



Configure Jamf Compliance Editor and Jamf Pro for Compliance Reporting



Contents

Preface	3
Section 1: Creating an API Role in Jamf Pro	5
Section 2: Configure the Jamf Compliance Editor Application	9
Section 3: Creating Smart Computer Groups	24
Section 4: Creating Policies	30
Section 5: Configure a JSON Schema	41
Section 6: Scoping the JCE Computer Configuration Profiles	47
Section 7: Creating an Advanced computer Search	50
Section 8: Creating a Jamf Compliance Editor CIS Level 2 Baseline for iOS	53
Section 9: Creating a Smart Device Group for iOS Devices using Account Driven Enrollment	57
Section 10: Run a local Mac Computer Audit	64
Section 11: Risk based benchmarks and reports	68
Section 12: Auditor Reports with Organization Defined Values	72



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

- 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. <u>https://github.com/usnistgov/macos_security/wiki</u>
- 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/securecontrolsframework/releases

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

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.

Username		
1		
Required		
Password		
		8
Required		
	Log in	

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

	Pro Pro			Q 8
	🔂 Dashboard		Settings	
	🖵 Computers	>	-	
	Devices	>	API Clear 3	Display icons
	& Users	>		
2 —	③ Settings		All System Global Jamfapps Self Service Server Network Computer management	Device management
			System 1 result found for "API"	
			API roles and clients	
			Configure access for API clients and define permission sets	

5. Click New.

Pro		\$ \$
윊 Dashboard	settings: System ← API roles and clients	+ New
🖵 Computers	>	
Devices	API Roles API Clients	
	Q Search filterable columns \leftarrow 1 \rightarrow 1-1 of 1	۵,



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 (\leftarrow).

Pro Pro	Q 8	
☐ Dashboard D	Settings : System > API roles and clients	
🕼 Devices >	Display name Display name for the API Role.	
🖧 Users >	Jamf Compliance Editor	——A
Settings	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	В
	Create iOS Configuration Profiles X Read iOS Configuration Profiles X Update iOS Configuration Profiles X Scripts	
	Create Scripts Delete Scripts Update Scripts Update Scripts	Tip: As you are entering a name of a Privliege, select the ones you need from the menu below.
	②	c

- 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.

Settinas : System
 API roles and clients
Display name Display name for the API Olient
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 4c
Generate client secret
Enable/disable API client
Enabled

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.

▲ 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)84c
Client secret:
n- 26CK /AFvcC
Copy client credentials to clipboard Close

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 disabiling the client does not end the lifetime of an active token.
60
Client ID
7∈ 1984c
Client secret

Rotate 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 <u>https://concepts.jamf.com</u>.
- 2. Scroll down to the Security, Compliance and Observability section and click Download under Compliance Editor.

Security, Compliar	nce and Observabil	ity
	Provide the second seco	Aftermath
Compliance Editor	Jamf Protect Detections	Aftermath
Jamf's implementation of the macOS Security Compliance project macOS	A repository of device monitoring modules for Jamf Protect Open Source Resources	macOS security incident response Open Source macOS Info Download

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.

Product Y Solutions Y Resources Y Open Source Y Enterprise Y Pricing	Search or jump to	Sign in Sign up
Jamf-Concepts / jamf-compliance-editor	A Notification	ns 및 Fork 0 ☆ Star 30
> Code 💿 Issues 🔹 📫 Pull requests 💿 Actions 🎛 Projects 🛈 Security 🗠 Insights		
eleases / v1.4		
Jamf Compliance Editor v1.4.0		Compare 👻
👹 macnotes released this Sep 16, 2024 🛇 v1.4 🗢 76298be 🥝		
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	s at the time of release.	
▼ Assets ₃		
	45.8 MB	Sep 16, 2024
]]Source code (zip)		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.



- 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.

G →	Pre	ferences	
	Authors		
в —	Keith Mitnick	HCS Technology Group	– C
	Craig Cohen	HCS Technology Group	
	Custom Banner	+ -	— A,D
Е	HĈS TECHNOLOSY GROUP	F 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.





- 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.

