Configure Jamf Compliance Editor and Jamf Pro for Compliance Reporting

Rev 20250422

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

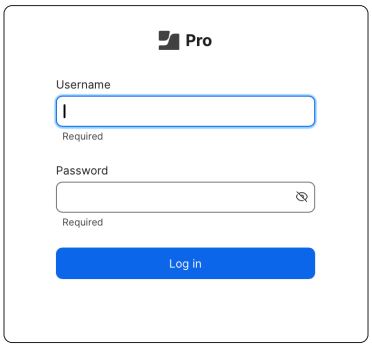
What You'll Need:
Learn what hardware, software, and information you'll need to complete the tutorials in this section.

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

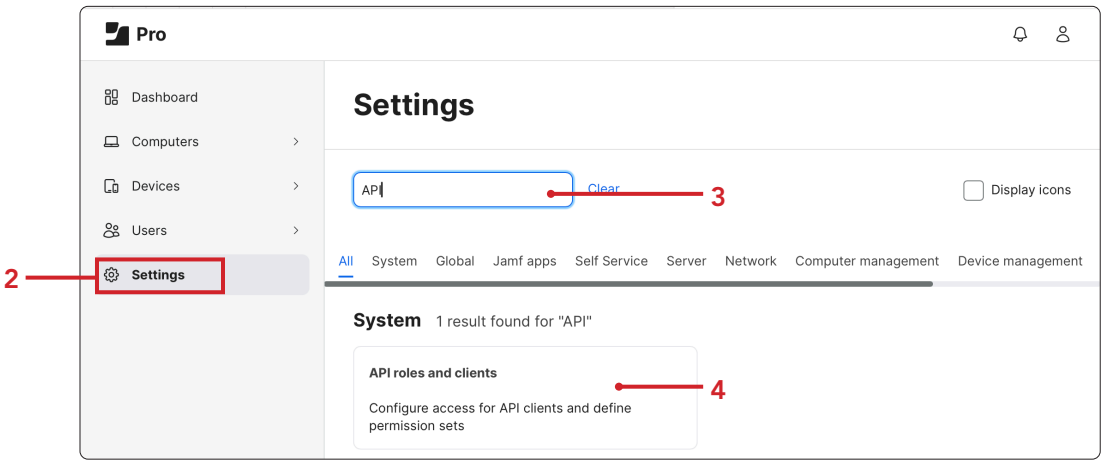
- A Jamf Pro server with administrative privileges to create or modify API roles and API Clients

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

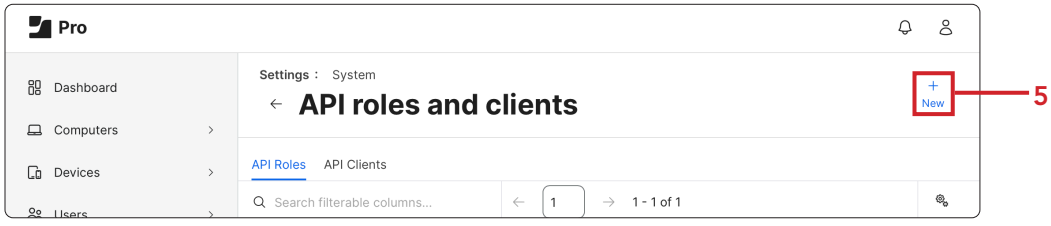
1. Log into your Jamf Pro Server with administrative privileges.



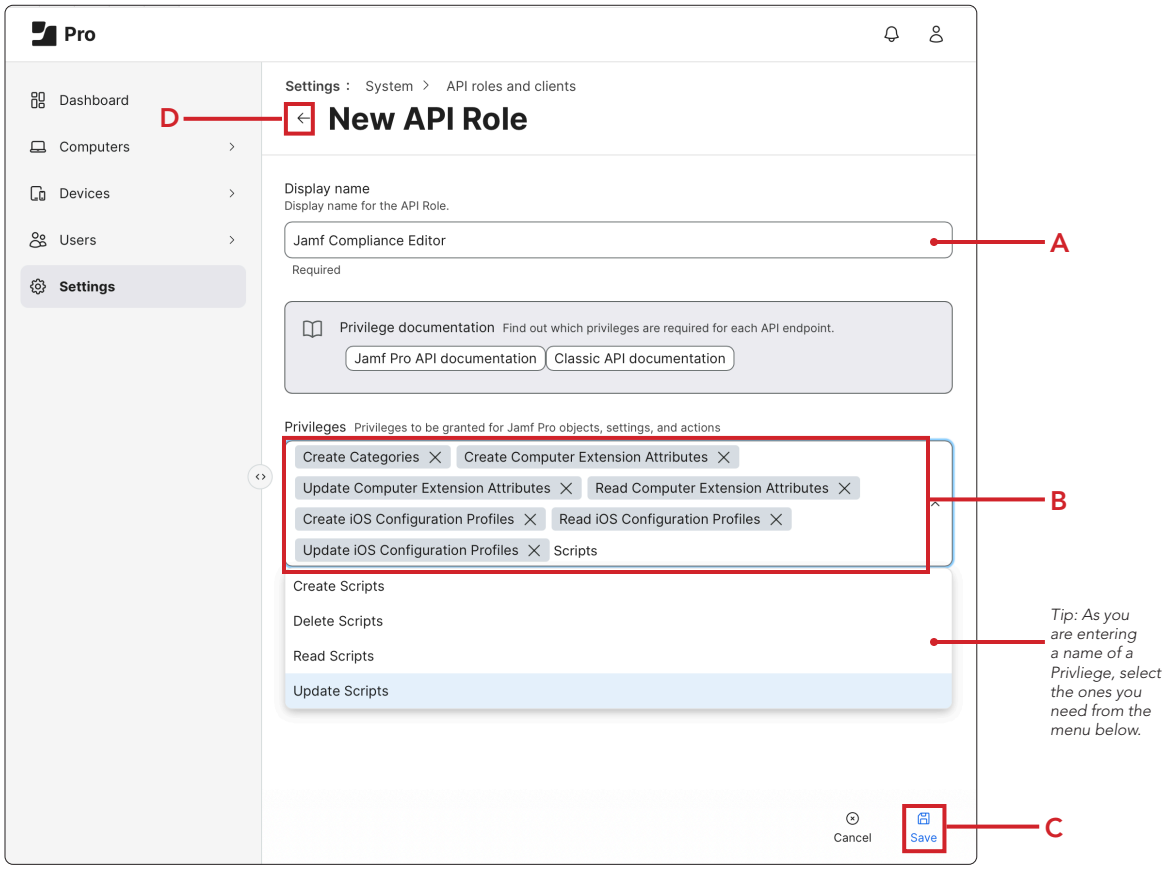
2. Click Settings.
3. Enter **API** in the search field.
4. Click on API roles and clients.



5. Click New.

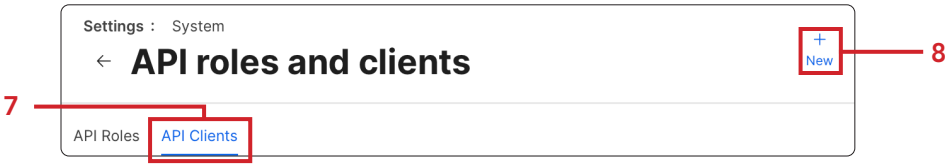


6. Configure the following:
   A. Enter **Jamf Compliance Editor** for the Display Name.
   B. Enter and select the following under Privileges:
      - **Categories**: Create
      - **Computer Extension Attributes**: Create, Read, Update
      - **macOS Configuration Profiles**: Create, Read, Update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

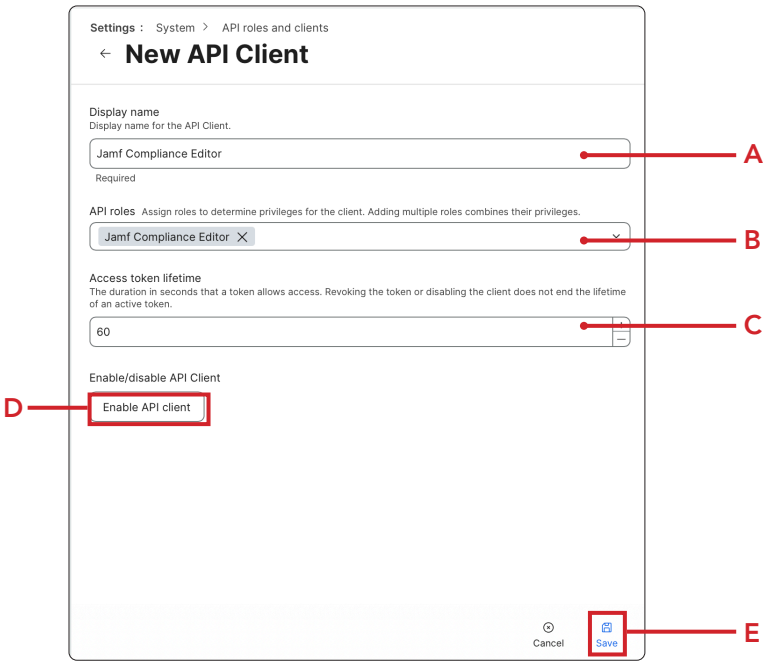


7. Click API Clients.

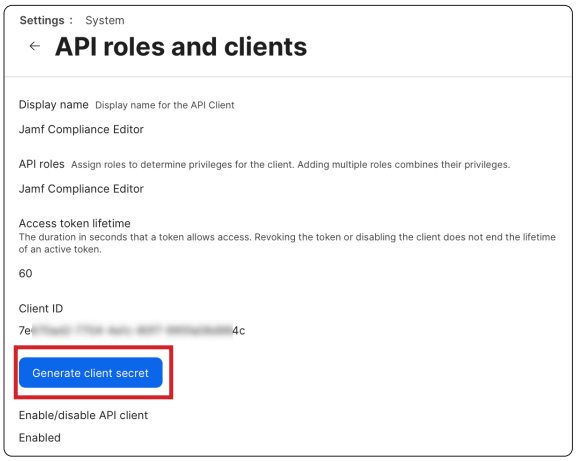
8. Click New (+).



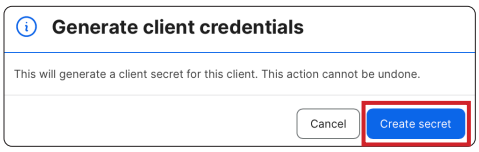
9. Configure the following:
    A. Enter **Jamf Compliance Editor** for the Display Name.
    B. Select **Jamf Compliance Editor** under API roles.
    C. Access token lifetime: **60.**
    D. Click enable API client.
    E. Click Save.



10. Click Generate client secret.

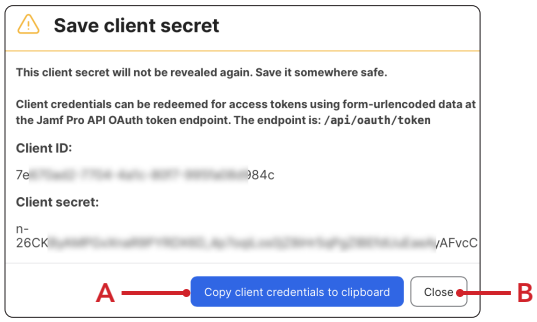


11. Click Create secret.

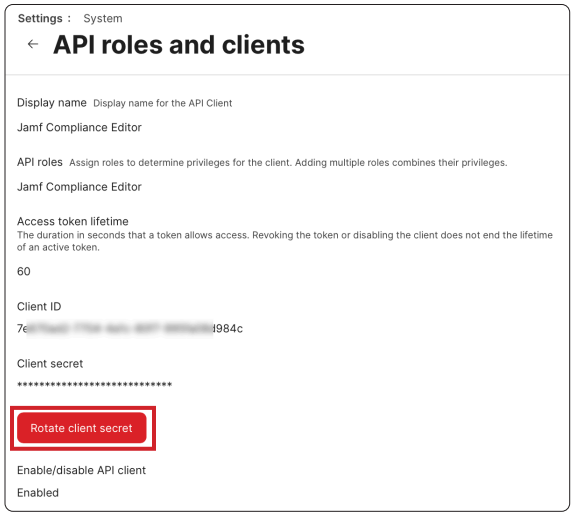


12. Perform the following:
    A. Click Copy client credentials to clipboard and paste into a text edit document. Save it to your Desktop with a name of your choosing.
    B. Click Close.

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



13. Confirm you see the Rotate client secret button.



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.

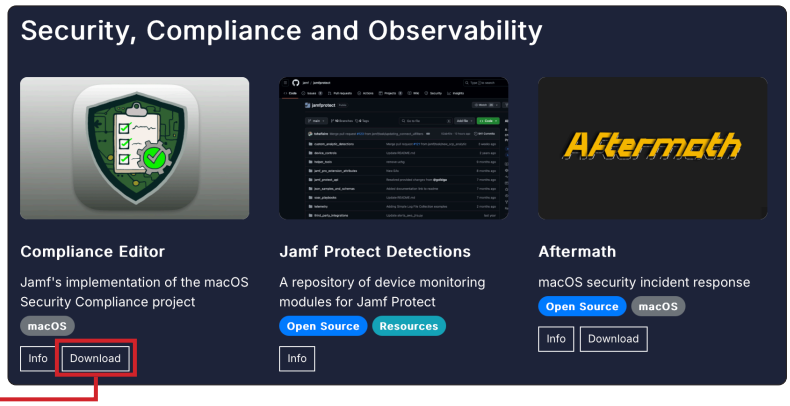
What You'll Need:
Learn what hardware, software, and information you'll need to complete the tutorials in this section.

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

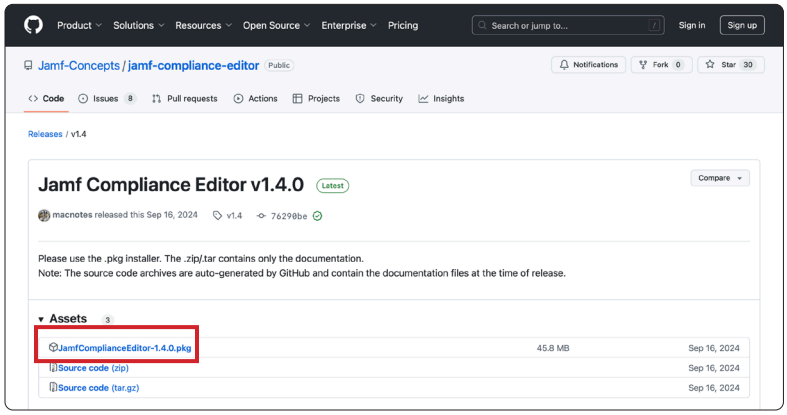
In this section we install and configure the Jamf Compliance Editor application to pre configure the Jamf Pro Server with the needed items for compliance.

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

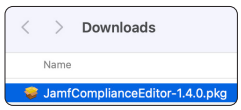


Click Download to receive Compliance Editor

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.

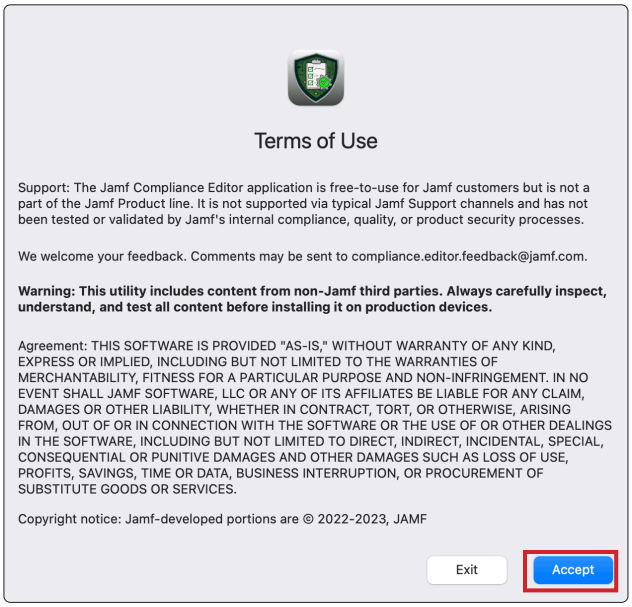


4. Go to your Downloads folder and double-click to open JamfComplianceEditor-1.4.0.pkg and follow the default prompts to install it.



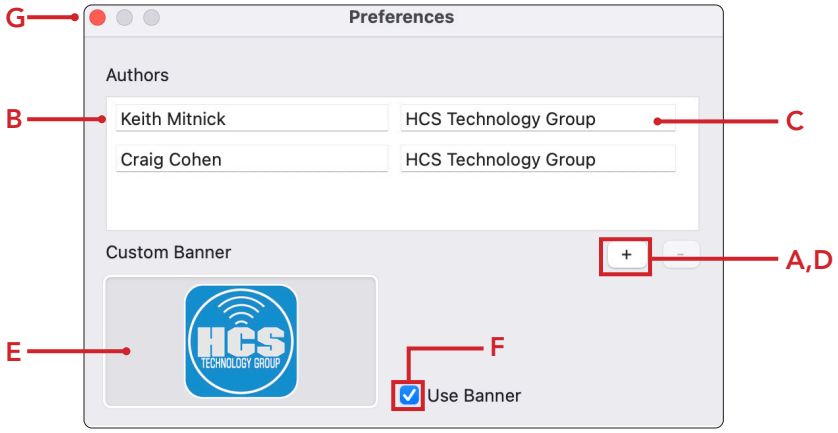
5. Open the Jamf Compliance Editor located in the Applications folder.

6. Read the Terms of Use then click Accept.



7. Click Jamf Compliance Editor menu.
8. Select Settings (⌘,).

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.

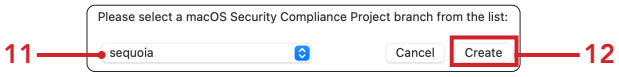


10. Configure the following:

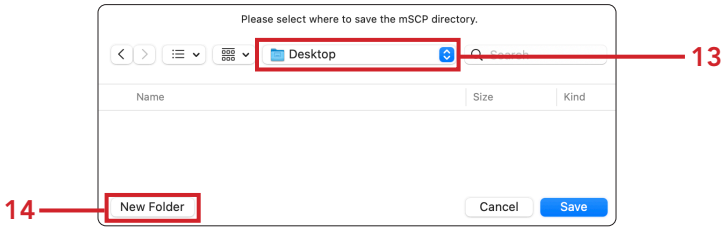
   A. Select the device you're looking to configure. macOS, iOS/iPadOS, visionOS - This guide will use macOS.
   B. Click Create new project.

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

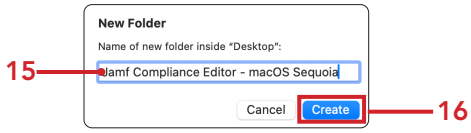
12. Click Create.



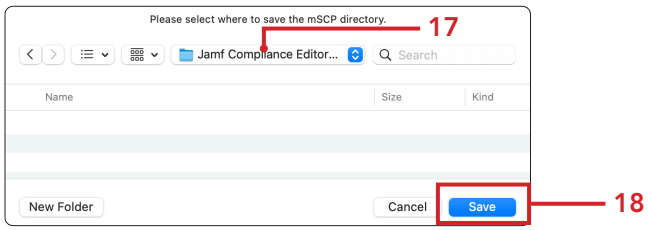
13. Select the Desktop as the destination.
14. Click New Folder.



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.



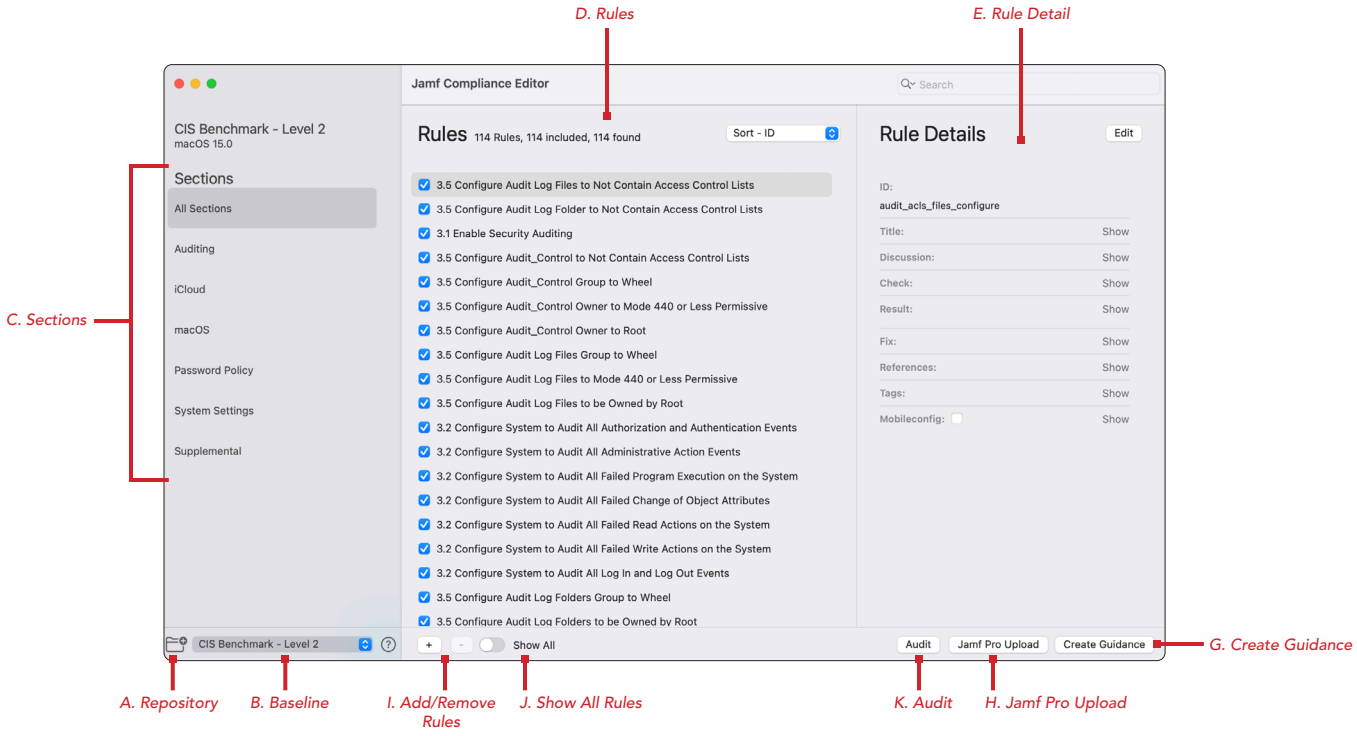
17. Confirm the location matches what you created in the previous step.
18. Click Save.



