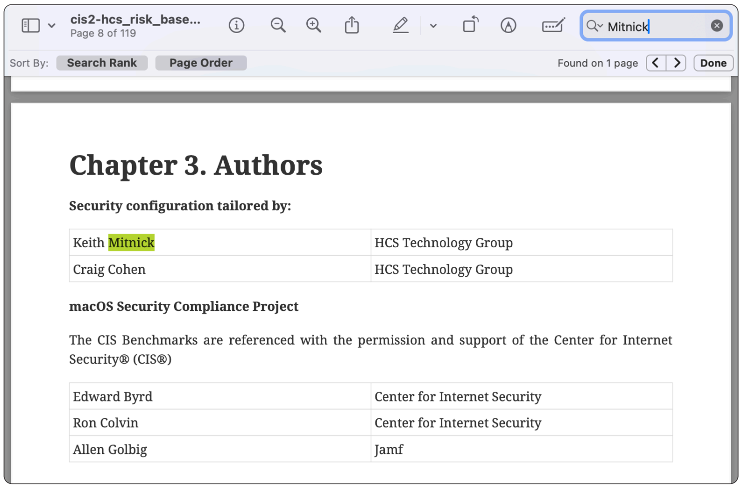


macOS 15.0

Security Configuration - cis2-hcs_risk_based_guidance

Sequoia Guidance, Revision 1.1 (2024-12-16)

15. Chapter three of the pdf document will show the authors that were set in the Jamf Compliance Editor app preferences in section two of this guide. The author information will only show up in a report if a baseline is manually altered to remove items from the baseline.



Chapter 3. Authors

Security configuration tailored by:

Keith Mitnick	HCS Technology Group
Craig Cohen	HCS Technology Group

macOS Security Compliance Project

The CIS Benchmarks are referenced with the permission and support of the Center for Internet Security® (CIS®)

Edward Byrd	Center for Internet Security
Ron Colvin	Center for Internet Security
Allen Golbig	Jamf

This completes this section. In the next section, we will create Auditor Reports with Organization Defined Values.

Section 12: Auditor Reports with Organization Defined Values

What You'll Need:
Learn what hardware, software, and information you'll need to complete the tutorials in this section.

Hardware and Software:
Requirements for following along with this section:

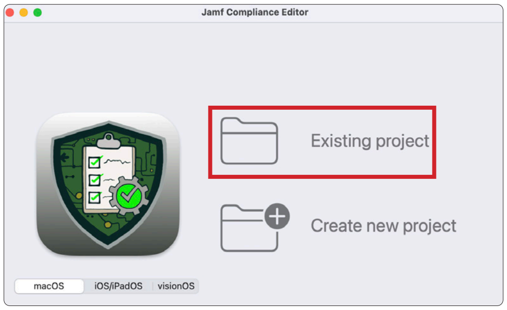
- A Mac computer with administrative privileges
- Jamf Compliance Editor Application
- The Jamf Compliance Editor - macOS Sequoia project we created in section two of this guide.

In this section, we will modify the Jamf Compliance Editor macOS Sequoia project created in section two, using the CIS Benchmark Level 2. We'll update an Organizational Defined Value (ODV) and generate a report to provide to an auditor, documenting the changes made.

An Organizational Defined Value (ODV) in Jamf Compliance Editor is a customizable setting within a compliance baseline. Instead of using a fixed benchmark value, ODVs (typically shown as $ODV) allow organizations to define values that align with their internal security policies or operational needs.

1. If necessary, Open Jamf Compliance Editor.

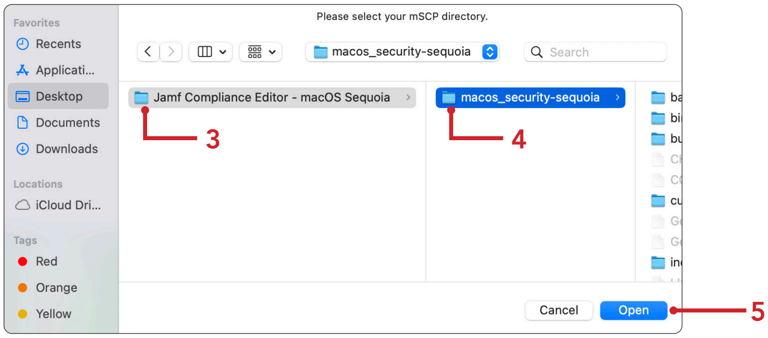
2. Click Existing project.