	New Folder Name of new folder inside "Desktop":	
15—	amf Compliance Editor - macOS Sequoia	
	Cancel	—— 16

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

Please select where to sav	te the mSCP directory. 1	7	
Name	Size	Kind	
	r		
New Folder	Cancel	Save	

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

	Please select a Sec	curity Benchma	ark from the list:	
19—	CIS Benchmark - Level 2	\bigcirc	Cancel	<u> </u>



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

< > cis_lvl2	:≡ ≎
Name	^
is_icis_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.



- 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.

•••	Jamf Compliance Editor	Q~ Search	
CIS Benchmark - Level 2 macOS 15.0	Rules 114 Rules, 113 included, 114 found	Rule Details	idit
Sections	3.5 Configure Audit Log Files to Not Contain Access Control Lists	ID:	
All Sections	3.5 Configure Audit Log Folder to Not Contain Access Control Lists	audit_auditd_enabled	
	3.1 Enable Security Auditing	Title: Che	
Auditing	3.5 Configure Audit_Control to Not Contain Access Control Lists	Discussion: Sho	w
iCloud	✓ 3.5 Configure Audit_Control Group to Wheel	Check: Sho	w
	3.5 Configure Audit_Control Owner to Mode 440 or Less Permissive	Result: Sho	w
macOS	✓ 3.5 Configure Audit_Control Owner to Root	Fix: Sho	
	3.5 Configure Audit Log Files Group to Wheel		
Password Policy	✓ 3.5 Configure Audit Log Files to Mode 440 or Less Permissive		
System Settings	3.5 Configure Audit Log Files to be Owned by Root	iags: Sno	
	3.2 Configure System to Audit All Authorization and Authentication Events	Mobileconfig: Sho	/W
Supplemental	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		
CIS Benchmark - Level 2 📀 🧿	+ - Show All	Audit Jamf Pro Upload Create Guid	dance

34.In the search field, enter Enforce Session.

35.In the Rule Details section, click Edit.

36. Click Show for Organization Defined Value.

•••	Jamf Compliance Editor		Q~ Enforce Session		
CIS Benchmark - Level 2 macOS 15.0	Rules 114 Rules, 114 included, 1 found	Sort - ID	Rule Details	Edit	
All Sections All Sections Auditing iCloud macOS Password Policy System Settings Supplemental	2.10.2 Enforce Session Lock After Screen Saver is Started		ID: system_settings_screensaver_ask_for_pr Title: Discussion: Check: Result: Fix: References: Organization Defined Value: Tags: Mobileconfig: ♥	assword_delay Show Show Show Show Show Show Show	36
CIS Benchmark - Level 2 ; ၇	+ - 🔵 Show All		Audit Jamf Pro Upload	Create Guidance	



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

•••	Jamf Compliance Editor	Q~ Enforce Session	٥
CIS Benchmark - Level 2 macOS 15.0	Rules 114 Rules, 114 included, 1 found Sort - ID C	Rule Details	t Done
Sections	✓ 2.10.2 Enforce Session Lock After Screen Saver is Started M	ID:	
All Sections		system_settings_screensaver_ask_for_pass	word_delay
		Title:	Show
Auditing		Discussion:	Show
iCloud		Check:	Show
		Result:	Show
macOS		Fix:	Show
Password Policy		References: Add New	Show
		Organization Defined Value:	Hide
System Settings		10	
Supplemental		Tags:	Show
		Mobileconfig: 🗹	Show
- CIS Benchmark - Level 2	3 + - Show All	Audit Lamf Pro Unload	ate Guidance

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.

•••	Jamf Compliance Editor	Q~ Enforce Session	• 42
CIS Benchmark - Level 2 macOS 15.0	Rules 114 Rules, 114 included, 1 found Sort - ID 3	Rule Details	Done 41
Sections	2.10.2 Enforce Session Lock After Screen Saver is Started M	ID:	
All Sections		system_settings_screensaver_ask_for_password	_delay
Auditing	<u>39</u>	Title:	Show
Auditing		Discussion:	show
iCloud		Check:	show
		Result:	show
macOS		Fix:	Show
Password Policy		References: Add New	Show
Custom Cattings		Organization Defined Value:	Hide
System Settings		-	40
Supplemental		Tags:	Show
		Mobileconfig: 🗹	Show
CIS Benchmark - Level 2	(?) + - Show All	Audit Jamf Pro Upload Create G	uidance

43.Click File.