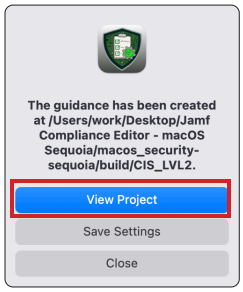
19. Select a Benchmark. This guide will select CIS Benchmark - Level 2
20. Click OK.

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)

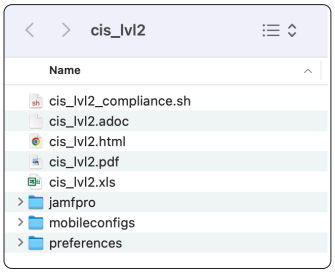
22. Click the Create Guidance button.



23. Click View Project.

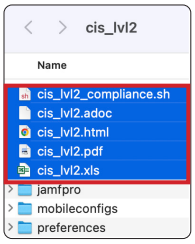


24. Confirm you see the the cis_lvl2 project files. These files contain everything that was configured when the Create Guidance button was clicked. The files are located in the project folder we created earlier in this guide. The path is: ~/Desktop/Jamf\ Compliance\ Editor\ -\ macOS\ Sequoia/macos_security-sequoia/build/cis_lvl2

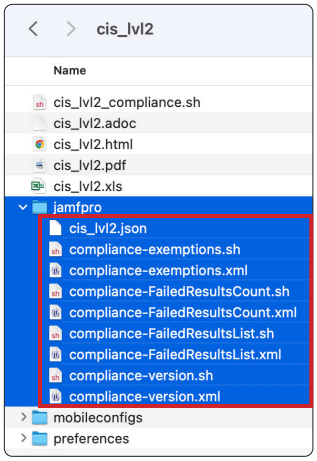


25. The script, ***cis_lvl2_compliance.sh***, is used with a policy in Jamf Pro to make sure all the CIS Level 2 guidance is accurate on all Mac computers. If a rule was changed by the user, the script can set it back to the CIS Level 2 default setting.

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.



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.

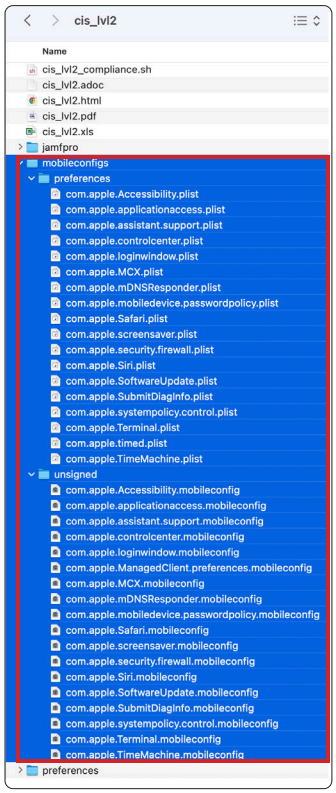


28. The three scripts: ***compliance-exemptions.sh, compliance-FailedResultsCount.sh, compliance-FailedResultsList.sh*** are used when running a local Mac audit without using Jamf Pro.

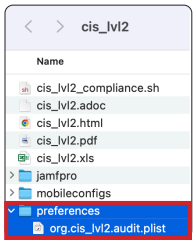
29. The three xml files, ***compliance-exemptions.xml, compliance-FailedResultsCount.xml, compliance-FailedResultsList.xml***, are imported into Jamf Pro and will create Extension Attributes for reporting.

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.

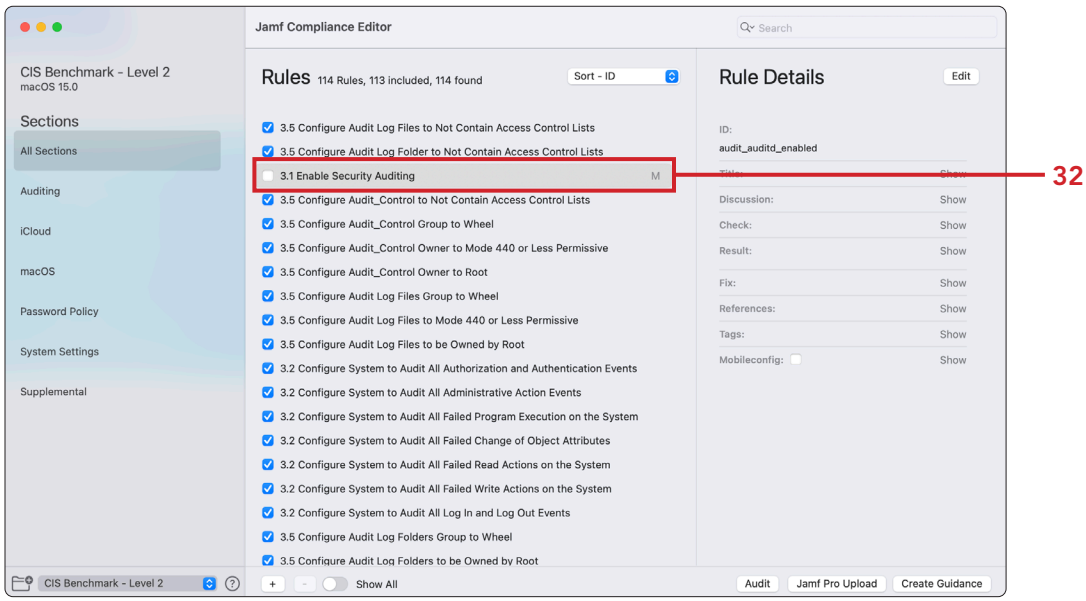


31. In the ***preferences*** folder, a file named ***org.cis_lvl2.audit.plist*** is used when running a local Mac audit without using Jamf Pro.



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.

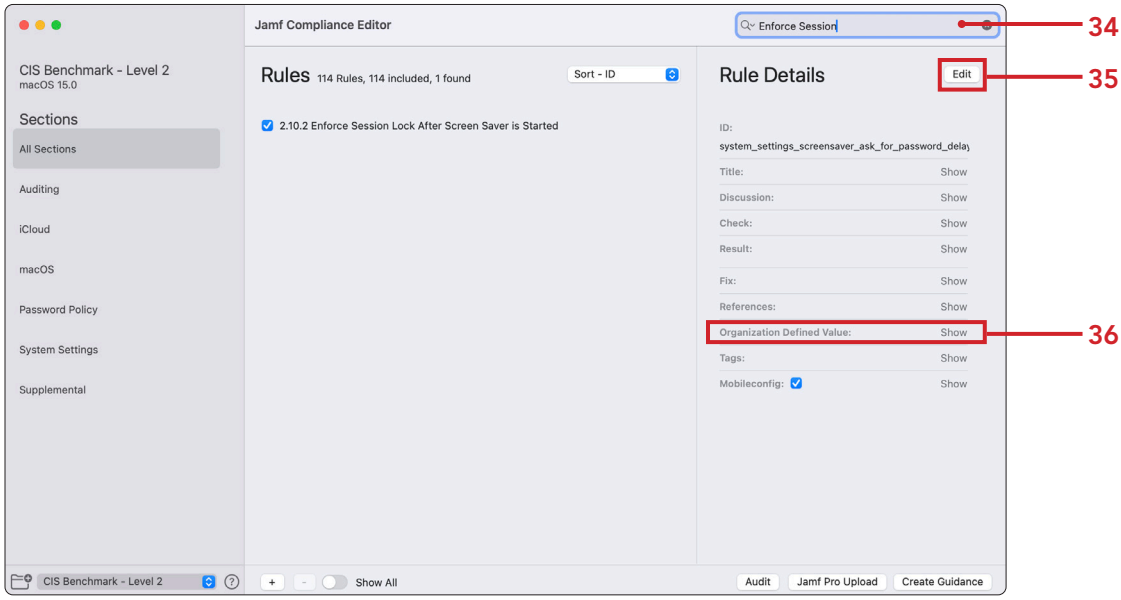
33. Re-enable the 3.1 Enable Security Auditing.



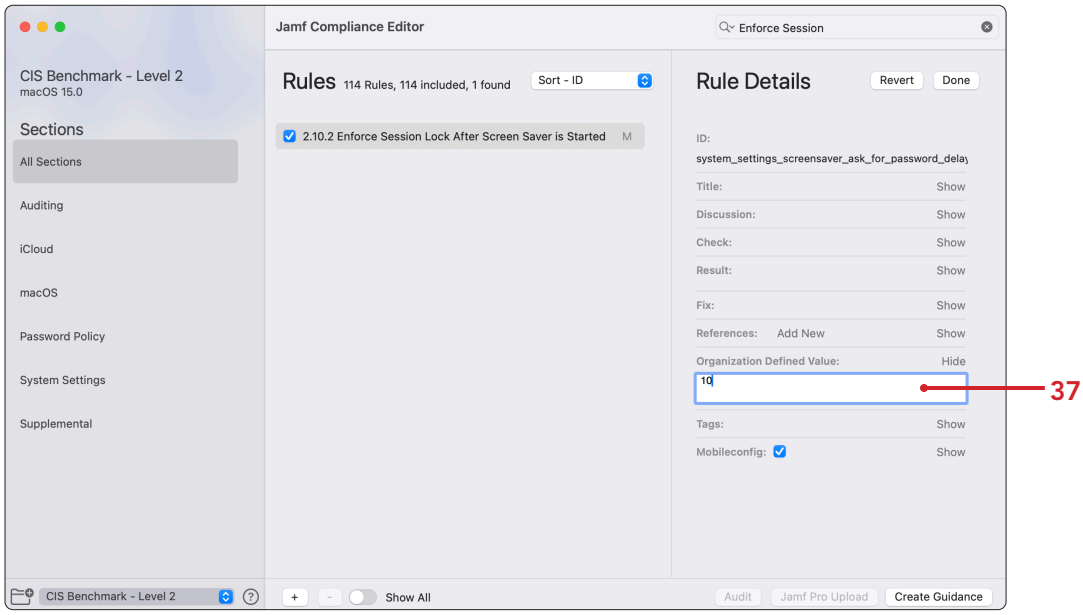
34. In the search field, enter **Enforce Session**.

35. In the Rule Details section, click Edit.

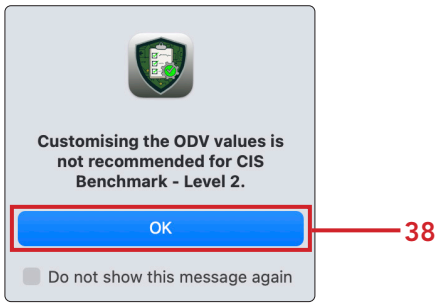
36. Click Show for Organization Defined Value.



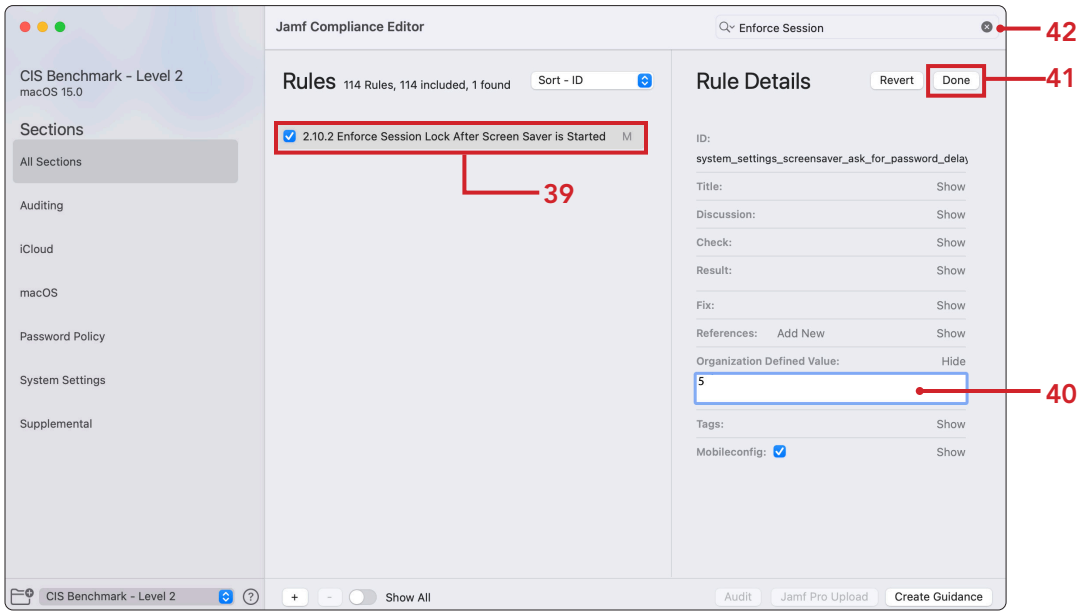
37. In the Organization Defined Value field, change from 5 to 10.



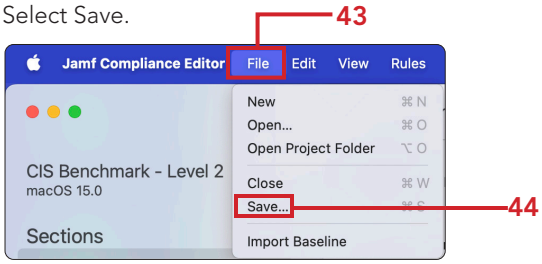
38. Confirm a message that states modifying is not recommended. Click OK.



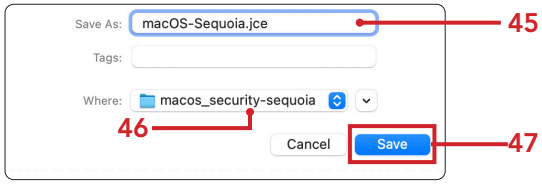
39. In the rules section, Notice the letter "M" next to the Enforce Session rule. This means the rule has been modified.
40. In the Organization Defined Valuefield, change from 10 to 5 to keep things back to the default value.
41. Click Done
42. Remove (⊗) "Enforce Session" from the search field.
    NOTE: This was to demonstrate that a rule does not have to be disabled to be modified in a benchmark.



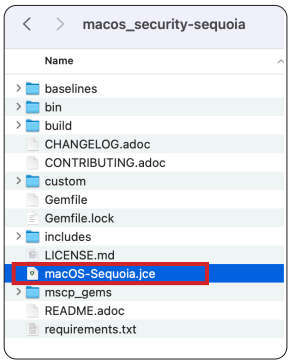
43. Click File.
44. Select Save.



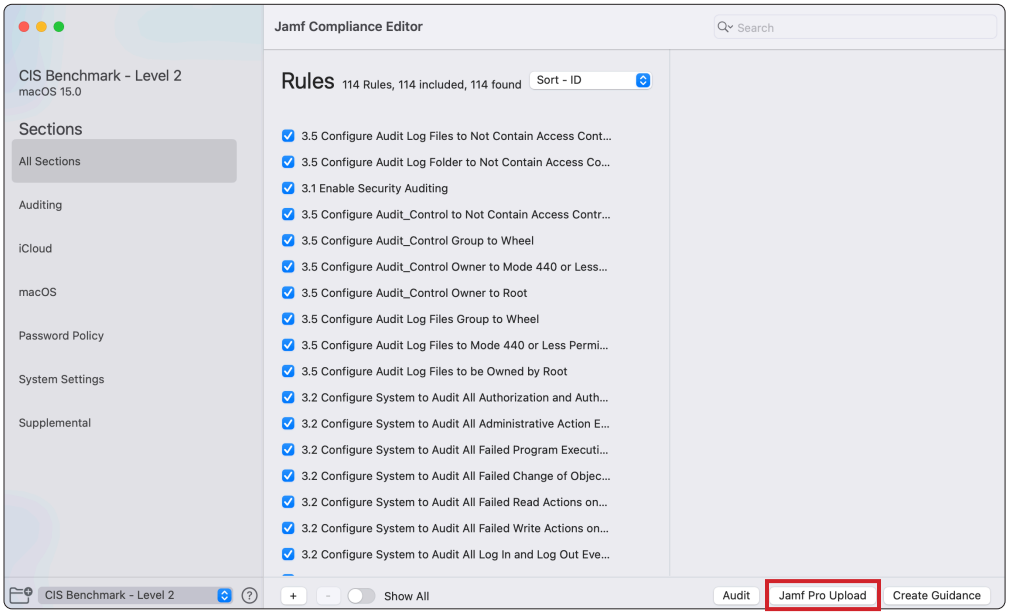
45. Enter **macOS-Sequoia.jce** for the File Name.
46. Save to a location of your choosing. This guide will save it to the existing project folder.
47. Click Save.



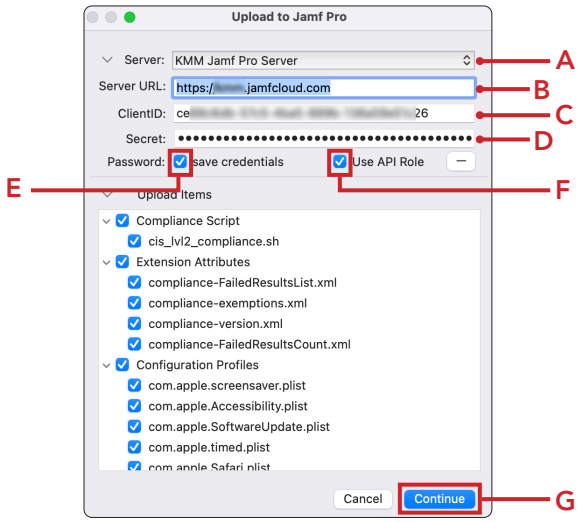
48. Confirm the macOS-Sequoia.jce was created in the location you saved it in.



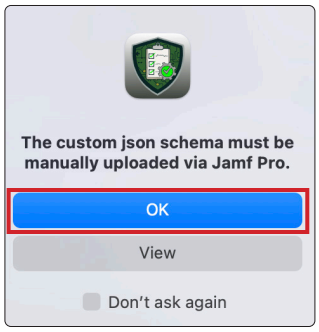
49. Click Jamf Pro Upload.



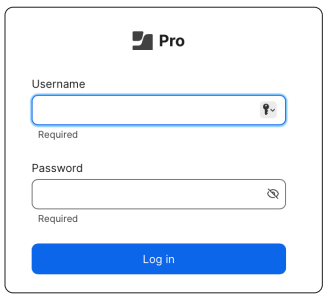
50. Configure the following:
    A. Enter the name of your Jamf Pro server.
    B. Enter the URL of your Jamf Pro server.
    C. Enter the client ID we saved in section one of this guide.
    D. Enter the secret we saved in section one of this guide.
    E. Select the checkbox for save credentials.
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



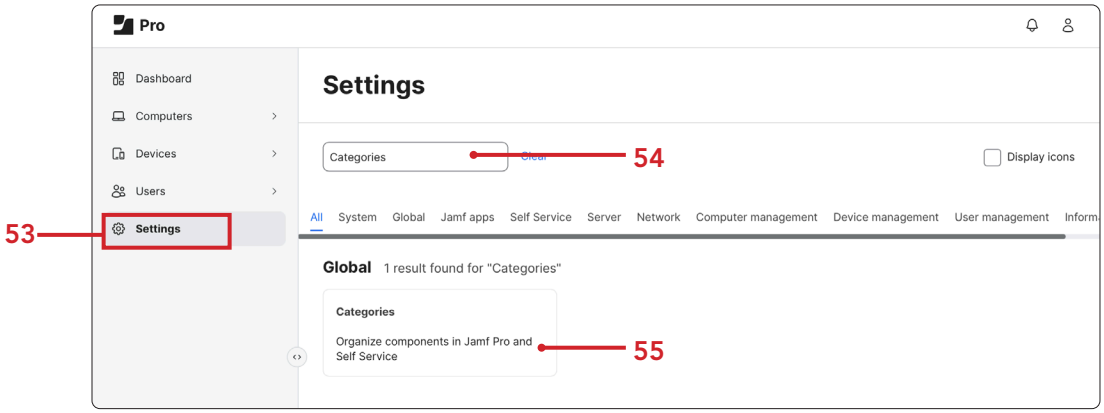
51. Click OK.