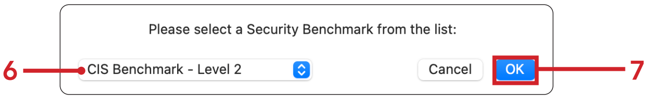
3. Select the Jamf Compliance Editor - macOS Sequoia folder located on your Desktop

4. Select the macos_security-sequoia folder

5. Click Open


Please select your mSCP directory.

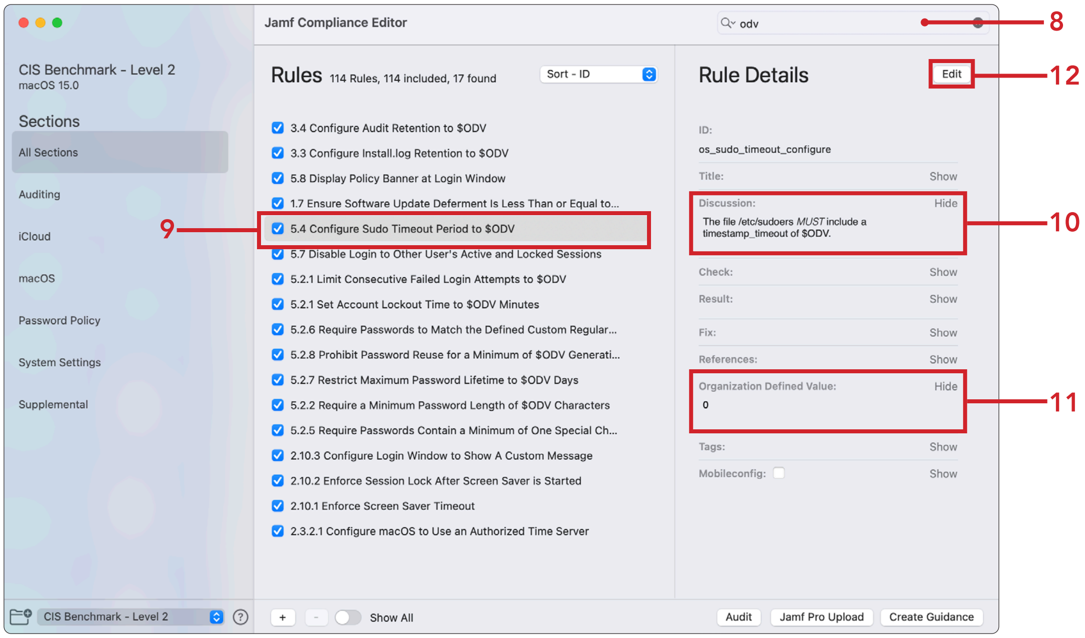
6. Select CIS Benchmark - Level 2.
7. Click OK.



Please select a Security Benchmark from the list:

CIS Benchmark - Level 2

8. Enter **odv** in the search field
9. Select: 5.4 Configure Sudo Timeout Period to $ODV
10. In the Rule Details section, Click Show next to Discussion
11. In the Rule Details section, Click Show next to Organization Defined Value
12. In the Rule Details section, Click Edit