Jamf Compliance Editor	File Edit View	Rules
	New	ЖN
•••	Open	жо
	Open Project Folder	20
CIS Benchmark - Level 2 macOS 15.0	Close	ж W

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	<u> </u>
Tags:		
Where:	🚞 macos_security-sequoia (🗸	
4	6 Cancel Save	47



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



49.Click Jamf Pro Upload.

•••	Jamf Compliance Editor	Qr Search
CIS Benchmark - Level 2 macOS 15.0	Rules 114 Rules, 114 included, 114 found Sort - ID	
Sections	3.5 Configure Audit Log Files to Not Contain Access Cont	
All Sections	3.5 Configure Audit Log Folder to Not Contain Access Co	
	✓ 3.1 Enable Security Auditing	
Auditing	✓ 3.5 Configure Audit_Control to Not Contain Access Contr	
iCloud	✓ 3.5 Configure Audit_Control Group to Wheel	
	✓ 3.5 Configure Audit_Control Owner to Mode 440 or Less	
macOS	✓ 3.5 Configure Audit_Control Owner to Root	
Descurred Dellars	✓ 3.5 Configure Audit Log Files Group to Wheel	
Password Policy	✓ 3.5 Configure Audit Log Files to Mode 440 or Less Permi	
System Settings	✓ 3.5 Configure Audit Log Files to be Owned by Root	
	3.2 Configure System to Audit All Authorization and Auth	
Supplemental	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	
CIS Benchmark - Level 2 📀 🤅	+ - Show All	Audit Jamf Pro Upload Create Guidance



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.

🖌 Pro	
Username	
	۴~
Required	
Password	
	Ø
Required	



- 53.Select Settings.
- 54. Enter categories in the search field.

55.Click Categories.

	Pro Pro			\$ &
	🗄 Dashboard		Settings	
	📮 Computers	>	-	
	Devices	>	Categories <u>Ciecci</u> 54	Display icons
	🖧 Users	>		
53—	Settings		All System Global Jamfapps Self Service Server Network Computer management Device management	User management Inform
			Global 1 result found for "Categories"	
			Categories	
		a	Organize components in Jamf Pro and - 55	

- 56.Confirm a category named Sequoia_cis_lvl2 was created.
- 57.Click Previous (\leftarrow).

57—	Settings : Global
	Maintenance
	Managed Items
	Managed Software Updates
56—	Sequoia_cis_lvi2

- 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 (←).

62——	Settings : Computer management						
	Q Search	← 1					
	NAME \uparrow						
	Compliance - Exemptions						
61	Compliance - Failed Result List						
	Compliance - Failed Results Count						
	Compliance - Version						

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 (\leftarrow).

66	Settings : Computer management			
	Q Search	\leftarrow	$1 \rightarrow$	
	NAME			
65 —	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.

	Pro						
67 —	88	Computers	Computers Configuration Profiles				
•••	Co Inventory		 Sequoia_cis_lvl2 			- 69	
	8	Search Inventory	Sequola_cis_IvI2-Accessibility	View	0		
	٢	Licensed Software	Sequoia_cis_IvI2-applicationaccess	View	0		
		Content Management	Sequoia_cis_lvl2-assistant.support	View	0		
		Policies	Sequoia_cis_lvl2-controlcenter	View	0		
68 —		Configuration Profiles	Sequoia_cis_lvl2-loginwindow	View	0		
		Software Updates	Sequoia_cis_lvl2-MCX	View	0		
		Mac Apps	Sequoia_cis_lvl2-mDNSResponder	View	0		
		Patch Management	Sequoia_cis_IvI2-mobiledevice.passwordpolicy	View	0		
		eBooks	Sequola_cis_IvI2-Safari	View	0		
		Groups	Sequoia_cis_lvl2-screensaver	View	0		
		Smart Computer Groups	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.