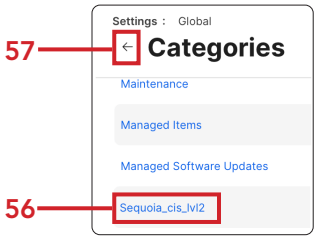
52. Let's confirm the category, configuration profiles, extension attributes and scripts were created by the JCE application, Switch back to your Jamf Pro server. If necessary, login with administrative privileges.



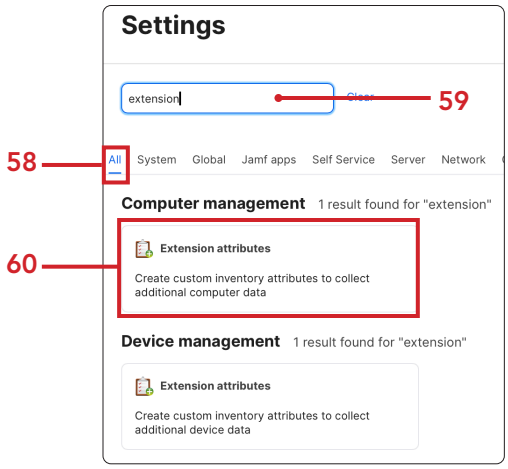
53. Select Settings.
54. Enter categories in the search field.
55. Click Categories.



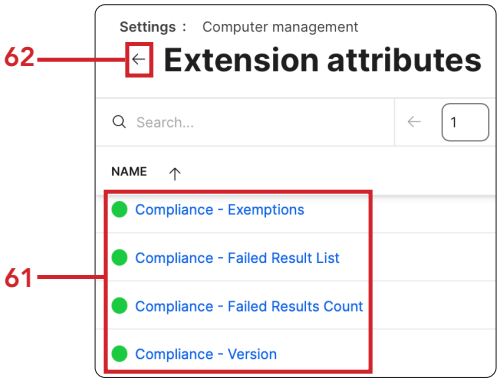
56. Confirm a category named Sequoia_cis_lvl2 was created.
57. Click Previous (←).



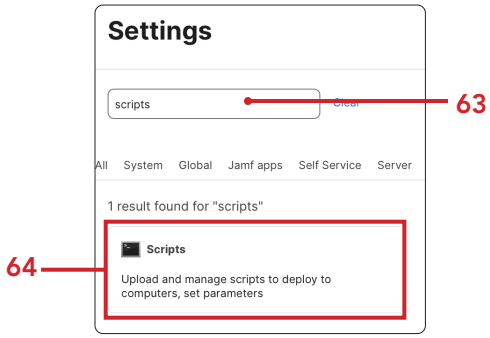
58. Click All.
59. Enter extension in the search field.
60. Click Extension attributes under Computer management.



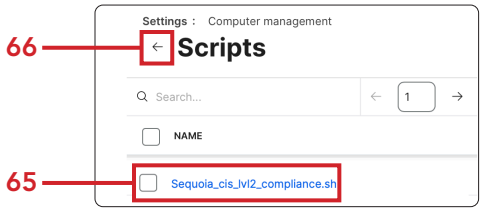
61. Confirm that four Extension Attributes that start with Compliance were created.
62. Click Previous (←).



63. Enter scripts in the search field.
64. Click Scripts.



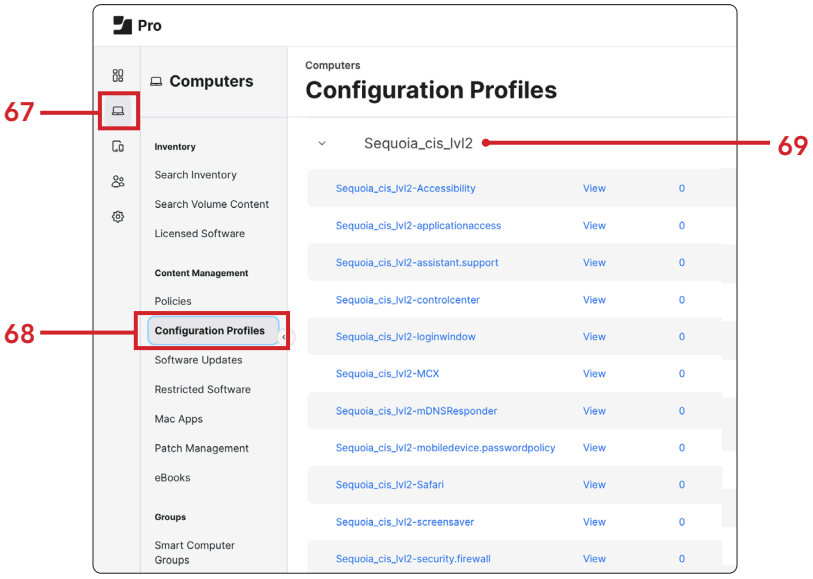
65. Confirm a script named Sequoia_cis_lvl2_compliance.sh was created.
66. Click Previous (←).



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.



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

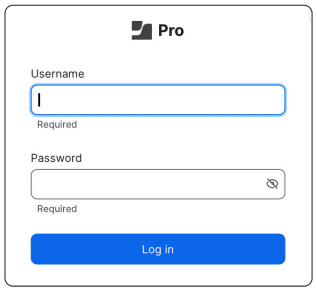
What You'll Need:
Learn what hardware, software, and information you'll need to complete the tutorials in this section.

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

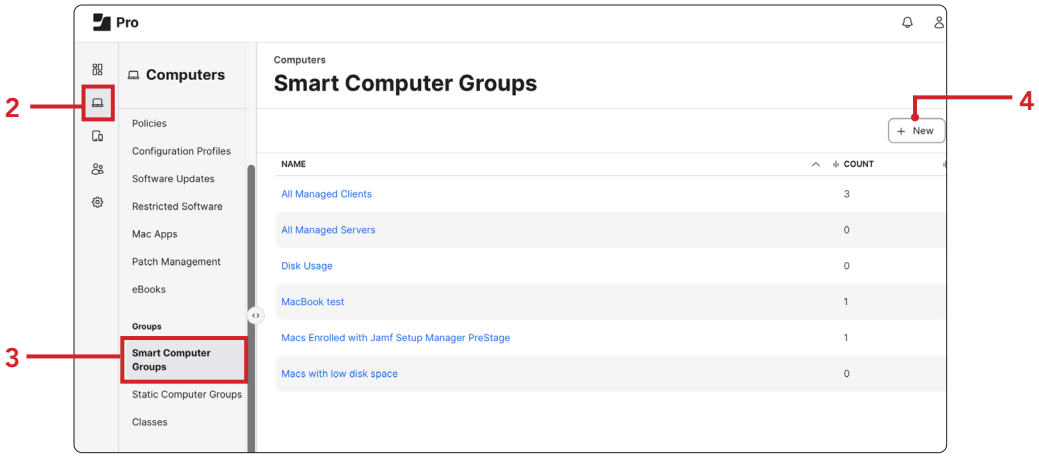
- A Jamf Pro server with administrative privileges

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

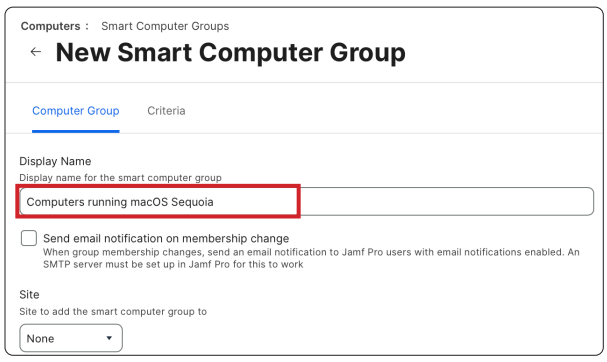
1. If necessary, Log into your Jamf Pro Server with administrative privileges.



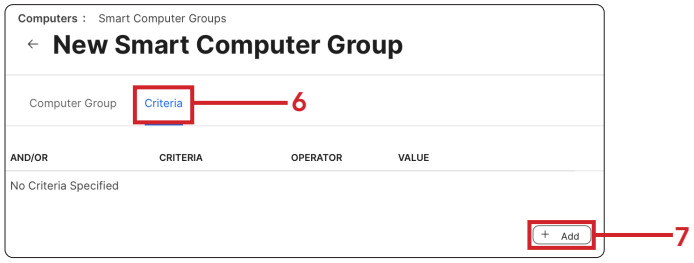
2. Click Computers.
3. Click Smart Computer Groups.
4. Click New.



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

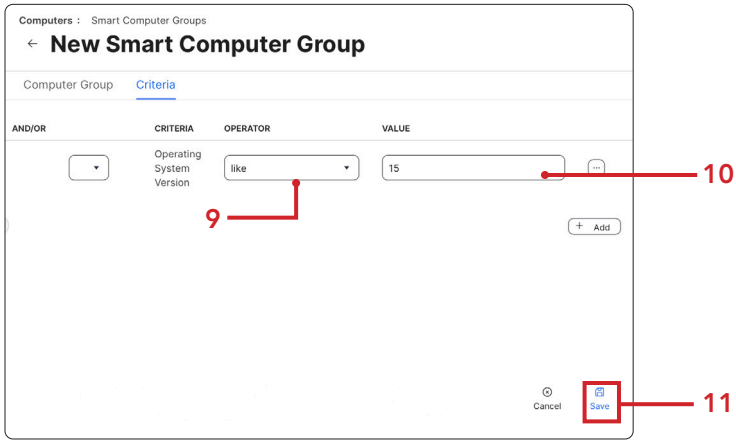


6. Click Criteria.
7. Click Add (+).

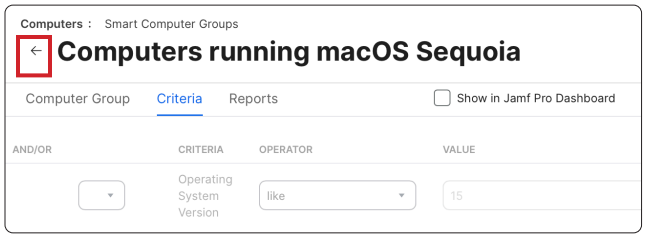


8. Scroll down to Operating System Version and click Choose.

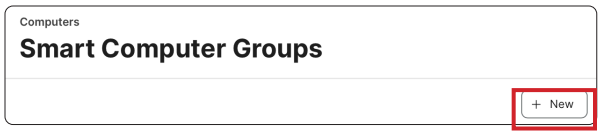
9. Set the Operator to **like.**
10. Enter the value to your needs. This guide will use **15.**
11. Click Save.



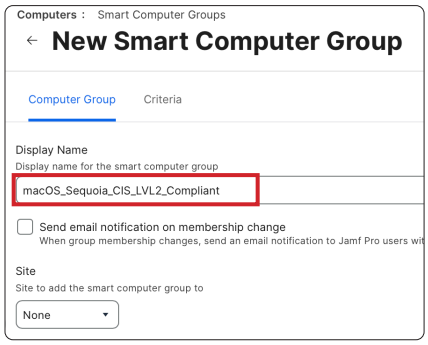
12. Click Previous (←).



13. Click New (+).

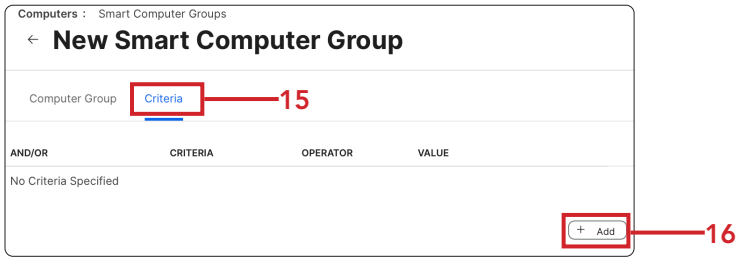


14. Enter **macOS_Sequoia_CIS_LVL2_Compliant** for the Display Name.
    NOTE: Change the macOS name to your needs.



15. Click Criteria.

16. Click Add (+).

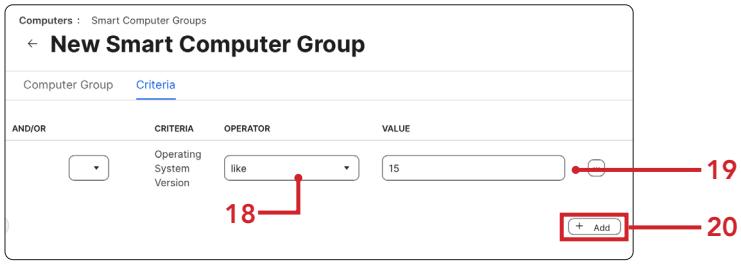


17. Scroll down to Operating System and click Choose.

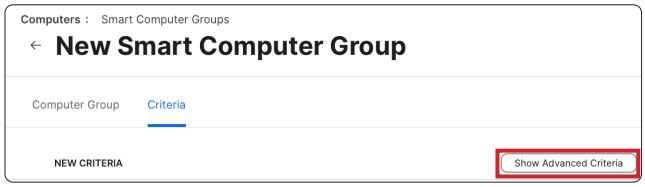
18. Set the Operator to **like.**

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

20. Click Add (+).



21. Click Show Advanced Criteria, if necessary.



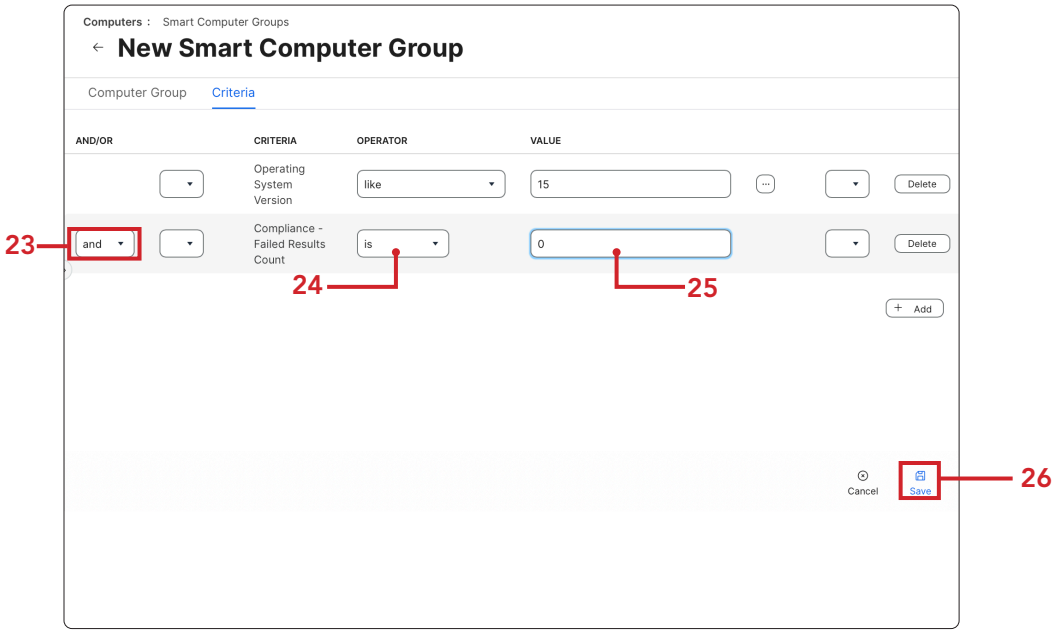
22. Scroll down to Compliance - Failed Results Count and click Choose.

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

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

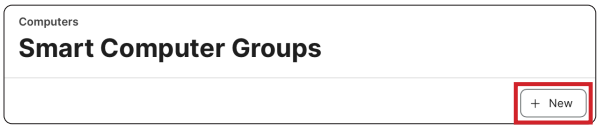
25. Enter the Value: **0.**

26. Click Save.

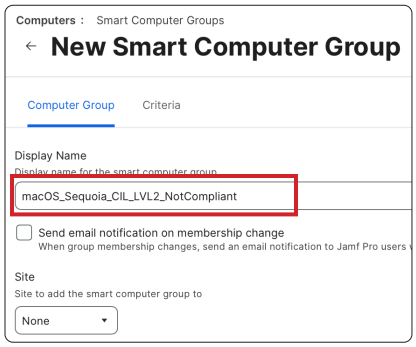


27. Click Previous (←).

28. Click New (+).

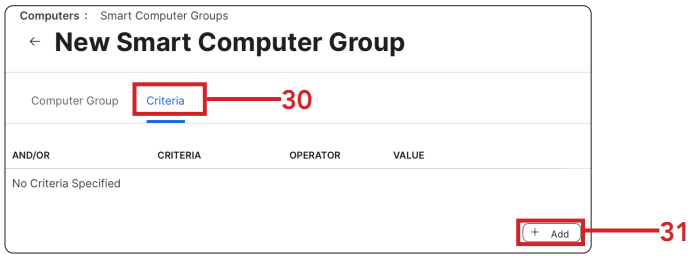


29. For the Display Name, enter: **macOS_Sequoia_CIL_LVL2_NotCompliant.**

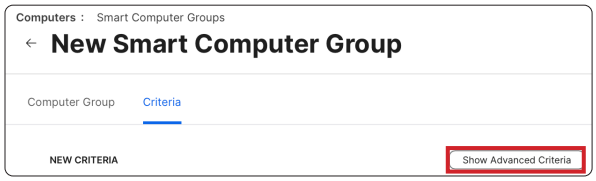


30. Click Criteria.

31. Click Add.

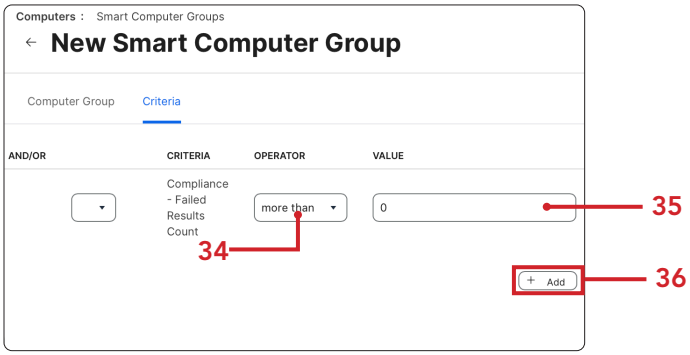


32. Click Show Advanced Criteria.



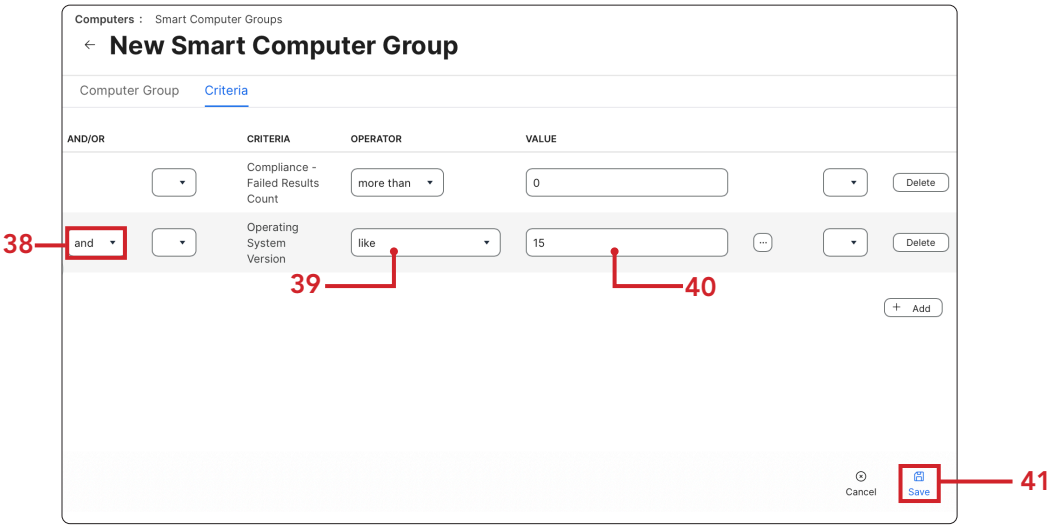
33. Scroll down to Compliance - Failed Results Count and click Choose.