odv

CIS Benchmark - Level 2
macOS 15.0

Rules 114 Rules, 114 included, 17 found

- ☑ 3.4 Configure Audit Retention to $ODV
- ☑ 3.3 Configure Install.log Retention to $ODV
- ☑ 5.8 Display Policy Banner at Login Window
- ☑ 1.7 Ensure Software Update Deferment Is Less Than or Equal to...
- ☑ 5.4 Configure Sudo Timeout Period to $ODV
- ☑ 5.7 Disable Login to Other User's Active and Locked Sessions
- ☑ 5.2.1 Limit Consecutive Failed Login Attempts to $ODV
- ☑ 5.2.1 Set Account Lockout Time to $ODV Minutes
- ☑ 5.2.6 Require Passwords to Match the Defined Custom Regular...
- ☑ 5.2.8 Prohibit Password Reuse for a Minimum of $ODV Generati...
- ☑ 5.2.7 Restrict Maximum Password Lifetime to $ODV Days
- ☑ 5.2.2 Require a Minimum Password Length of $ODV Characters
- ☑ 5.2.5 Require Passwords Contain a Minimum of One Special Ch...
- ☑ 2.10.3 Configure Login Window to Show A Custom Message
- ☑ 2.10.2 Enforce Session Lock After Screen Saver is Started
- ☑ 2.10.1 Enforce Screen Saver Timeout
- ☑ 2.3.2.1 Configure macOS to Use an Authorized Time Server

Rule Details

ID:
os_sudo_timeout_configure

Title: Show

Discussion: Hide
The file /etc/sudoers *MUST* include a timestamp_timeout of $ODV.

Check: Show

Result: Show

Fix: Show

References: Show

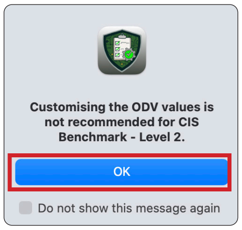
Organization Defined Value: Hide
0

Tags: Show

Mobileconfig: □ Show

CIS Benchmark - Level 2

13. In the Rule Details section, change Organization Defined Value from 0 to 5.
14. Click OK.



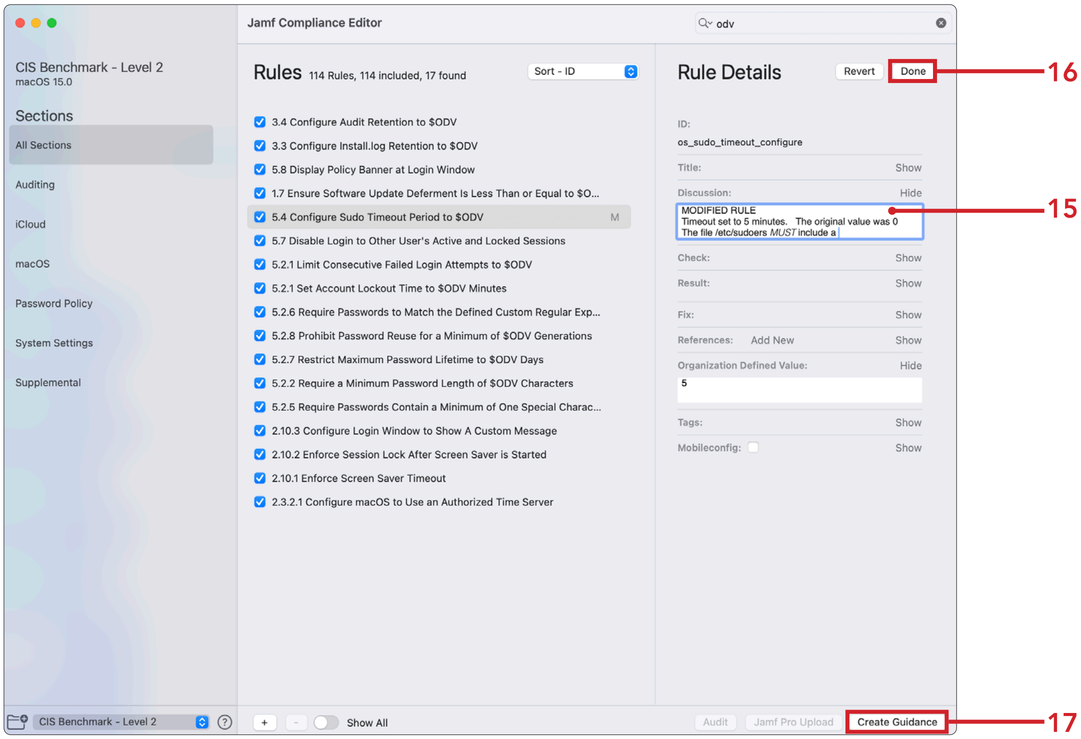
Customising the ODV values is not recommended for CIS Benchmark - Level 2.