Ucornamo	
I	
Required	
Password	
	8
Required	

- 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.

computers : Smart ← New S	Computer Groups mart Comput	er Group
Computer Group	Criteria	
Display Name Display name for the sma	art computer group	_
Computers running r	nacOS Sequoia	
Send email notific When group member SMTP server must I	cation on membership change ership changes, send an email notif se set up in Jamf Pro for this to wo	ication to Jamf Pro users with email notifications enabled. An 'k
Site		
Site to add the smart co	mputer group to	
None		



6. Click Criteria.

7. Click Add (+).

Computers : Smart Computer Groups					
Computer Group	Criteria	6			
AND/OR No Criteria Specified	CRITERIA	OPERATOR	VALUE		
				+ Add	

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

Operating System Version	Choose

9. Set the Operator to like.

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

11.Click Save.

ND/OR							
	CRITERIA	OPERATOR		VALUE			
•	Operating System Version	like	•	15		(···)	-10
	9	,			(+	Add	
					0	8	

12.Click Previous (←).

Computers : Smart Computer Groups							
Computer Group	Criteria Reports	Show in Jamf Pro Dashboard					
AND/OR	CRITERIA OPERATOR	VALUE					
· ·	Operating System Version	•					

13.Click New (+).

Computers	
Smart Computer Groups	
	+ 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 Com	puter Group
Computer Group Criteria	
Display Name Display name for the smart computer group	
macOS_Sequoia_CIS_LVL2_Compliant	
Send email notification on membership cl When group membership changes, send an em	nange Iail 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	-15		
AND/OR	CRITERIA	OPERATOR	VALUE	
				(+ Add

17. Scroll down to Operating System and click Choose.

Operating System Version	Choose

18.Set the Operator to like.

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

20.Click Add (+).

Computers : Smart ← New S	Computer Groups	mputer G	Froup			
Computer Group	Criteria					
AND/OR	CRITERIA	OPERATOR		VALUE		
•	Operating System Version	like	•	15]•	19
		18—			+ Add	20

21. Click Show Advanced Criteria, if necessary.

computers : Smart ← New S	Computer Groups mart Computer Group	
Computer Group	Criteria	
NEW CRITERIA		Show Advanced Criteria



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

Compliance - Failed Results Count	Choose

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

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

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

26.Click Save.

Computer Group	Criteria			
AND/OR	CRITERIA	OPERATOR	VALUE	
•	Operating System Version	like •	m	Delete
and •	Compliance - Failed Results Count	is	0	• Delete
	24-		L25	(+ Add
				Cancel Save

27.Click Previous (\leftarrow).

Computers : Smart Computer Groups

28.Click New (+).

^{Computers} Smart Computer Groups	
	+ New



29. For the Display Name, enter: macOS_Sequoia_CIL_LVL2_NotCompliant.

computers : ← Ne	^{Smart} WS	Computer Gro mart C	ompu	iter Group
Computer G	roup	Criteria		
Display Name	r the sma	art computer aro	un	
macOS_Sequ	ioia_CIL.	_LVL2_NotCom	ipliant	
Send ema When grou	il notific p membe	ation on memb rship changes, s	pership chang end an email no	e otification to Jamf Pro users
Site				
Site to add the	mart cor	nputer group to		
None	•			

30.Click Criteria.

31.Click Add.

New S	Smart Con	nputer Gro	oup	
Computer Group	Criteria	 30		
AND/OR	CRITERIA	OPERATOR	VALUE	
No Criteria Specified				

32.Click Show Advanced Criteria.

computers : Smart ← New S	Computer Groups mart Computer Group	o
Computer Group	Criteria	
NEW CRITERIA		Show Advanced Criteria

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

Compliance - Failed Results Count	Choose



34.For the Operator, select more than.

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

36.Click Add.

Computer Group	Criteria			
AND/OR	CRITERIA	OPERATOR	VALUE	
•	Compliance - Failed Results Count	more than 🔹	0	•
	54			+ Add

37.Scroll down to Operating System and click Choose.