34. For the Operator, select **more than.**
35. Enter **0** for the Value.
36. Click Add.



37. Scroll down to Operating System and click Choose.

38. From the menu, select **and.**
39. Set the Operator to **like.**
40. Enter **15** for the Value.
41. Click Save.



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

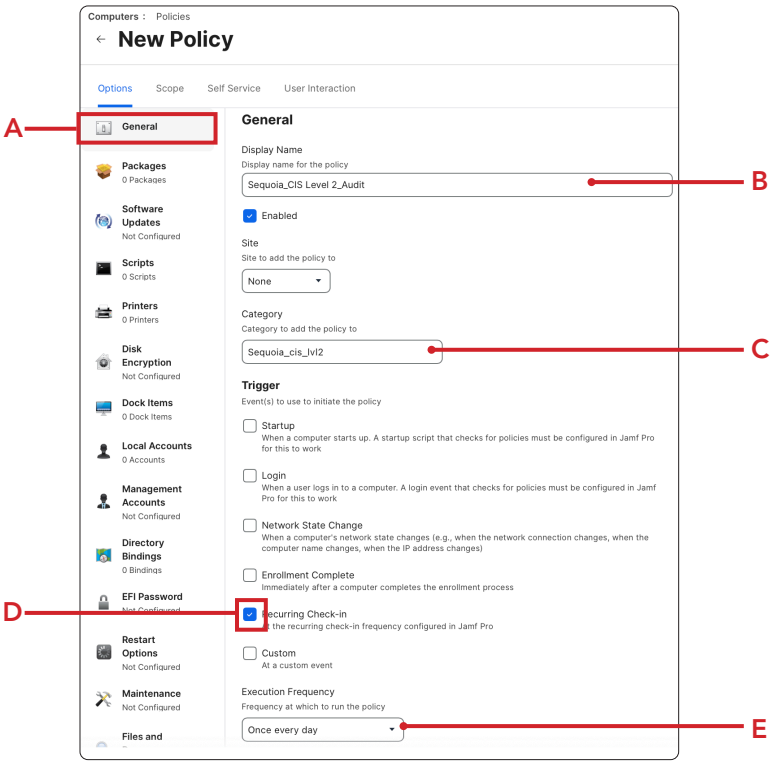
- Script flags: `--reset --check`
- Purpose: Clears previous results and runs a fresh audit.