□ Do not show this message again

15. In the Rule Details section, Add the following to the top of the Discussion:
    MODIFIED RULE
    Timeout set to 5 minutes. The original value was 0

16. Click Done

17. Click Create Guidance



CIS Benchmark - Level 2
macOS 15.0

Rules 114 Rules, 114 included, 17 found

☑ 3.4 Configure Audit Retention to $ODV
☑ 3.3 Configure Install.log Retention to $ODV
☑ 5.8 Display Policy Banner at Login Window
☑ 1.7 Ensure Software Update Deferment Is Less Than or Equal to $O...
☑ 5.4 Configure Sudo Timeout Period to $ODV
☑ 5.7 Disable Login to Other User's Active and Locked Sessions
☑ 5.2.1 Limit Consecutive Failed Login Attempts to $ODV
☑ 5.2.1 Set Account Lockout Time to $ODV Minutes
☑ 5.2.6 Require Passwords to Match the Defined Custom Regular Exp...
☑ 5.2.8 Prohibit Password Reuse for a Minimum of $ODV Generations
☑ 5.2.7 Restrict Maximum Password Lifetime to $ODV Days
☑ 5.2.2 Require a Minimum Password Length of $ODV Characters
☑ 5.2.5 Require Passwords Contain a Minimum of One Special Charac...
☑ 2.10.3 Configure Login Window to Show A Custom Message
☑ 2.10.2 Enforce Session Lock After Screen Saver is Started
☑ 2.10.1 Enforce Screen Saver Timeout
☑ 2.3.2.1 Configure macOS to Use an Authorized Time Server

Rule Details

ID:
os_sudo_timeout_configure

Title:

Discussion:
MODIFIED RULE
Timeout set to 5 minutes.   The original value was 0
The file /etc/sudoers *MUST* include a

Check:

Result:

Fix:

References:

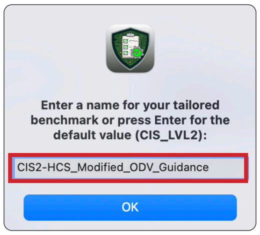
Organization Defined Value:
5

Tags:

Mobileconfig: □

CIS Benchmark - Level 2

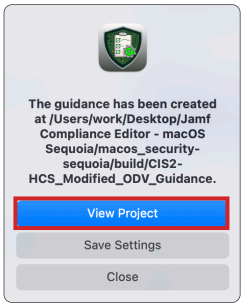
18. Enter a name for the benchmark. This guide will name it: CIS2-HCS_Modified_ODV_Guidance. If you use spaces, JCE will rename it with underscores and dashes.



Enter a name for your tailored benchmark or press Enter for the default value (CIS_LVL2):

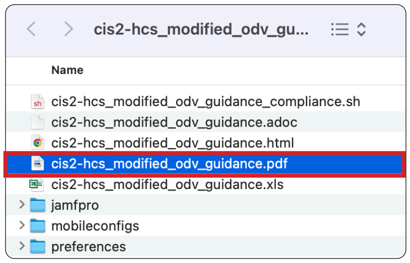
CIS2-HCS_Modified_ODV_Guidance

19. Click View Project.



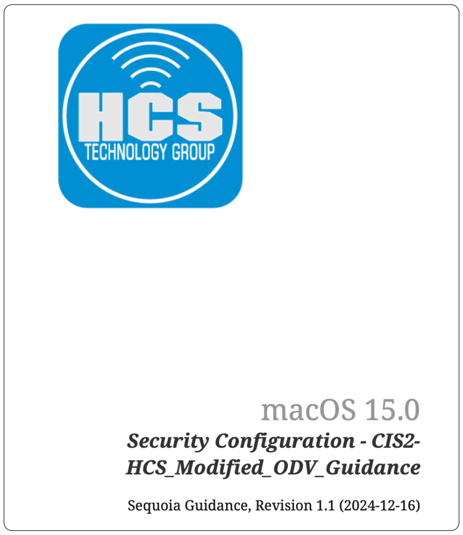
The guidance has been created at /Users/work/Desktop/Jamf Compliance Editor - macOS Sequoia/macos_security-sequoia/build/CIS2-HCS_Modified_ODV_Guidance.