Operating System Version Choose

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

ND/OR	CRITERIA	OPERATOR	VALUE		
•	Compliance - Failed Results Count	more than 🔹	0		• Delete
and 🔹	Operating System Version	like	• 15		• Delete
	39-		L	— 40	(+ Add

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]	<pre>[cfc] [stats] [compliant] [non_compliant] [reset] [reset-all] [quiet=<value>]"</value></pre>
"Optional parame	eters:"	
"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	t :	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:< td=""><td></td><td>1 - show only failed and exempted checks in output"</td></value:<>		1 - show only failed and exempted checks in output"
		2 - show minimal output"
)		

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

		Pro		\$ &
1	88	□ Computers	Computers Policies	
•	G 88	Inventory Search Inventory	C Filter Policies 1 - 3 of 3	+ New := 88
	۲	Search Volume Content Licensed Software	NAME A 0 PREQUENCY 0 IROUGER 0 SCOPE	
2 —		Content Management Policies		



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.

÷	New Policy		
	Options Scope Self Service U	ser Interaction	
	a General	Configure Scripts	
4	Packages O Packages	Use this section to run scripts.	
C	Software Updates Not Configured		
L L	Scripts		

7. Find the sequoia_cis_lvl2_compliance.sh and click Add.

Add

Sequoia_cis_lvl2_compliance.sh Sequoia_cis_lvl2



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.

Comp ←	New Policies	су	
Opt	ions Scope S	Self Service User Interaction	
	Packages O Packages	Scripts	
(0)	Software Updates Not Configured	Sequoia_cis_lvl2_compliance.sh (x) (+) Priority	
	Scripts 1 Script	Priority to use for running the script in relation to other actions After ••••••••••••••••••••••••••••••••••••	—— A
8	Printers 0 Printers	Parameter Values Values for script parameters. Parameters 1-3 are predefined as mount point, computer name, and username	
0	Disk Encryption Not Configured	Parameter 4 check	— В
	Dock Items 0 Dock Items	Parameter 5	

9. Scroll down and click Maintenance.

10.Click Configure.

9

Comp ←	New Policies	cy	
	Inst Scope Oparus S Net Conflaured Scripts Scripts Printers Printers Printers Disk Encryption Net Conflaured Dock Items 0 Dock Ite	Self Service User Interaction	10

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 n	natch the computer name in Jamf Pro



12.Click Scope.

13. Confirm Specific Computers is selected for Target Computers.

14.Click Add.

	Computers : Policies ← New Policy			
4.0	Options Scope Self Service	User Interaction		-
12 —	Targets	Limitations	Exclusions	
13—	Target Computers Computers to deploy the policy to Expecific Computers	Target Users Users to deploy the policy to Specific Users •		
	Selected Deployment Targets	TVPE	+ Add	14
	No Targets	I YPE		

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.

Targets Limitations Exclusion:			
Add Deployment Targets	Targets	Limitations	Exc
Buildings Departments	Computers Buildings	Computer Groups	Users User Departments
Q omputers runnind 1 - 1 of 1		1	



16.Click Save.

Targets	Limitations	Exclusions
Target Computers	Target Users	
Computers to deploy the policy to	Users to deploy the policy to	
Specific Computers	Specific Users 🗸	
Selected Deployment Targets		+ Ac
Selected Deployment Targets	түре	+ Ac
Selected Deployment Targets TARGET Computers running macOS Sequola	TYPE Smart Computer Group	(+ Ac
Selected Deployment Targets TARGET Computers running macOS Sequola	TYPE Smart Computer Group	+ Ac

17.Click Previous (\leftarrow).

Computers : Policies

18.Click New (+).

Comput Poli	cies		
	Q Filter Policies	1 - 99 of 99	+ 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.

Scripts	
Sequoia_cis_lvl2_compliance.sh	× +
Priority	
Priority to use for running the script in relation to other actions	
Parameter Values	
Values for script parameters. Parameters 1–3 are predefined as mount point, co	omputer name, and username
Parameter 4	
cfc	•
Parameter 5	

24.Scroll down and select Maintenance.

25.Click Configure.

Options Scope Self Serv	User Interaction	
Not Configured		
Scripts 1 Script		
Printers 0 Printers		
Disk Encryption Not Configured		
Dock Items		
Local Accounts	Configu	re Maintenance
Accounts Not Configured	Use this section to computer names, in and run commo	vupdate inventory, reset stall all cached packages, n maintenance tasks.
Directory Bindings 0 Bindings	C	onfigure
EFI Password Not Configured		

26.Confirm the checkbox is selected for Update Inventory.