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

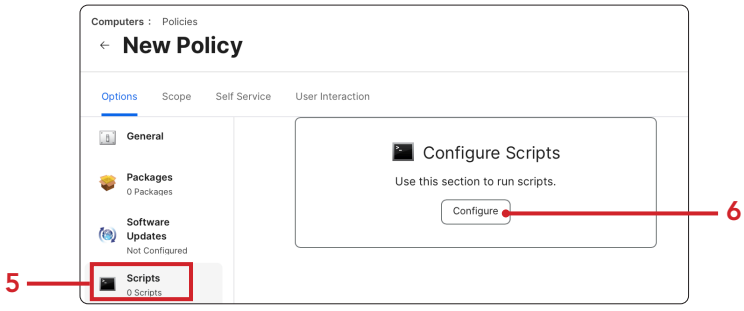
```
usage=(
    "$0 Usage"
    "$0 [--check] [--fix] [--cfc] [--stats] [--compliant] [--non_compliant] [--reset] [--reset-all] [--quiet=<value>]"
    " "
    "Optional parameters:"
    "--check            :   run the compliance checks without interaction"
    "--fix              :   run the remediation 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.**

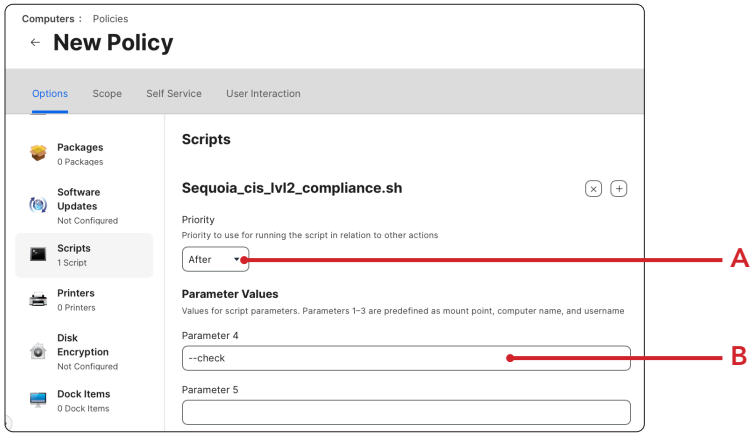


5. Select Scripts.
6. Click Configure.



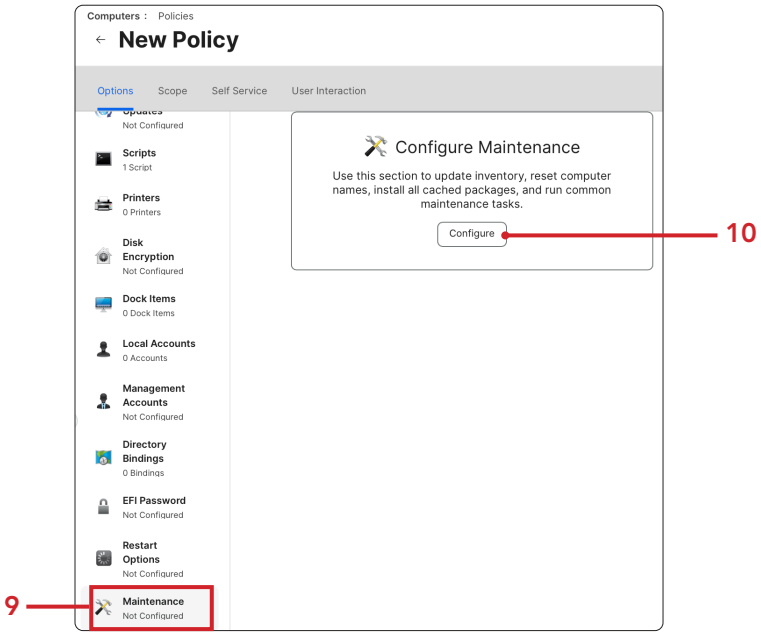
7. Find the sequoia_cis_lvl2_compliance.sh and click Add.

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.

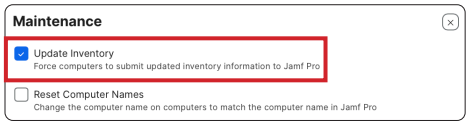


9. Scroll down and click Maintenance.

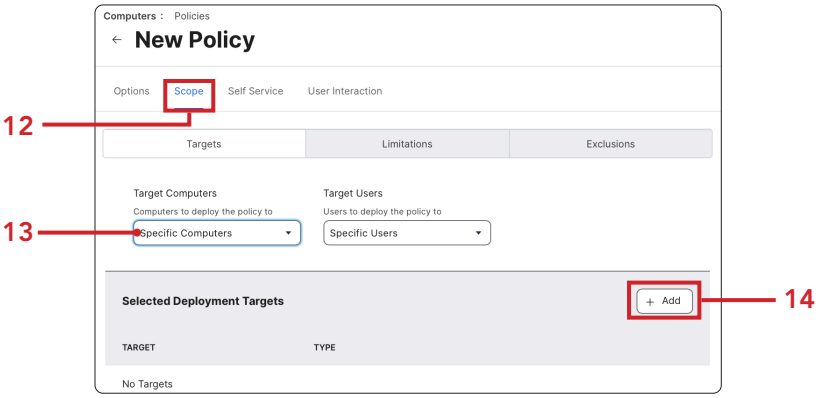
10. Click Configure.



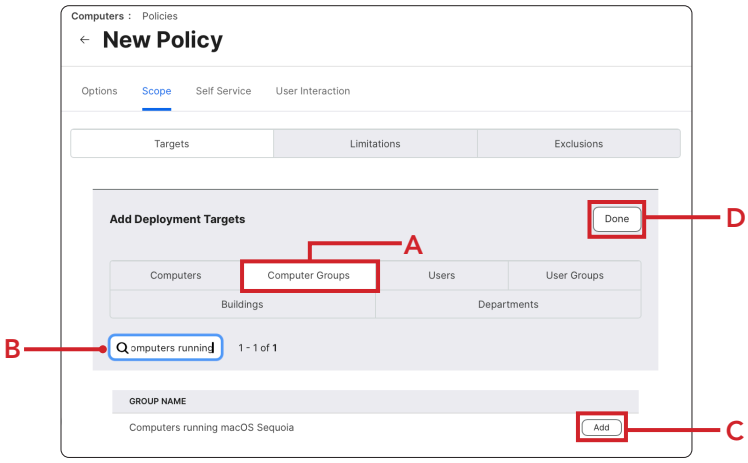
11. Confirm the the checkbox is selected for Update Inventory.



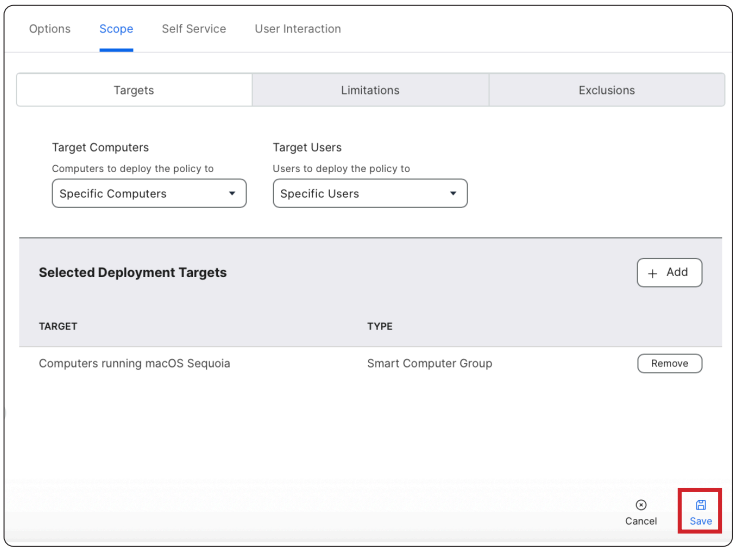
12. Click Scope.
13. Confirm Specific Computers is selected for Target Computers.
14. Click Add.



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.



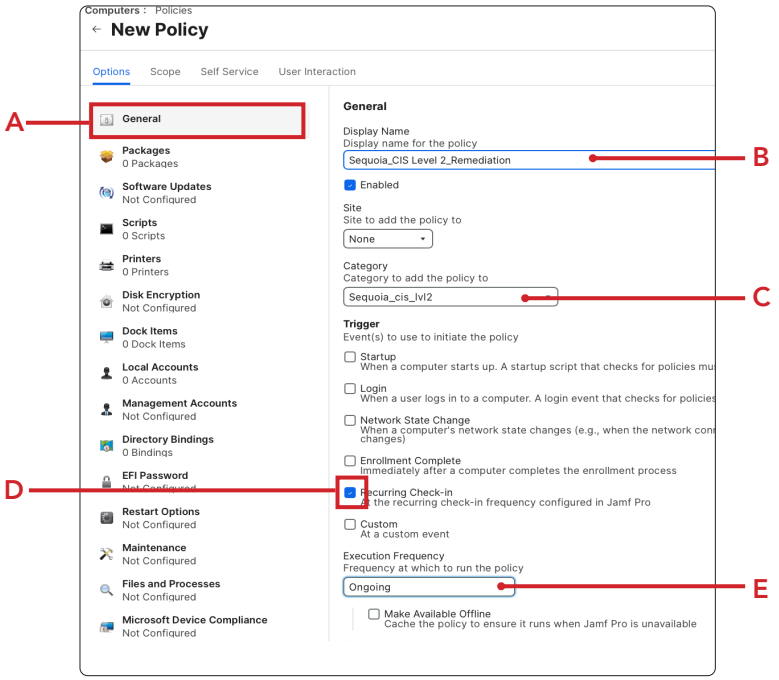
16. Click Save.



17. Click Previous (←).

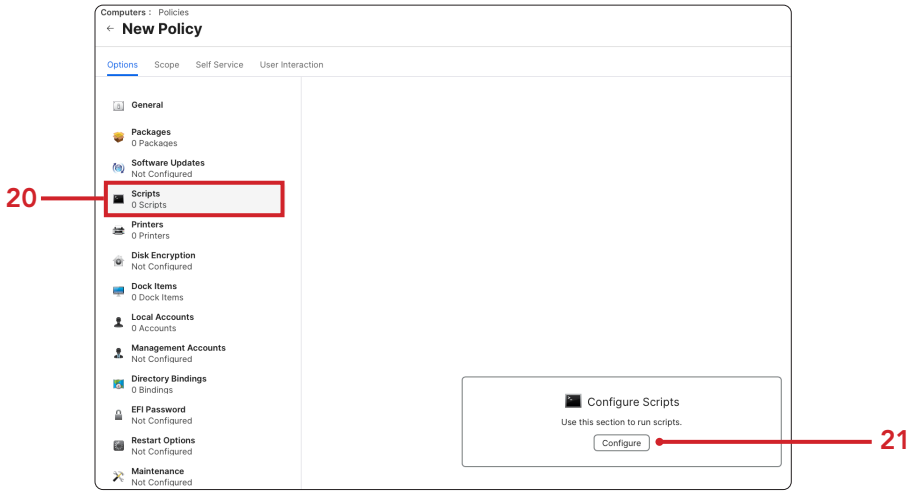
18. Click New (+).

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

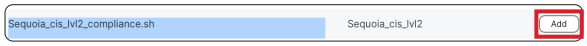


20. Click Scripts.

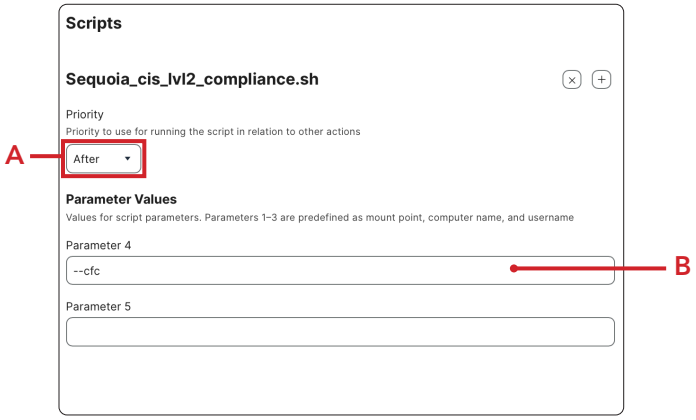
21. Click Configure.



22. Locate sequoia_cis_lvl2_compliance.sh and click Add.

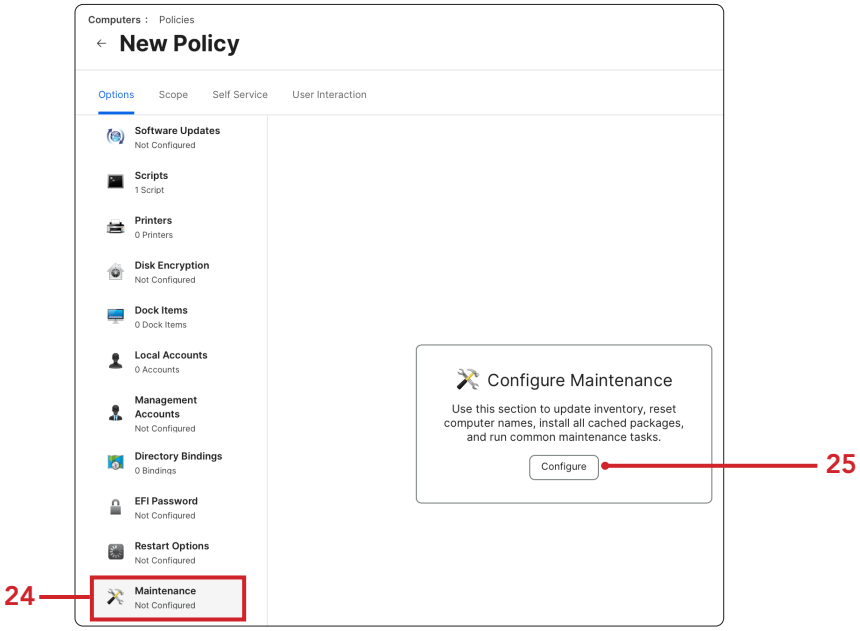


23. Configure the following:
    A. Priority: **After.**
    B. Parameter 4: **--cfc.**
       NOTE: The --cfc flag runs a compliance check, fixes anything that is not compliant, then run another check. It does all of this without any user interaction and it part of the compliance script.

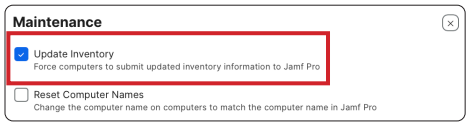


24. Scroll down and select Maintenance.

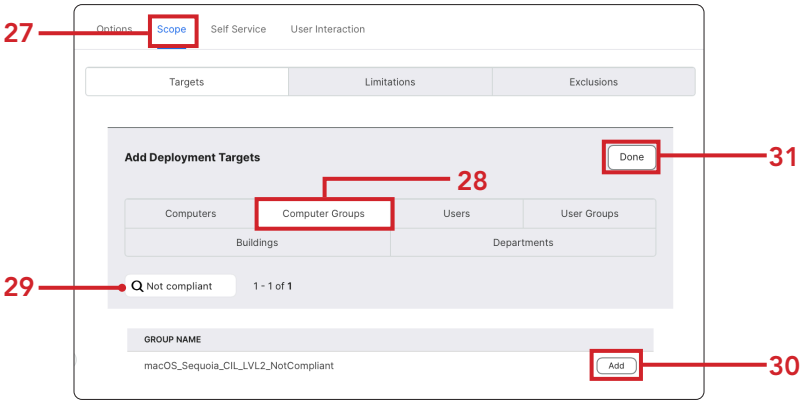
25. Click Configure.



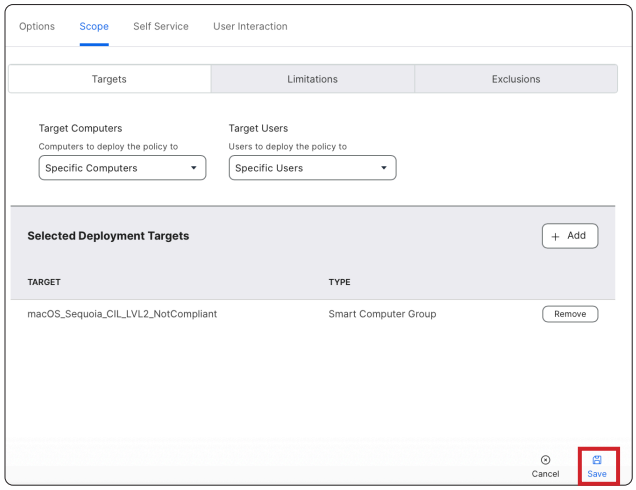
26. Confirm the checkbox is selected for Update Inventory.



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.



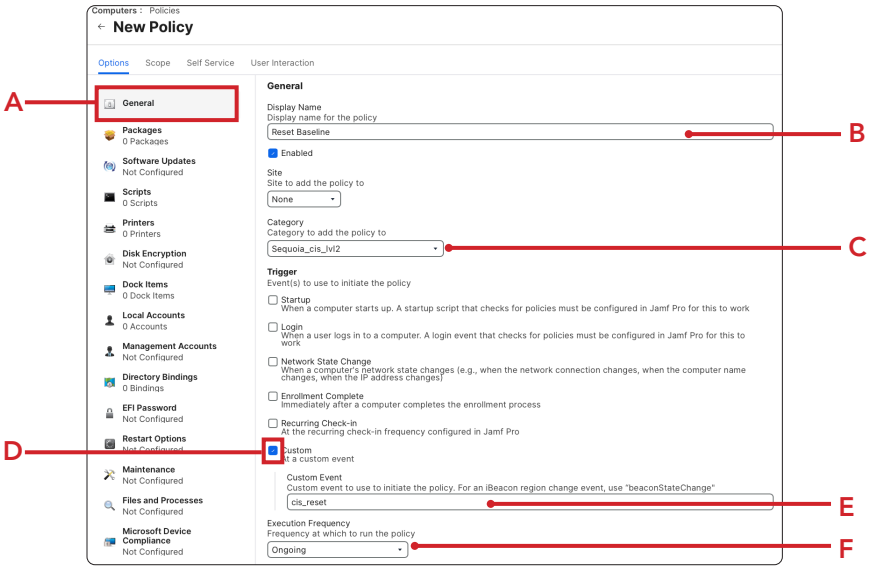
33. Click Previous (←).

34. Click New (+).

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

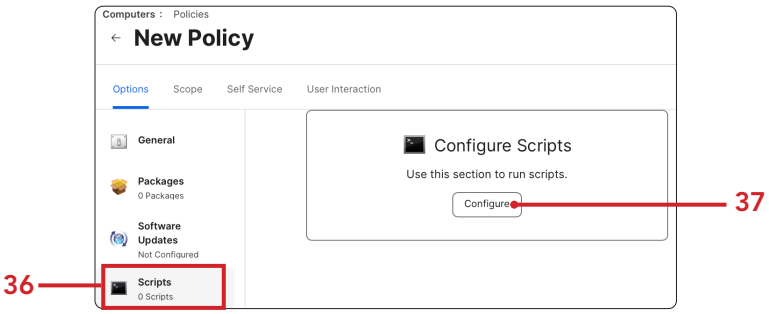
    NOTE: This policy needs to be run manually either by offering it in Self Service or by running the command:

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



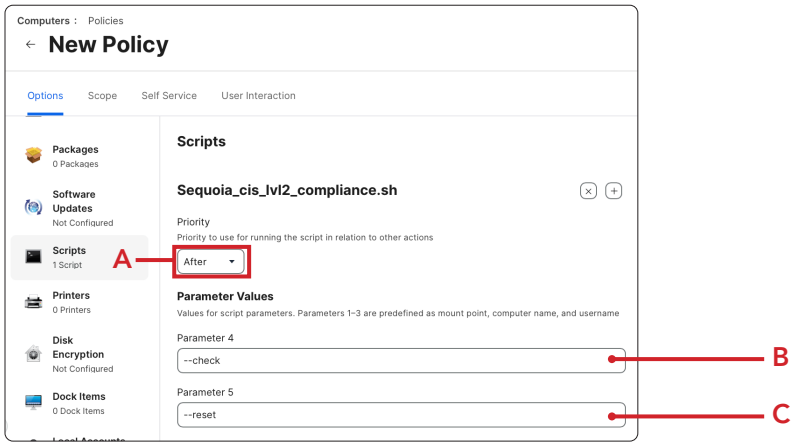
36. Click Scripts.

37. Click Configure.



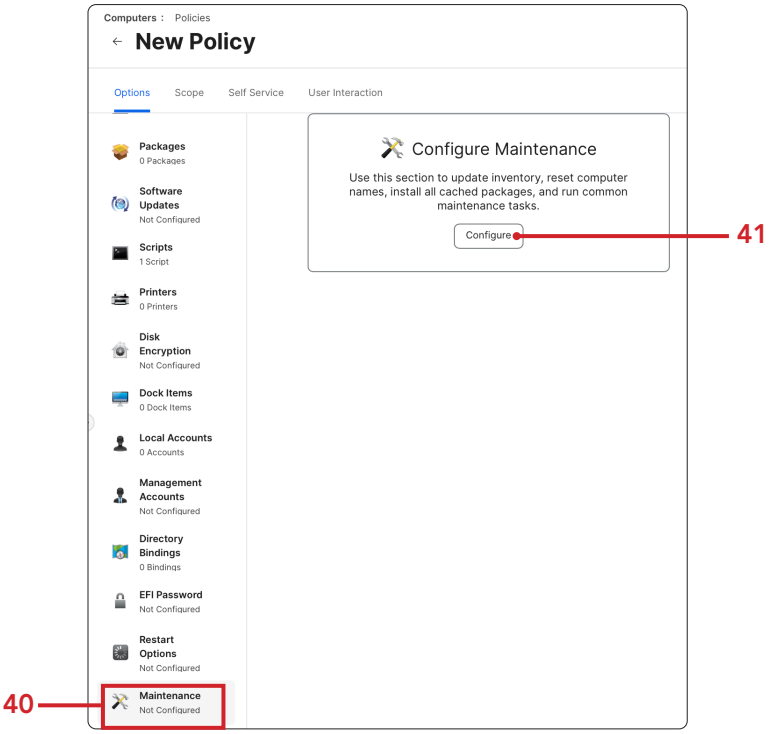
38. Find the sequoia_cis_lvl2_compliance.sh and click Add.

39. Configure the following:
    A. Priority: After.
    B. Parameter 4: **--check**.
    C. Parameter 5: **--reset**.

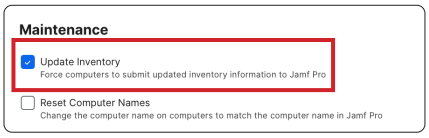


40. Click Maintenance.

41. Click Configure.



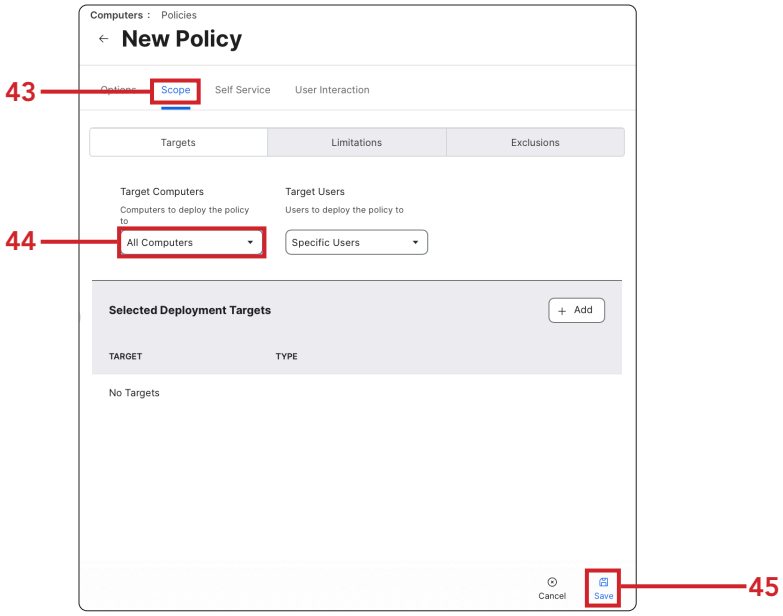
42. Confirm the the checkbox is selected for Update Inventory.



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.



46. Click Previous (←).

47. Go to the Sequoia_cis_lvl2 category.

Expand the category to view the policies

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

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:

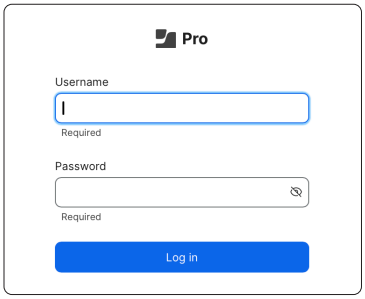
- A Jamf Pro server with administrative privileges

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.

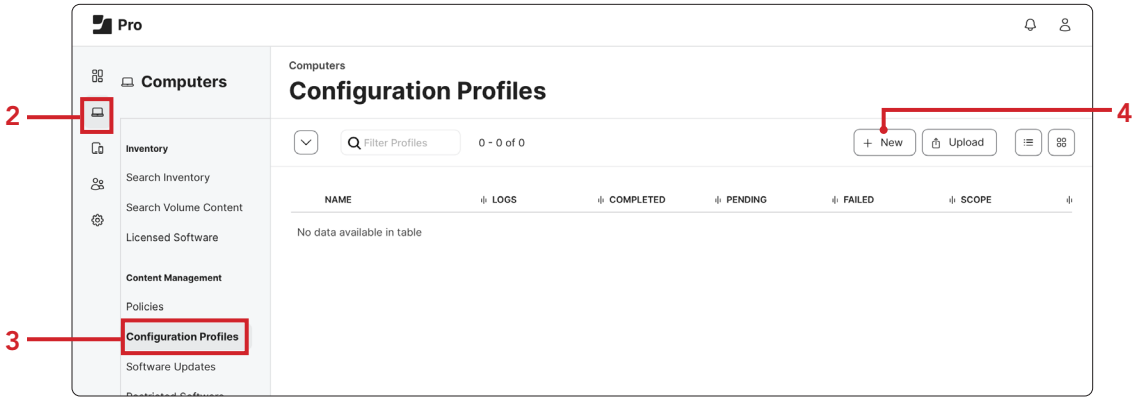
Earlier in the guide, we created an Extension Attribute called "Compliance – Failed Result List." When a JSON schema is used to manage exemptions, those exemptions will still appear in the "Compliance – Failed Result List."

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

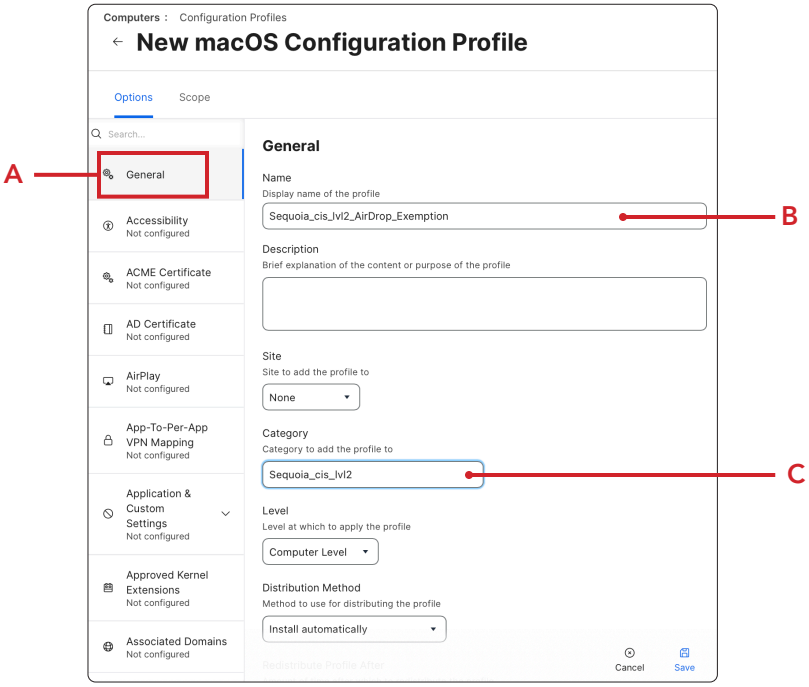
1. If necessary, Log into your Jamf Pro Server with administrative privileges.



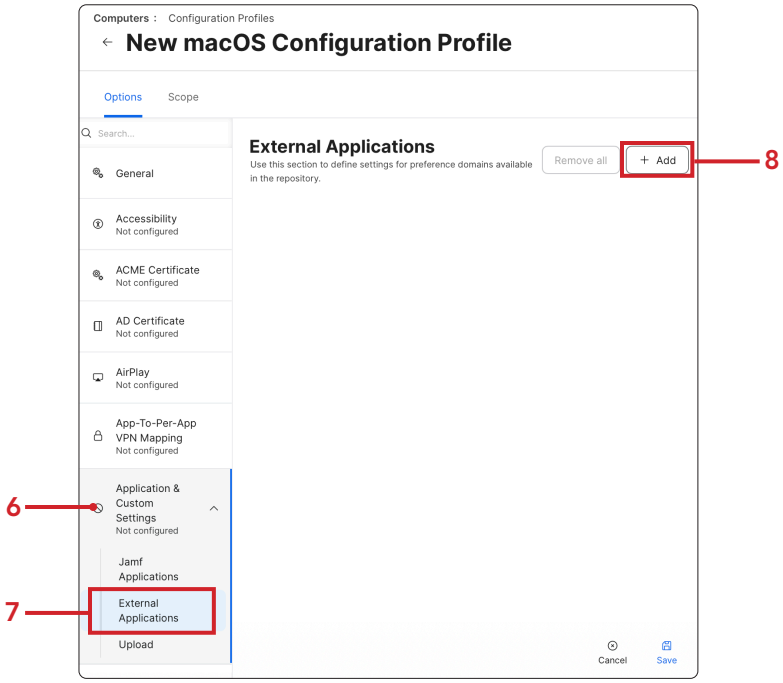
2. Click Computers.
3. Click Configuration Profiles.
4. Click New.



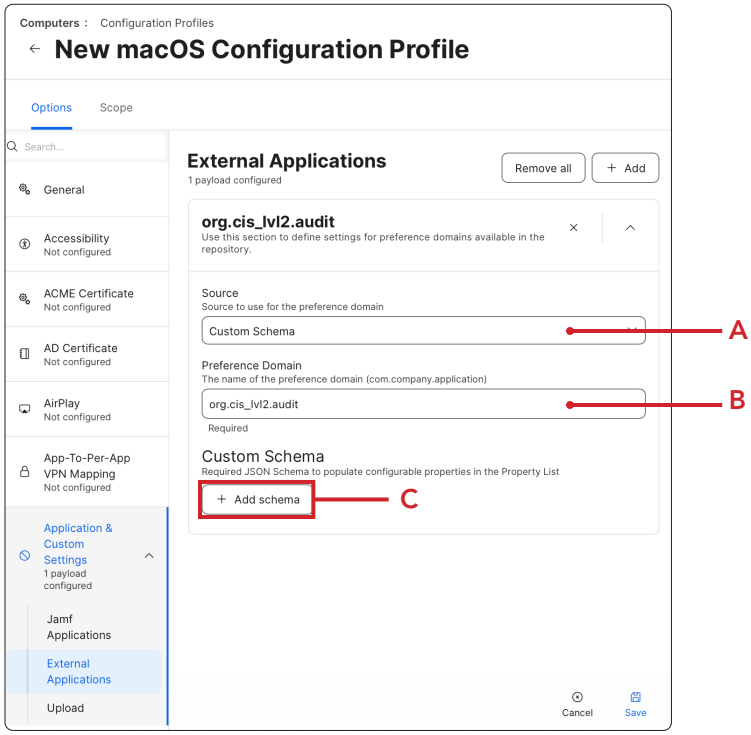
5. Configure the following:
    A. Select the General Payload.
    B. Enter **Sequoia_cis_lvl2_AirDrop_Exemption** for the Name.
    C. Select **Sequoia_cis_lvl2** for the Category.



6. Scroll down and select the Application & Custom Settings Payload.
7. Click External Applications.
8. Click Add (+).