20. Open the file named cis2-hcs_modified_odv_guidance.pdf.
NOTE: Your filename will be different.



- cis2-hcs_modified_odv_guidance_compliance.sh
- cis2-hcs_modified_odv_guidance.adoc
- cis2-hcs_modified_odv_guidance.html
- cis2-hcs_modified_odv_guidance.pdf
- cis2-hcs_modified_odv_guidance.xls
- jamfpro
- mobileconfigs
- preferences

21. The report will have your organizations logo on the cover page.



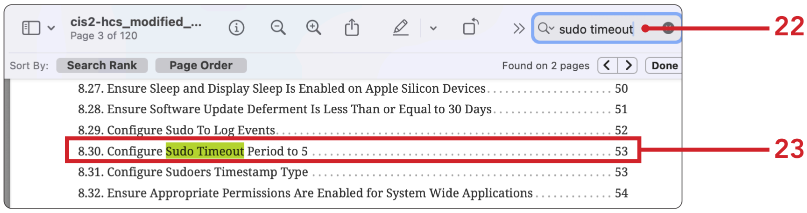
macOS 15.0

Security Configuration - CIS2-HCS_Modified_ODV_Guidance

Sequoia Guidance, Revision 1.1 (2024-12-16)

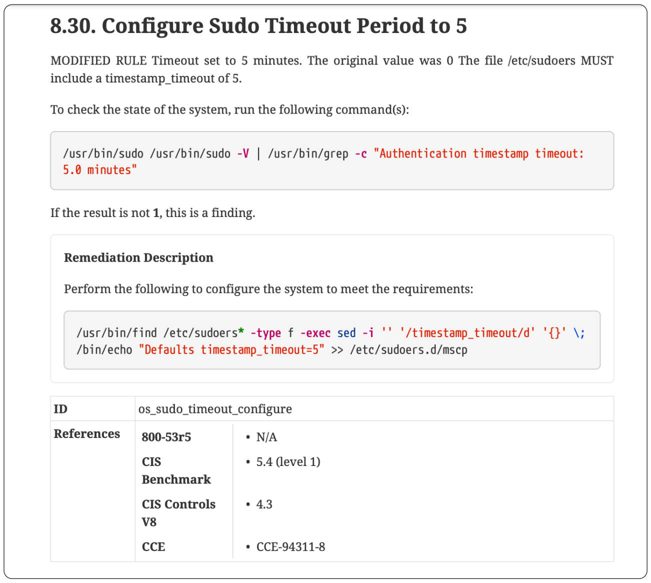
22. In the search field of the pdf, enter sudo timeout.

23. Click the highlighted page.



24. The modified rule will show with the new value of 5 and the will clearly state MODIFIED RULE in the explanation.

Including the phrase MODIFIED RULE in the explanation field is highly recommended when generating your report for an auditor. This makes it easy to identify all modified rules by searching for “MODIFIED RULE” in the report which will streamline the auditor’s review process.



8.30. Configure Sudo Timeout Period to 5

MODIFIED RULE Timeout set to 5 minutes. The original value was 0 The file /etc/sudoers MUST include a timestamp_timeout of 5.

To check the state of the system, run the following command(s):

```
/usr/bin/sudo /usr/bin/sudo -V | /usr/bin/grep -c "Authentication timestamp timeout:
5.0 minutes"
```

If the result is not **1**, this is a finding.

Remediation Description

Perform the following to configure the system to meet the requirements:

```
/usr/bin/find /etc/sudoers* -type f -exec sed -i '' '/timestamp_timeout/d' '{}' \;
/bin/echo "Defaults timestamp_timeout=5" >> /etc/sudoers.d/mscp
```

ID	os_sudo_timeout_configure	
References	**800-53r5**	• N/A
	CIS Benchmark	• 5.4 (level 1)
	CIS Controls V8	• 4.3
	CCE	• CCE-94311-8

This completes the guide.