M	aintenance	×
	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.

	Limitations	Exclusions
Target Computers	Target Users	
Computers to deploy the policy to	Users to deploy the policy to	
Selected Deployment Targets	түре	+ Add
macOS_Sequoia_CIL_LVL2_NotComplian	t Smart Computer G	Group

33.Click Previous (\leftarrow).





34.Click New (+).

Computers Polici	es		
	Q 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	
Α	Ceneral Control Contro Control Control Control Control Control Control Con	General Display Name Display name for the policy Reset Baseline E tabled Site to add the policy to	— В
	O Scripts Printers O Printers	Kenne - Category Category to add the policy to Genuine is M2 -	
	Disk Encryption Not Configured Dock Items 0 Dock Items	Trigger Event(s) to use to initiate the policy Startup	C
	Local Accounts 0 Accounts Management Accounts Not Configured	When a computer starts up, a startup script that checks for policies must be configured in Jamf Pro for this to work Login Using a user logis in to a computer. A login event that checks for policies must be configured in Jamf Pro for this to Description Descript	
	Directory Bindings 0 Bindings	 Network State Change When a computer's network state changes (e.g., when the network connection changes, when the computer name changes, when the P address changes) 	
	EFI Password Not Configured	Initialitie Computer computer scheduler Immediately after a computer completes the enrollment process Recurring Chacken At the comprised chacken frequency configured in Lanf Bro	
D	Restart Options	Little recurring checken requercy configured in Jami Pro Sustom	
-	X Maintenance Not Configured	Custom Event Custom Event Custom Event Custom event to use to initiate the policy. For an iBeacon region change event, use "beaconStateChange"	
	Files and Processes Not Configured		— Е
	Microsoft Device Compliance Not Configured	Execution Frequency Frequency at which for run the policy Origing	— F

- 36.Click Scripts.
- 37.Click Configure.





38. Find the sequoia_cis_lvl2_compliance.sh and click Add.

Sequ	uoia_cis_lvl2_c	compliance.sh	Sequoia_cis_lvl2	Add
P.Con A. B. C.	figure the Priority: A Paramete Paramete	following: fter. r 4: check . r 5: reset .		
Compr ←	uters : Policies New Polic	Y If Service User Interaction		
	Packages 0 Packages	Scripts		
(@)	Software Updates Not Configured	Sequoia_cis_IvI2_compliance.sh Priority Priority to use for running the script in relation to other act	(x) (+)	
	Scripts 1 Script A-	After Parameter Values		
0	0 Printers Disk Encryption Not Configured	Values for script parameters. Parameters 1–3 are predefine Parameter 4check	ed as mount point, computer name, and username	E
-	Dock Items 0 Dock Items	Parameter 5		(

- 40. Click Maintenance.
- 41.Click Configure.





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 N Change the comput	lames rr name on computers to match the computer name in .	lamf 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.

1	Computers : Policies	
	 New Policy 	
_	Scope Self Service User Interaction	
	Targets Limitations	Exclusions
	Target Computers Target Users Computers to deploy the policy Users to deploy the policy to to All Computers • Specific Users •	
	Selected Deployment Targets	+ Add
	No Targets	
		© (⊟ Cancel Save

46.Click Previous (←).



47.Go to the Sequoia_cis_lvl2 category.

Expand the	^d 48.Confirm all three policies have been created as shown below.							
category to view		V	Sequoia_cis_lvl2					
the policies		>	Reset Baseline	(Dngoing	cis_reset	All computers,	
		>	Sequoia_CIS Level 2_Audit	(Once every day	Check-in	Computers running macOS Sequoia	
		>	Sequoia_CIS Level 2_Remediation	c	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.

	5	Pro	
U	sername		
ſ			
	Required		
Р	assword		
ſ			8
	Required		
	Log	, in	

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

		Pro							Q 8	
2	8	Computers	Computers Configuration	Profiles						
2—	G	Inventory	C Filter Profiles	0 - 0 of 0			+ New	🖞 Upload		-
	8 Ø	Search Inventory Search Volume Content	NAME	⊕ LOGS	I COMPLETED	I PENDING	I FAILED	I SCOPE	ψ	
		Licensed Software Content Management	No data avaliable in table							
3—		Policies Configuration Profiles								
-		Software Updates								J



Α

- 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.