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



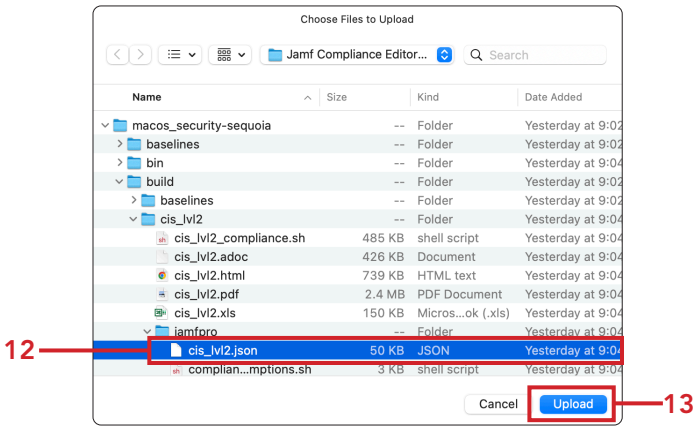
10. Click Upload.

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

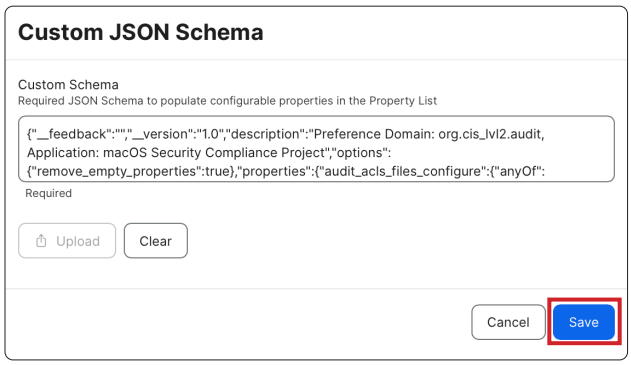
    NOTE: The **Jamf Compliance Editor - macOS Sequoia** folder was created on your Desktop in Section 2 of this guide.

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

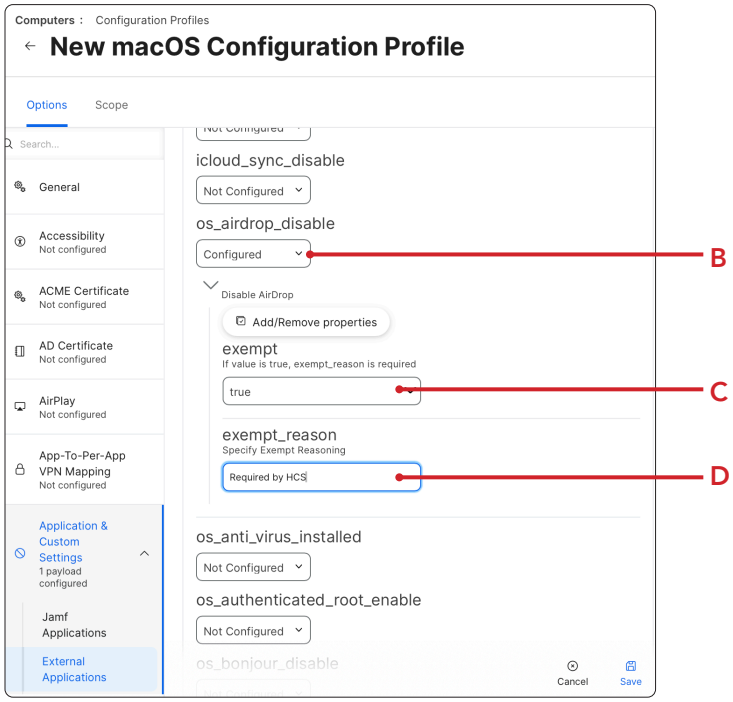
13. Click Upload.



14. Click Save.



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.**



16. Click Scope.
17. Scope to your needs. This guide will scope to All Computers.
18. Click Save.

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

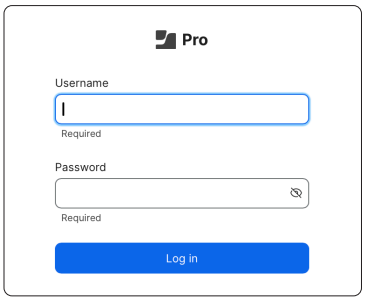
What You'll Need:
Learn what hardware, software, and information you'll need to complete the tutorials in this section.

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

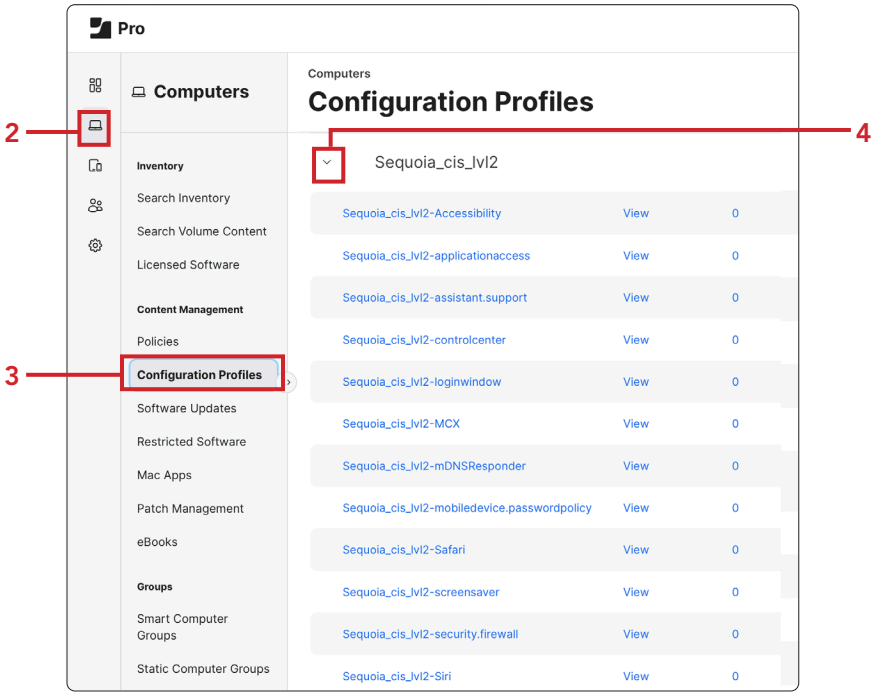
- A Jamf Pro server with administrative privileges

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.

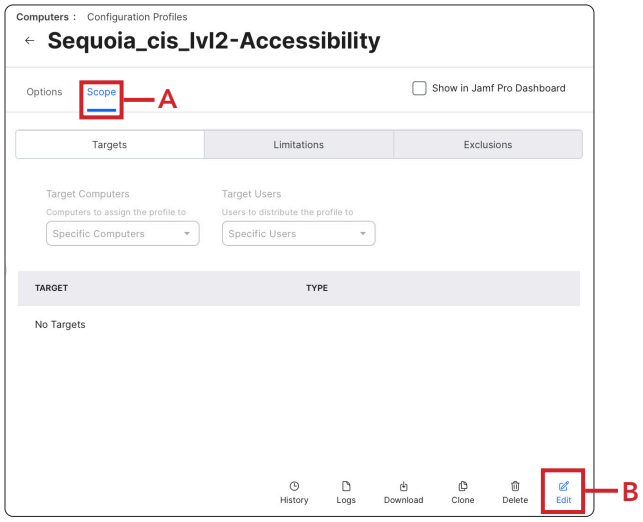
1. If necessary, Log into your Jamf Pro Server with administrative privileges.



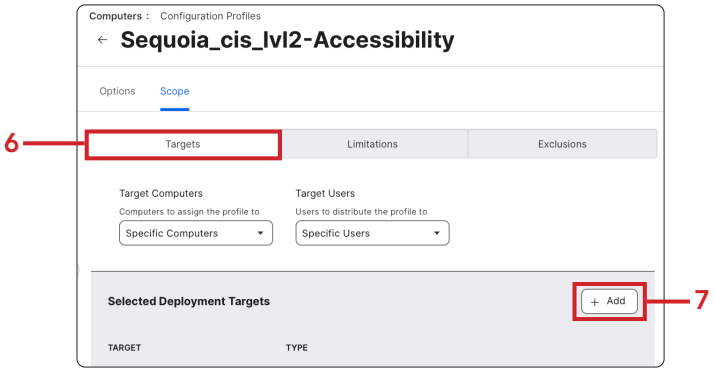
2. Click Computers.
3. Click Configuration Profiles.
4. Go to the Sequoia_cis_lvl2 category and expand the category to see all the computer configuration profiles that were created by the Jamf Compliance Editor application. Notice none of the computer configuration profiles are scoped. We need to scope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



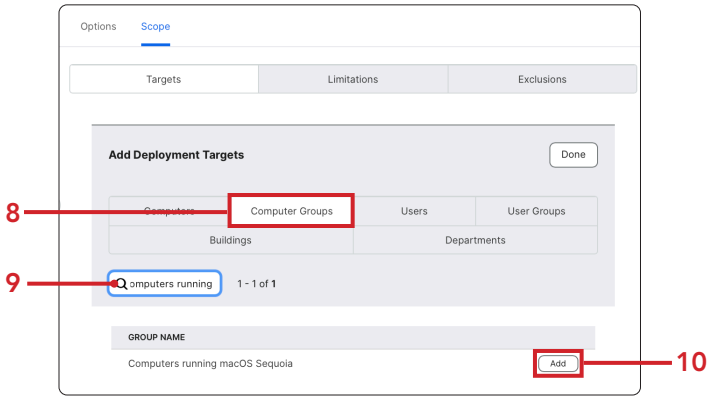
5. Select the first computer configuration profile in the list. Perform the following:
   A. Click Scope.
   B. Click Edit.



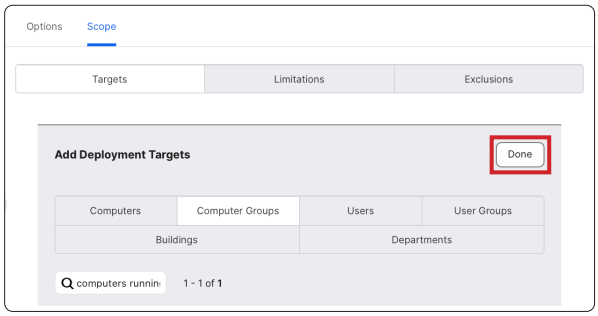
6. Click Targets.
7. Click Add.



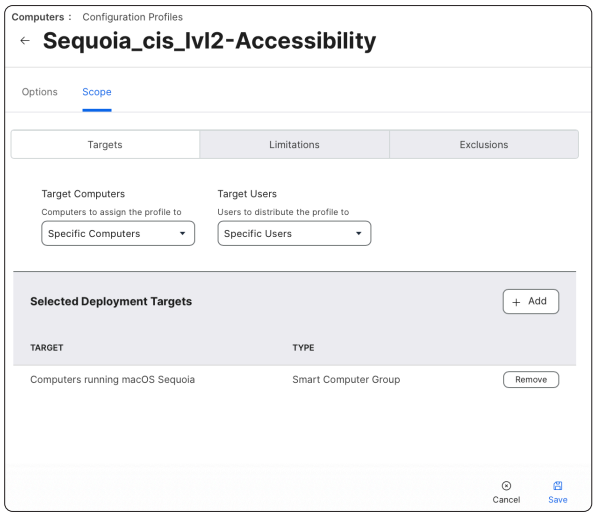
8. Click **Computer Groups**.
9. In the search field, enter: **computers running.**
10. Click Add for the group named: **Computers running macOS Sequoia.**



11. Click Done.

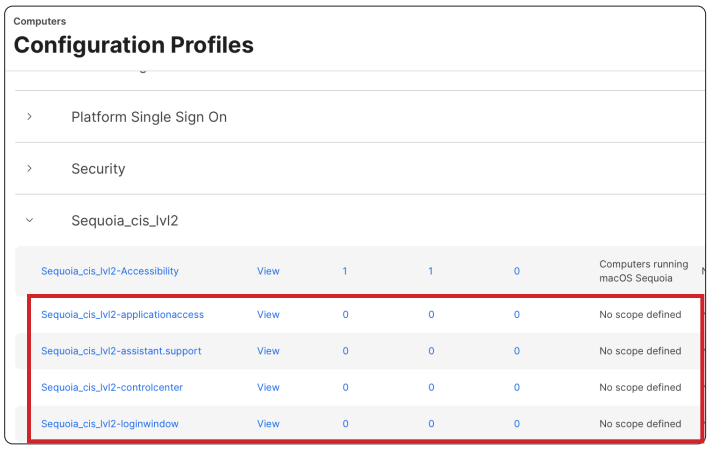


12. Click Save.



13. Click Previous (←).

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



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

Section 7: Creating an Advanced computer Search

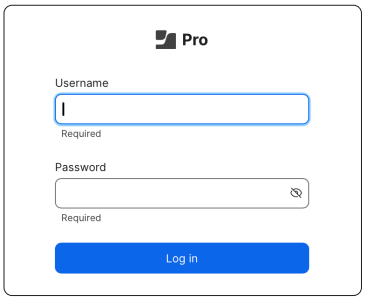
What You'll Need:
Learn what hardware, software, and information you'll need to complete the tutorials in this section.

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

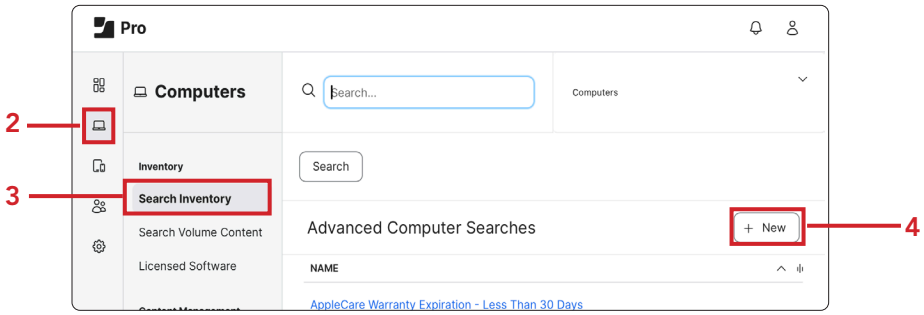
- A Jamf Pro server with administrative privileges

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

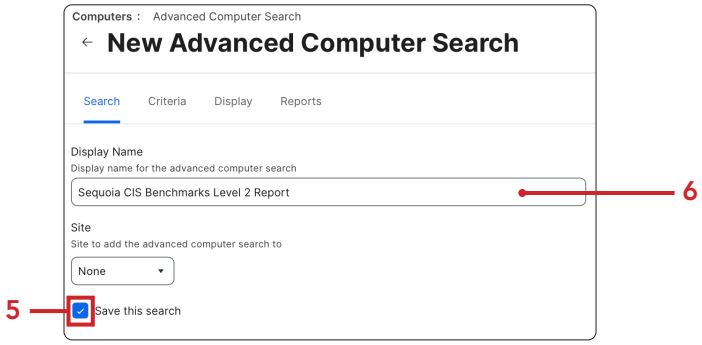
1. If necessary, Log into your Jamf Pro Server with administrative privileges.



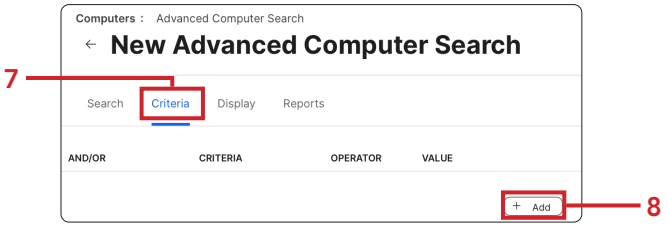
2. Click Computers.
3. Click Search Inventory.
4. Click New.



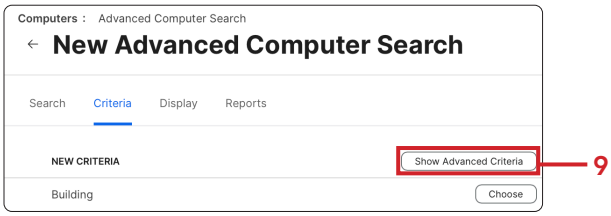
5. Select the checkbox for Save this search.
6. Enter **Sequoia CIS Benchmarks Level 2** Report for the Display Name.



7. Click Criteria.
8. Click Add.

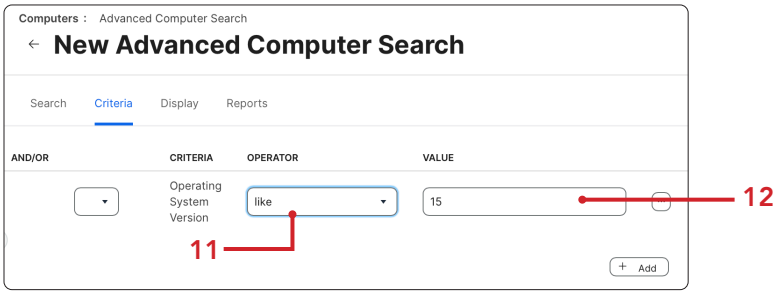


9. Click Show Advanced Criteria.

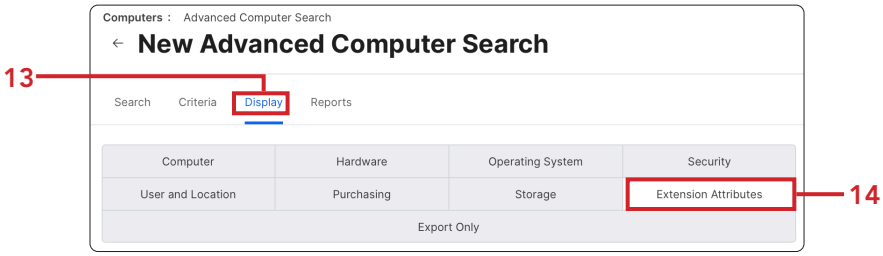


10. Find Operating System Version and click Choose.

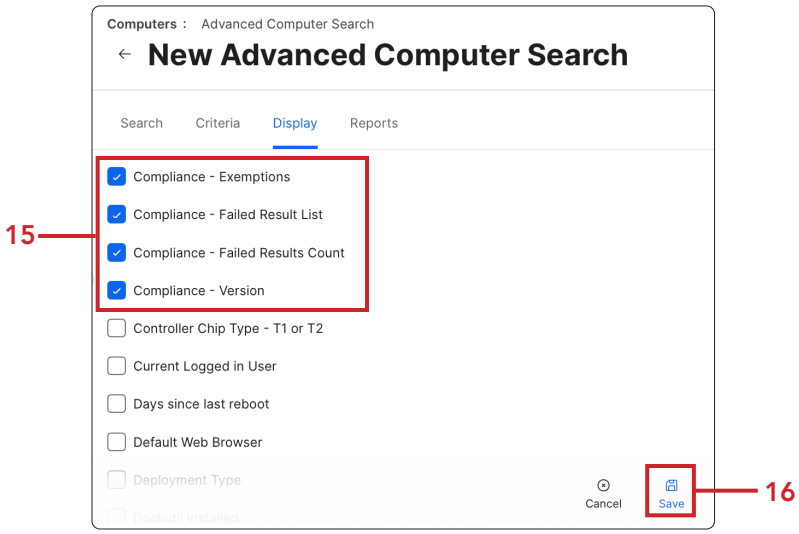
11. Select **like** for the Operator.
12. Enter **15** for the Value.



13. Click Display.
14. Click Extension Attributes.

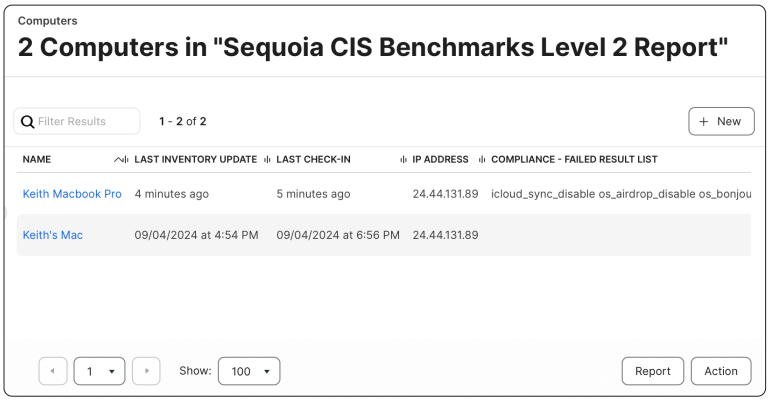


15. Select the following extension attributes:
    - Compliance - Exemptions
    - Compliance - Failed Result List
    - Compliance - Failed Results Count
    - Compliance - Version
16. Click Save



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.



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:

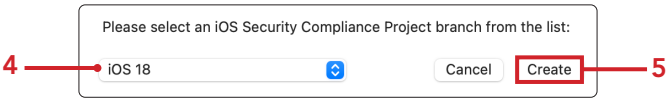
- Jamf Compliance Editor Application
- A Jamf Pro server with administrative privileges

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

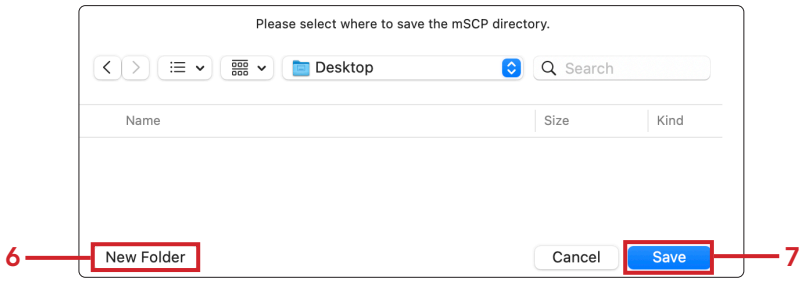
1. Open the Jamf Compliance Editor located in the Applications folder.

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

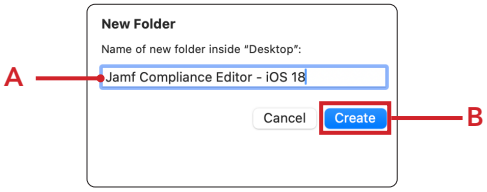
4. Select your iOS version. This guide will use iOS 18.
5. Click Create.



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

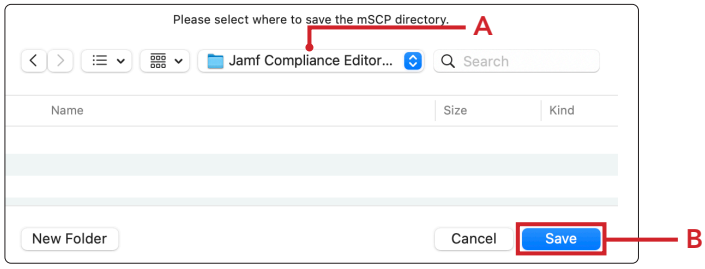


8. Configure the following:
   A. Folder name Jamf Compliance Editor - iOS 18 (Change iOS 18 to match whatever version you selected in step 3)
   B. Click Create



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

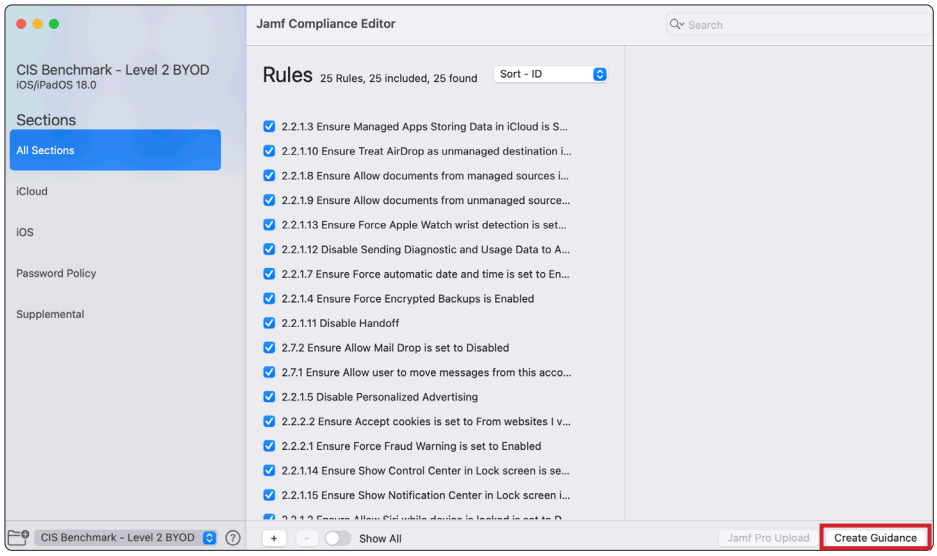
10. Click Save



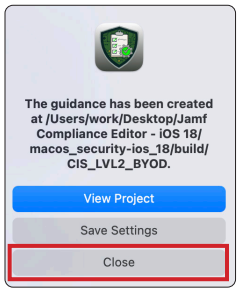
11. Select a Benchmark. This guide will select CIS Benchmark - Level 2 BYOD.

12. Click OK.

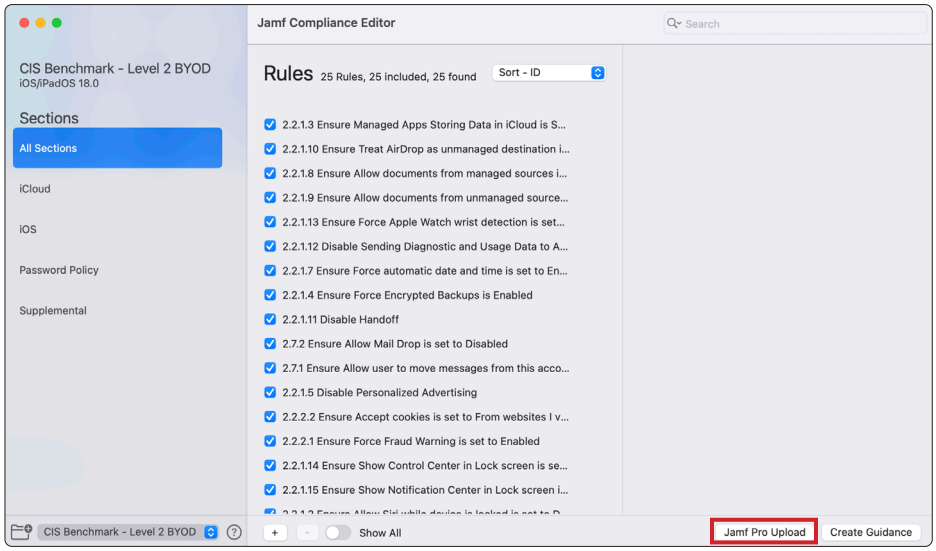
13. Click Create Guidance.



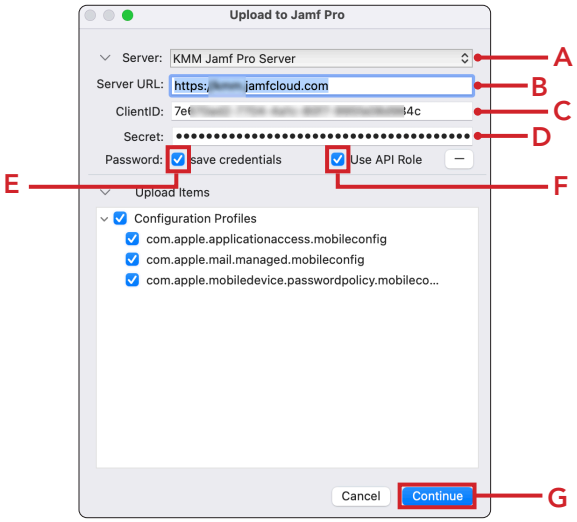
14. At the message below, click Close.



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.



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.



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

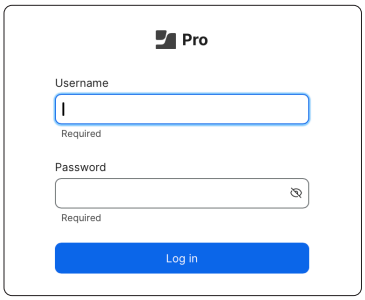
In this section we will create a Smart Device Group for iOS Devices using Account Driven Enrollment. We will use iPadOS 18.3 with CIS Benchmark Level 2 for Account Driven user enrollment as our example for this section. The process is the same for other versions of iOS/iPadOS/visionOS using different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

Remediation/Scripts for iOS/iPadOS/visionOS:

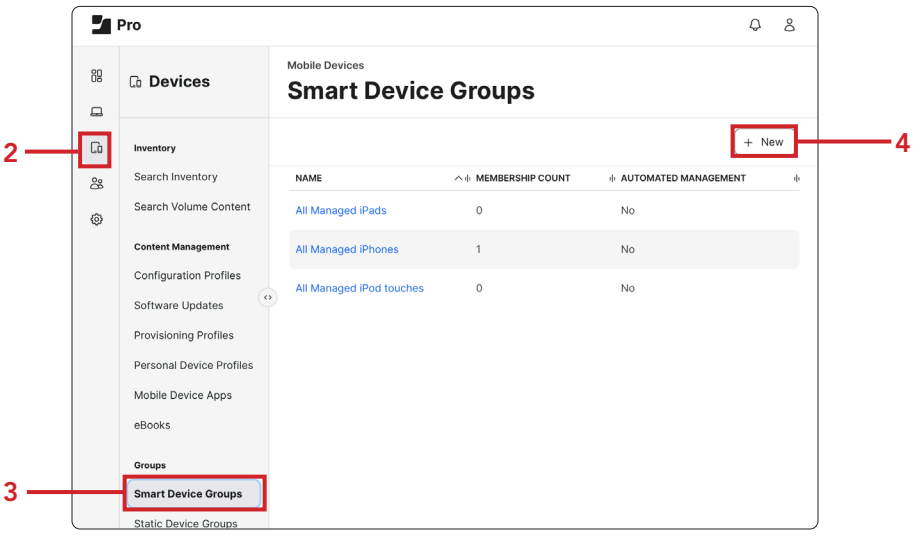
The ability to audit or remediate does not exist for iOS/iPadOS/visionOS. Once the configuration profile has been validated as deployed by the MDM server it is

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

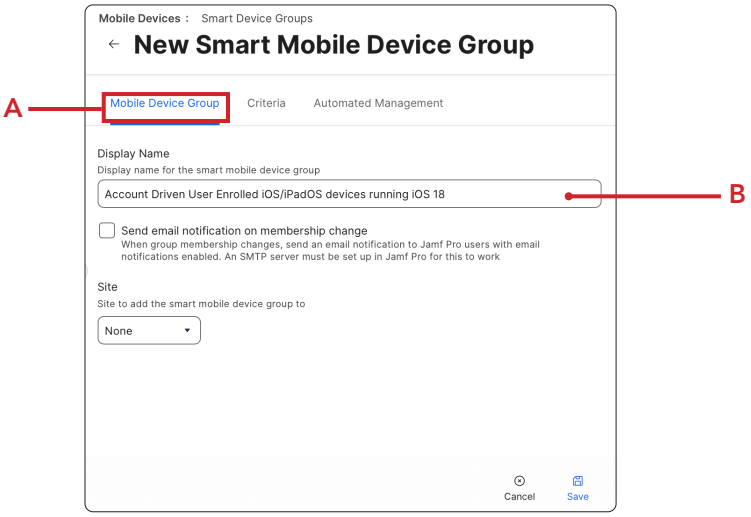
1. If necessary, Log into your Jamf Pro Server with administrative privileges.



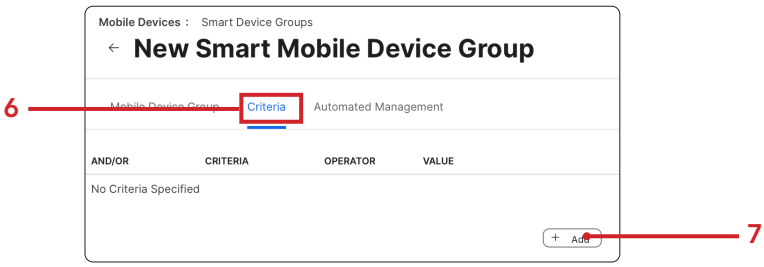
2. Click Devices.
3. Click Smart Device Groups.
4. Click New.



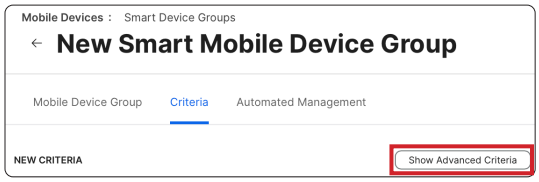
5. Configure the following:
   A. Click Mobile Device Group.
   B. Enter **Account Driven User Enrolled iOS/iPadOS devices running iOS 18** for the Display Name.



6. Click Criteria.
7. Click Add.

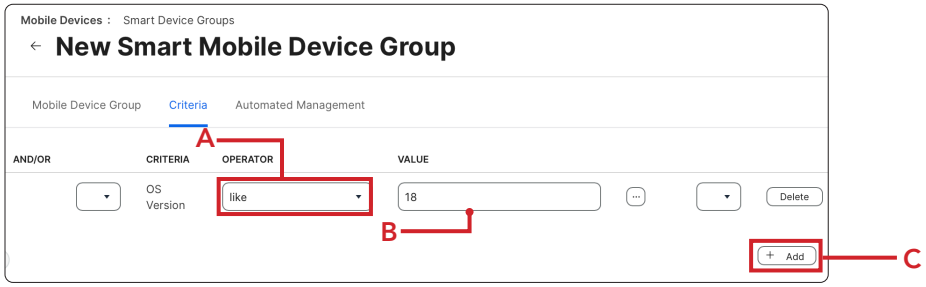


8. Click Show Advanced Criteria.

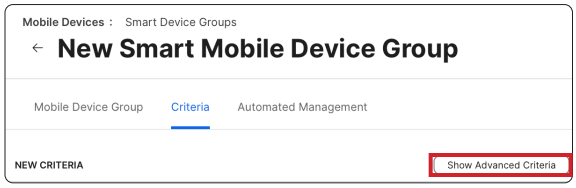


9. Scroll down to OS Version and click Choose.

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

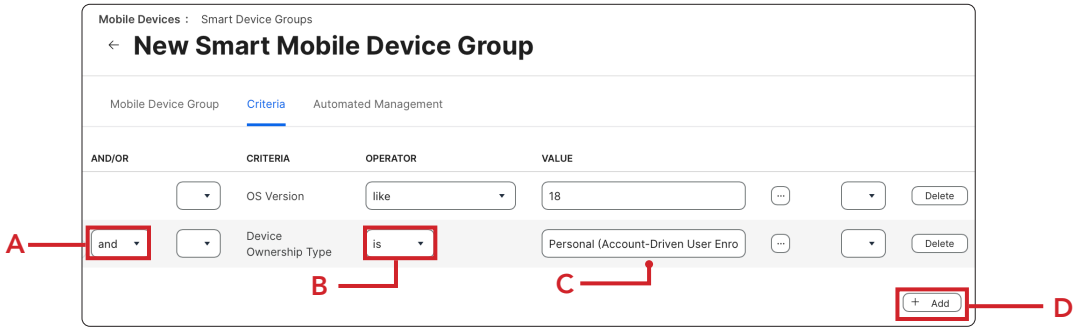


11. Click Show Advanced Criteria.

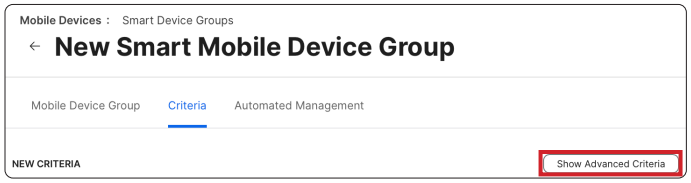


12. Select Device Ownership Type and click Choose.

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

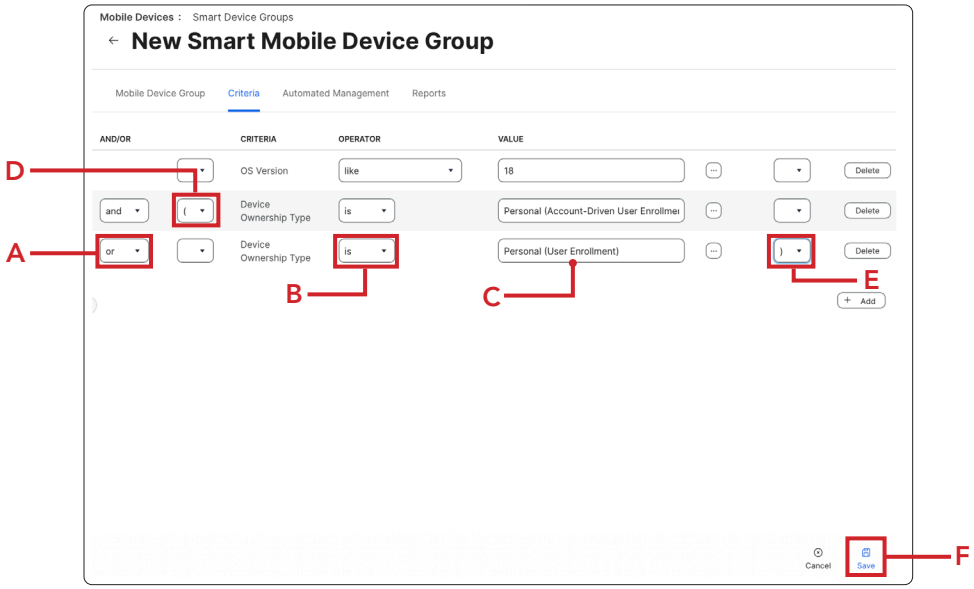


14. Click Show Advanced Criteria.



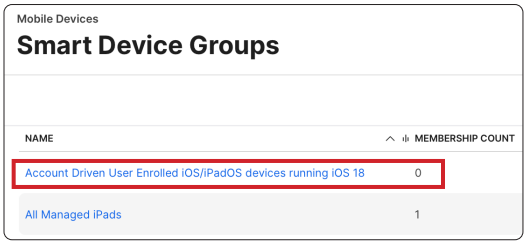
15. Select Device Ownership Type and click Choose.

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

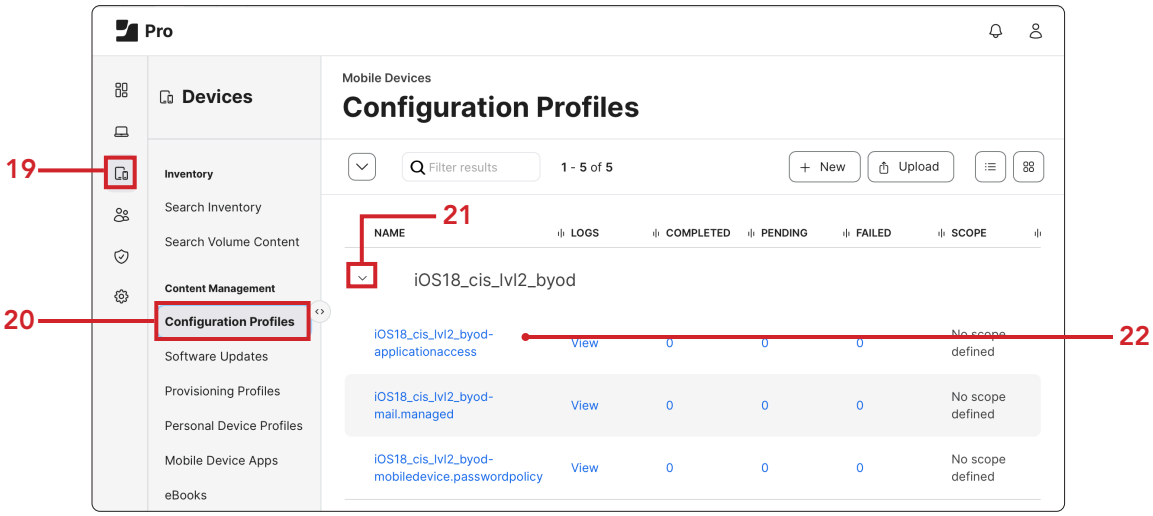


17. Click Previous (←).

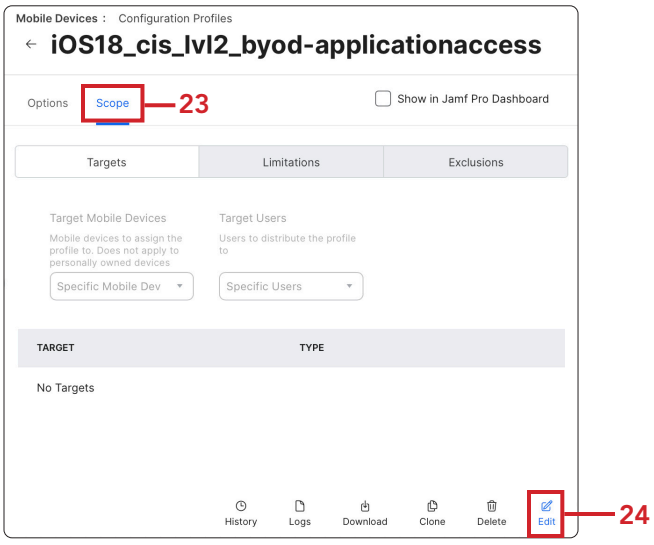
18. Confirm Account Driven User Enrolled iOS/iPadOS devices running iOS 18 is shown in the list.



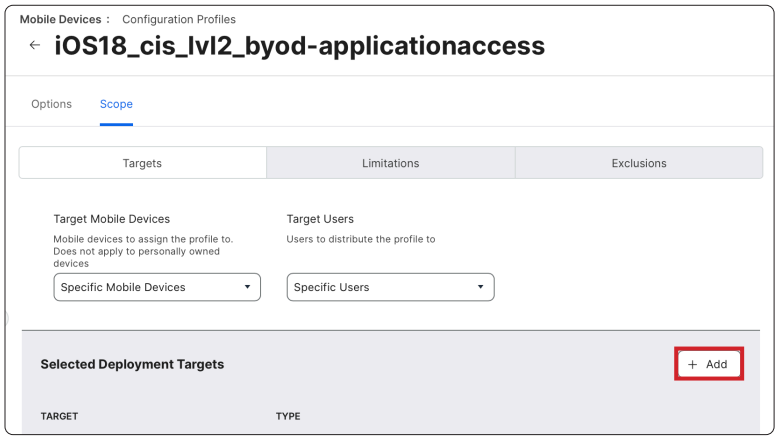
19. Click Devices.
20. Click Configuration Profiles.
21. Go to **iOS18_cis_lvl2_byod** category and expand the category to see all the computer configuration profiles that were created by the Jamf Compliance Editor app.
22. Select the first configuration profile in the list.



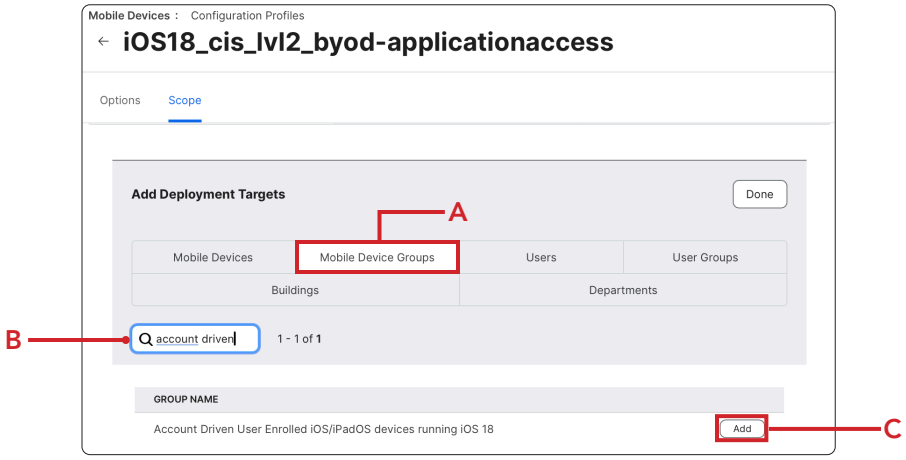
23. Select Scope.
24. Click Edit.



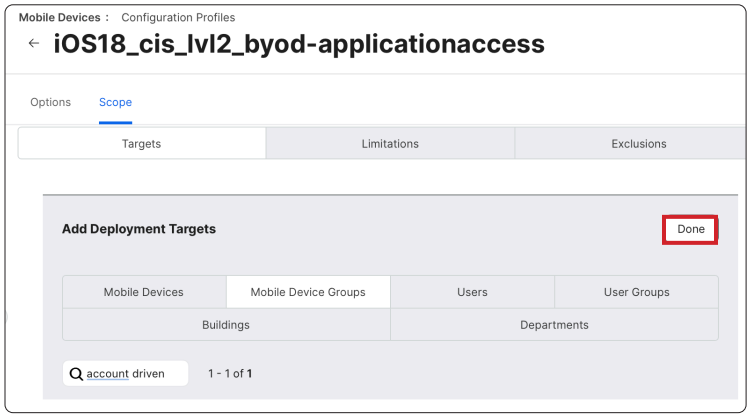
25. Click Add.



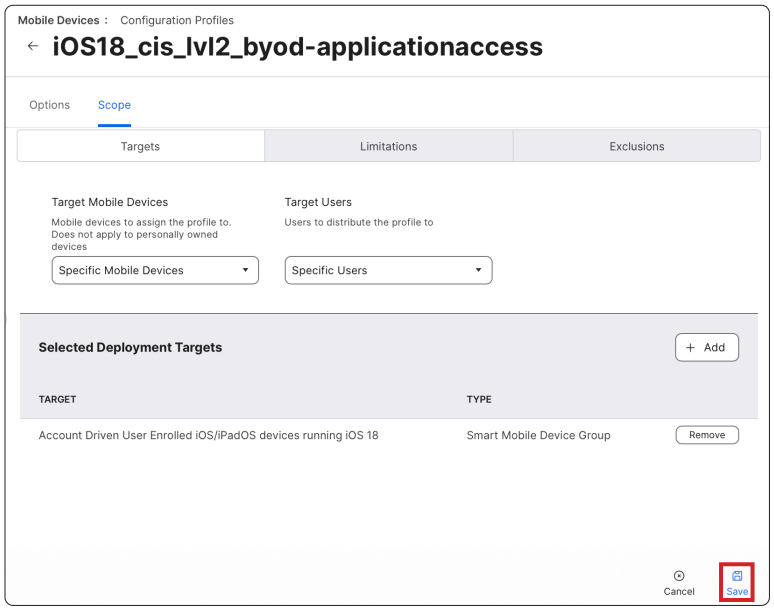
26. Perform the following:
    A. Select Mobile Device Groups
    B. In the search field enter: account driven
    C. Click add next to Account Driven User Enrolled iOS/iPadOS devices running iOS 18



27. Click Done.

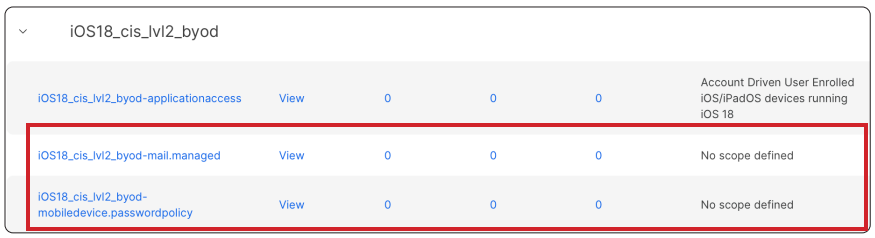


28. Click Save.



29. Click Previous (←).

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



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.

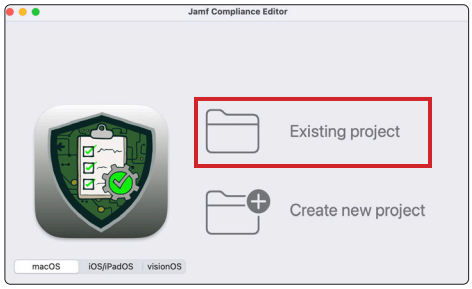
Hardware and Software
Requirements for following along with this section:

- 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.

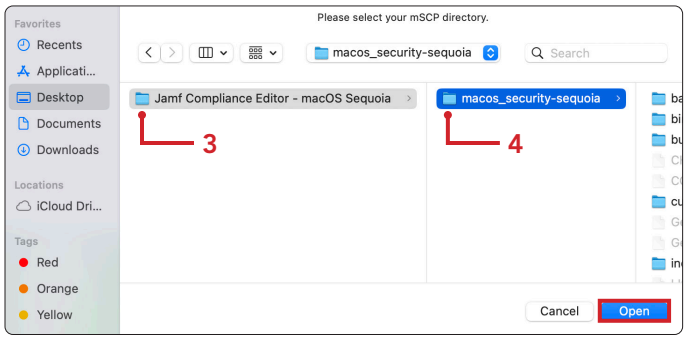
In this section, we use the Jamf Compliance Editor - macOS Sequoia project we created in section two of this guide using the CIS Benchmark - Level 2 to audit a local Mac computer.

1. If necessary, Open Jamf Compliance Editor.

2. Click Existing project.

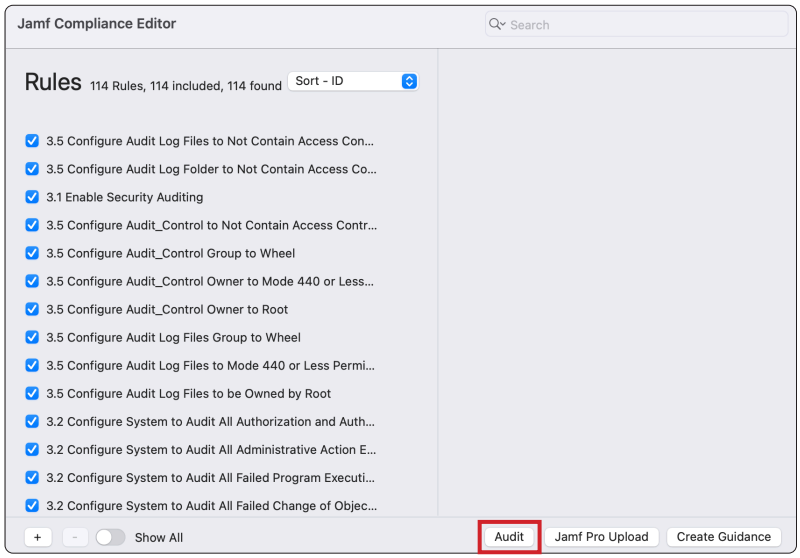


3. Select the Jamf Compliance Editor - macOS Sequoia folder located on your Desktop.
4. Select the macos_security-sequoia folder.
5. Click Open.

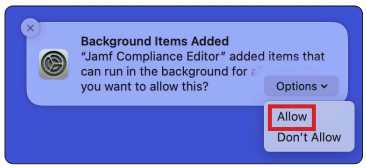


6. Select CIS Benchmark - Level 2.
7. Click OK.