Options Scope		
Q. Search	General	
General	Name Display name of the profile	
Accessibility Not configured	Sequoia_cis_lvl2_AirDrop_Exemption	
ACME Certificate Not configured	Description Brief explanation of the content or purpose of the profile	
AD Certificate Not configured		
AirPlay Not configured	Site Site to add the profile to None	
App-To-Per-App VPN Mapping Not configured	Category Category to add the profile to	
Application & Custom ~ Settings Not configured	Sequela_cis_tVl2	
Approved Kernel Extensions Not configured	Distribution Method Method to use for distributing the profile	
- Associated Demoins	Install automatically	
Not configured	Redistribute Profile After Cancel Save	

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

	Options Scope		
Q Se	arch	External Applications	
®,	General	Use this section to define settings for preference domains available Remove all + A in the repository.	dd
۲	Accessibility Not configured		
۵,	ACME Certificate Not configured		
٥	AD Certificate Not configured		
Ģ	AirPlay Not configured		
a	App-To-Per-App VPN Mapping Not configured		
	Application & Custom Settings Not configured		
	Jamf Applications		
	External Applications		
	Upload	0	2



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

Ċ	Options Scope		
ς Se	arch	External Applications	
0,	General	1 payload configured	
۲	Accessibility Not configured	org.cis_lvl2.audit × ^	
۰,	ACME Certificate Not configured	Source to use for the preference domain	
۵	AD Certificate Not configured	Custom Schema Preference Domain The name of the preference domain (com.company.application)	— A
G	AirPlay Not configured	org.cis_lvl2.audit	<u> </u>
۵	App-To-Per-App VPN Mapping Not configured	Custom Schema Required JSON Schema to populate configurable properties in the Property List	
0	Application & Custom Settings 1 payload configured		
	Jamf Applications		
	External Applications		
	Upload	• 8	

10.Click Upload.

	Custom JSON Schema
	Custom Schema Required JSON Schema to populate configurable properties in the Property List
	Required
10—	Dupload Clear
	Cancel



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.

	Choo	se Files to Upl	load	i	
$\langle \rangle \equiv \bullet \bigcirc \bullet$	📄 Jamf Compliance Editor 📀 🔍 Se		r 😒 🔍 Sear	arch	
Name	^	Size		Kind	Date Added
✓	a			Folder	Yesterday at 9:0
> 🚞 baselines				Folder	Yesterday at 9:0
> 🚞 bin				Folder	Yesterday at 9:0
v 🚞 build				Folder	Yesterday at 9:0
> 🚞 baselines				Folder	Yesterday at 9:0
✓ is_lvl2				Folder	Yesterday at 9:0
📠 cis_lvl2_complia	nce.sh	485 K	В	shell script	Yesterday at 9:0
b cis_lvl2.adoc		426 K	В	Document	Yesterday at 9:0
cis_lvl2.html		739 K	В	HTML text	Yesterday at 9:0
is_lvl2.pdf		2.4 N	1B	PDF Document	Yesterday at 9:0
cis_lvl2.xls		150 K	В	Microsok (.xls)	Yesterday at 9:0
v 🗖 iamforo				Folder	Yesterday at 9:0
cis_lvl2.json		50 K	в	JSON	Yesterday at 9:0
si complianmp	tions.sh	3 K	В	shell script	Yesterday at 9:0
				Cance	Upload

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	
Upload Clear	
Cancel	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**.

Co ¢	mputers : Configuration	Profiles OS Configuration Profile	
(Options Scope		
2 Se	arch	Not configured	
۵,	General	icloud_sync_disable	
۲	Accessibility Not configured	os_airdrop_disable	— в
۵,	ACME Certificate Not configured	Disable AirDrop Add/Remove properties	
۵	AD Certificate Not configured	exempt If value is true, exempt_reason is required	
Q	AirPlay Not configured		—c
8	App-To-Per-App VPN Mapping Not configured	Specify Exempt Reasoning Required by HCS	— D
0	Application & Custom Settings ^ 1 payload configured	os_anti_virus_installed	
	Jamf Applications	os_authenticated_root_enable	
	External Applications	os_bonjour_disable © (2) Cancel Save	



16.Click Scope.