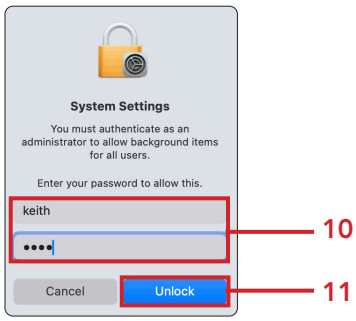
8. Click the Audit button.



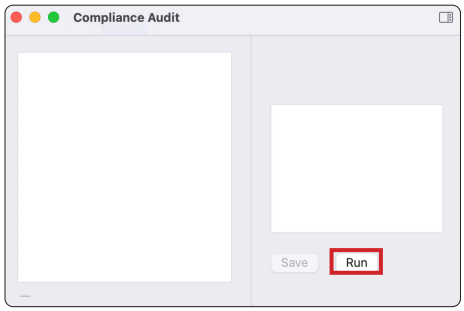
9. If prompted with the message below, select Allow.
   NOTE if you did not see notification, you can enable the background item for Jamf Compliance Editor here: System Settings > General > Login Items & Extensions > Allow in Background.



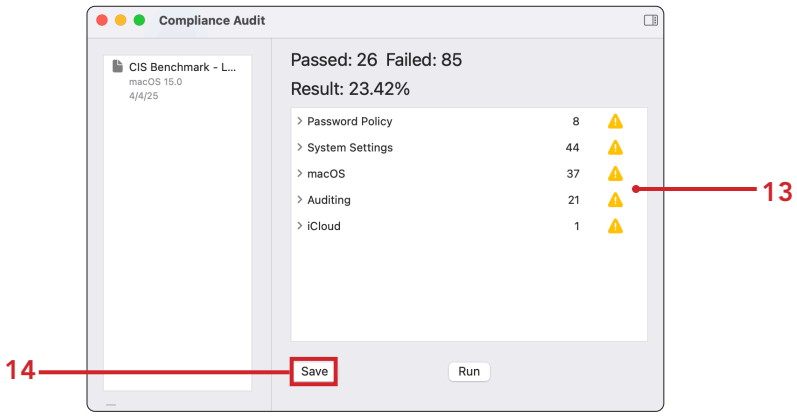
10. Enter your administrator credentials.
11. Click Unlock.



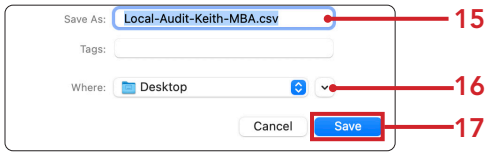
12. Click Run.



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.



15. Enter **Local-Audit-Keith-MBA.csv** (replace Keith with your name.)
16. Select Desktop as the destination.
17. Click Save



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:

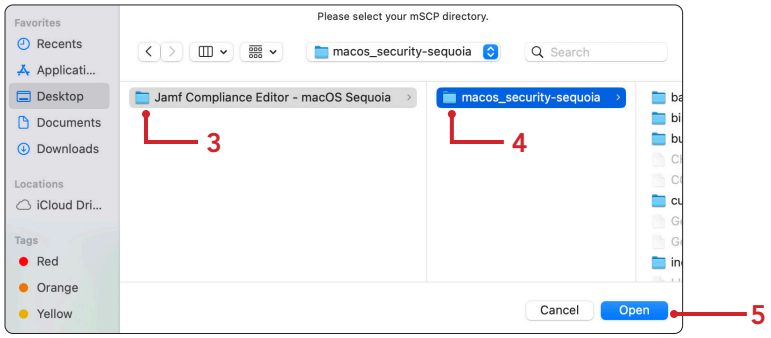
- A Mac computer with administrative privileges
- Jamf Compliance Editor Application
- The Jamf Compliance Editor - macOS Sequoia project we created in section two of this guide.

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.

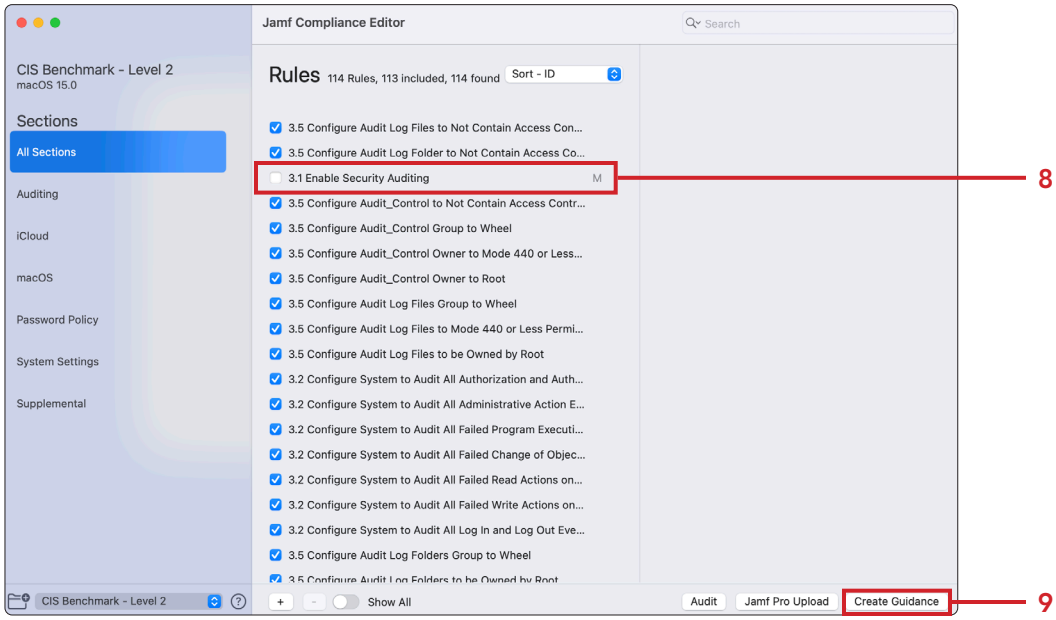
2. Select Existing project.

3. Select the Jamf Compliance Editor - macOS Sequoia folder located on your Desktop
4. Select the macos_security-sequoia folder
5. Click Open

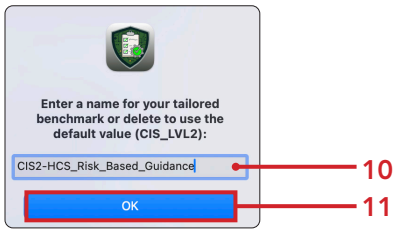


6. Select CIS Benchmark - Level 2.
7. Click OK.

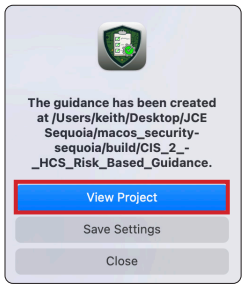
8. Deselect the checkbox for 3.1 Enable Security Auditing. Confirm an "M" to the right of 3.1 Enable Security Auditing. This means the baseline was modified
9. Click Create Guidance



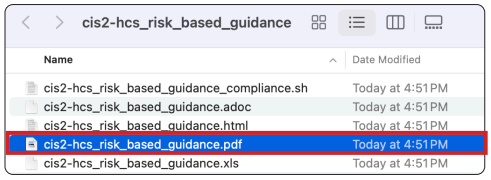
10. Enter a name for the benchmark. This guide will use **CIS2-HCS_Risk_Based_Guidance**. NOTE: If you use spaces, JCE will rename it with underscores and dashes.
11. Click OK.



12. Click View Project.

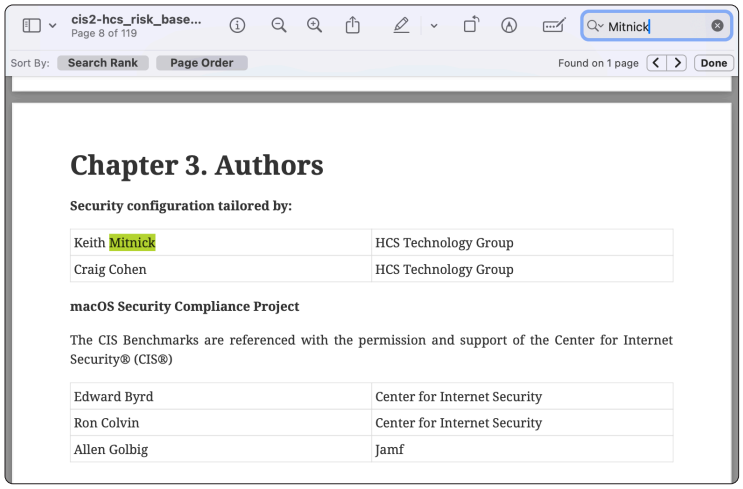


13. Open the file named cis2-hcs_risk_based_guidance.pdf. NOTE: You filename will be different.



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

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.



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:

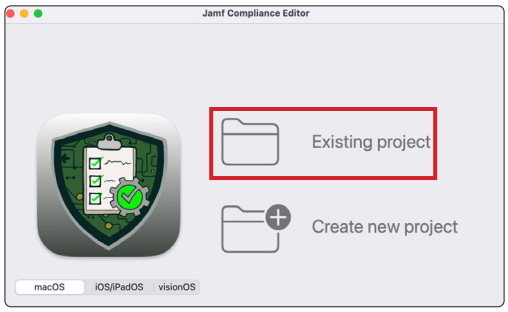
- A Mac computer with administrative privileges
- Jamf Compliance Editor Application
- The Jamf Compliance Editor - macOS Sequoia project we created in section two of this guide.

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.

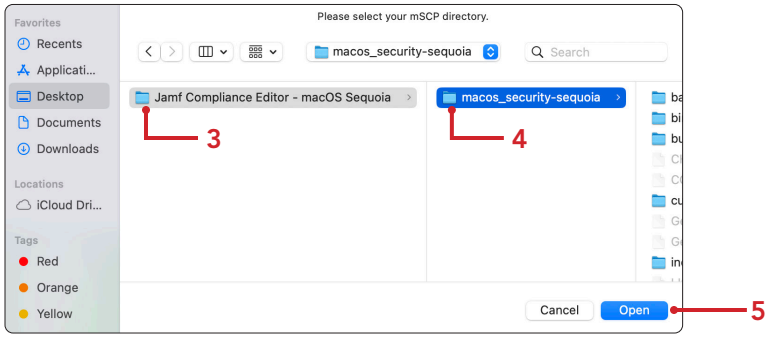
An Organizational Defined Value (ODV) in Jamf Compliance Editor is a customizable setting within a compliance baseline. Instead of using a fixed benchmark value, ODVs (typically shown as $ODV) allow organizations to define values that align with their internal security policies or operational needs.

1. If necessary, Open Jamf Compliance Editor.

2. Click Existing project.

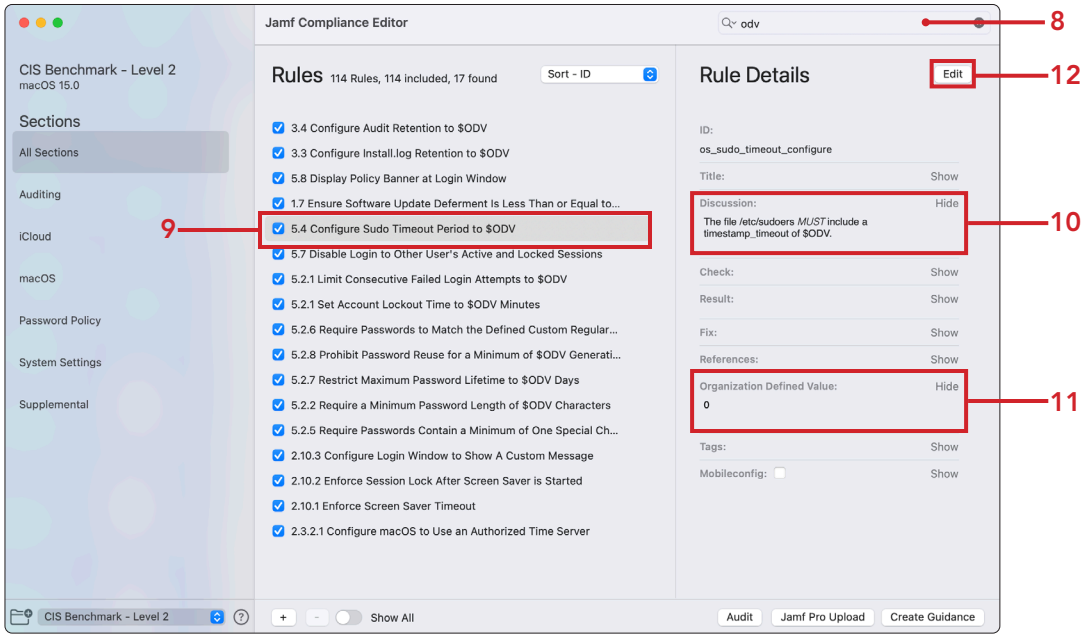


3. Select the Jamf Compliance Editor - macOS Sequoia folder located on your Desktop
4. Select the macos_security-sequoia folder
5. Click Open

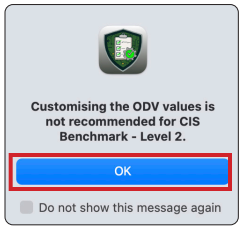


6. Select CIS Benchmark - Level 2.
7. Click OK.

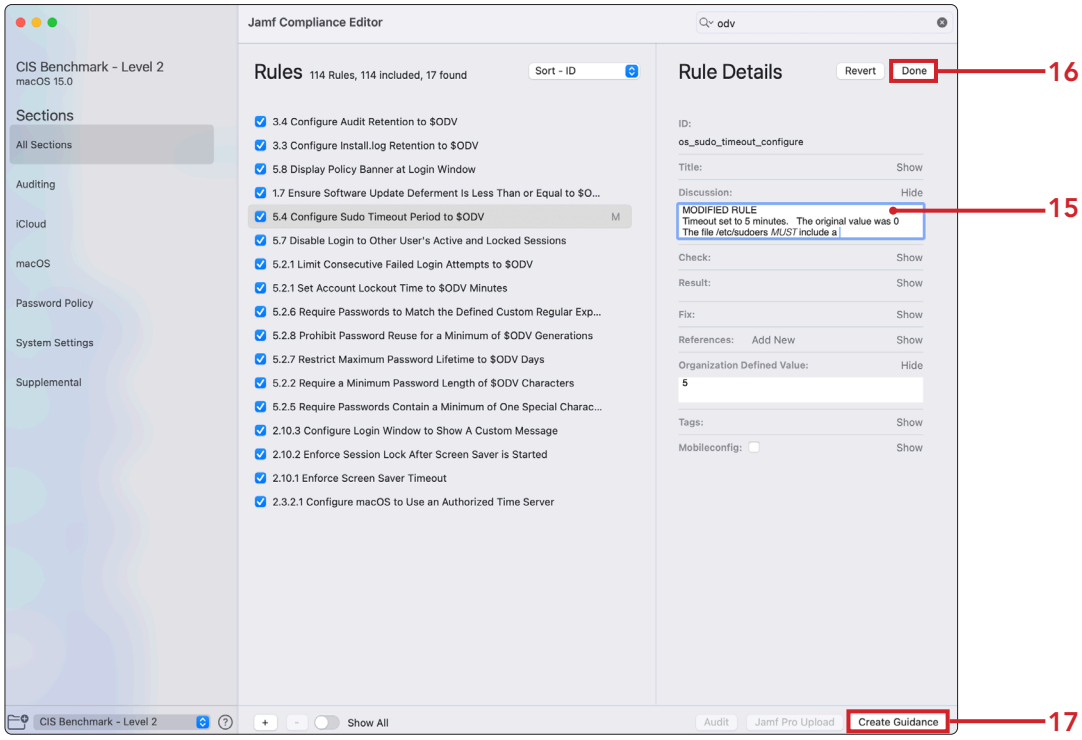
8. Enter **odv** in the search field
9. Select: 5.4 Configure Sudo Timeout Period to $ODV
10. In the Rule Details section, Click Show next to Discussion
11. In the Rule Details section, Click Show next to Organization Defined Value
12. In the Rule Details section, Click Edit



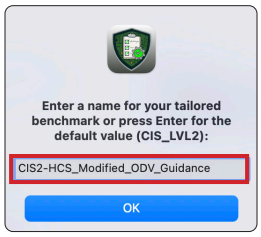
13. In the Rule Details section, change Organization Defined Value from 0 to 5.
14. Click OK.



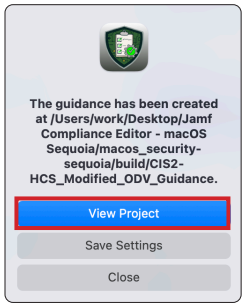
15. In the Rule Details section, Add the following to the top of the Discussion:
    MODIFIED RULE
    Timeout set to 5 minutes. The original value was 0
16. Click Done
17. Click Create Guidance



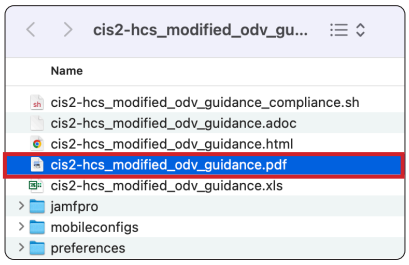
18. Enter a name for the benchmark. This guide will name it: CIS2-HCS_Modified_ODV_Guidance. If you use spaces, JCE will rename it with underscores and dashes.



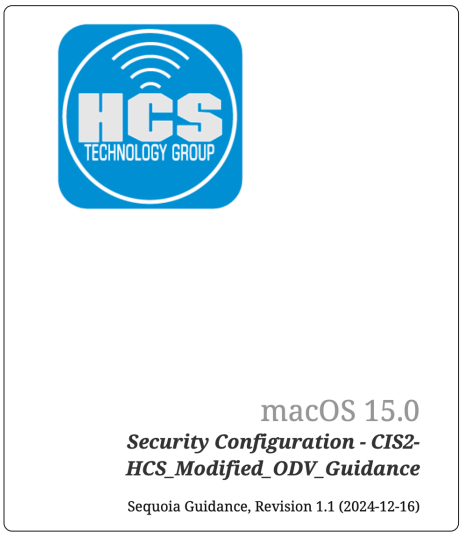
19. Click View Project.



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

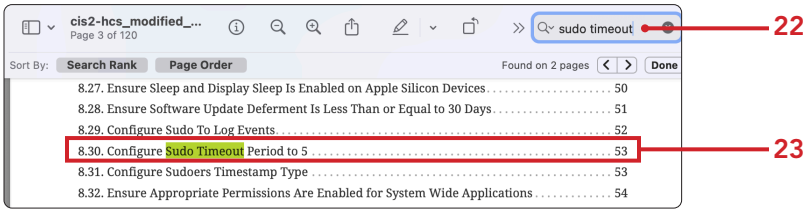


21. The report will have your organizations logo on the cover page.



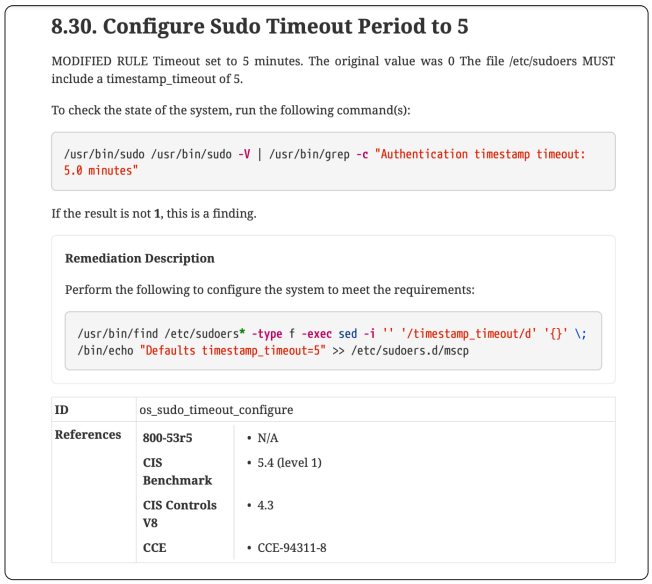
22. In the search field of the pdf, enter sudo timeout.

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.