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

← New macOS (Configuration Profi	le
Scope		
Targets	Limitations	Exclusions
Target Computers Computers to assign the profile to All Computers	Target Users Users to distribute the profile to Specific Users	
Selected Deployment Target	5	+ Add
TARGET	ТҮРЕ	
No Targets		
		Cancel 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.

	- Pro	
Username		
1		
Required		
Password		
		ଷ
Required		

- 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.

	Pro			
	□ Computers	Computers Configuration Profiles		
	Inventory	 ✓ Sequoia_cis_lvl2 		
8	Search Inventory	Sequoia_cis_IvI2-Accessibility	View	0
۲	Licensed Software	Sequoia_cis_IvI2-applicationaccess	View	0
	Content Management	Sequoia_cis_lvl2-assistant.support	View	0
	Policies	Sequoia_cis_lvl2-controlcenter	View	0
3 —	Configuration Profiles	Sequoia_cis_lvl2-loginwindow	View	0
	Software Updates	Sequoia_cis_lvl2-MCX	View	0
	Mac Apps	Sequoia_cis_lvl2-mDNSResponder	View	0
	Patch Management	Sequoia_cis_lvl2-mobiledevice.passwordpolicy	View	0
	eBooks	Sequoia_cis_lvl2-Safari	View	0
	Groups	Sequoia_cis_lvl2-screensaver	View	0
	Smart Computer Groups	Sequoia_cis_lvl2-security.firewall	View	0
l	Static Computer Groups	Sequoia_cis_lvl2-Siri	View	0



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

imitations Exclusions s thute the profile to sers * TYPE
s ibute the profile to sers * TYPE
Ibule the profile to sers * TYPE
туре

- 6. Click Targets.
- 7. Click Add.

 Sequoia 	_cis_lvl2-	Accessibility	,
Options Scope			
Targets		Limitations	Exclusions
Target Computers Computers to assign Specific Compute	Tar the profile to Use ers • Sp	get Users rs to distribute the profile to pecific Users	
Selected Deploym	ent Targets		+ Add

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

	Opti	ons Scope					
		Targets	Limita	itions	Excl	usions	
		Add Deployment Target	S			Done	
8—		Computers	Computer Groups	Users	User G Departments	Groups	
9 —		Q omputers running	1 - 1 of 1				
		GROUP NAME					
		Computers running mac	OS Sequoia			Add	1



11.Click Done.

Targets		Limita	tions	Exclusions
Add Deployment	Targets			Done
Computers	Computers Co		Users	User Groups

12.Click Save.

Sequoia_cis_lv	I2-Accessibility	
Options Scope		
Targets	Limitations	Exclusions
Target Computers Computers to assign the profile to Specific Computers • Selected Deployment Targets	Target Users Users to distribute the profile to Specific Users	+ Add
TARGET	TYPE	
TARGET Computers running macOS Sequoia	TYPE Smart Computer Group	Remove

13.Click Previous (←).

Computers : Configuration Profiles

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

Comput	omputers Configuration Profiles							
>	Platform Single Sign On							
>	Security							
~	Sequoia_cis_lvl2							
Se	equoia_cis_IvI2-Accessibility	View	1	1	0	Computers running macOS Sequoia		
Se	equoia_cis_IvI2-applicationaccess	View	0	0	0	No scope defined		
Se	equoia_cis_IvI2-assistant.support	View	0	0	0	No scope defined		
Se	equoia_cis_IvI2-controlcenter	View	0	0	0	No scope defined		
Se	equoia_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.

Username Required	
Required	
Required	
Password	
rassworu	
	8
Required	
Login	

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

		Pro		Q 8
2 —	8	Computers	Q Bearch Computers	~
- 2	G	Inventory	Search	
3 —	8	Search Inventory Search Volume Content	Advanced Computer Searches	+ New
	0	Licensed Software	NAME	へ ψ
		Content Mensel	AppleCare Warranty Expiration - Less Than 30 Days	

- 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	
Display Name Display name for the advanced computer search	
Sequoia CIS Benchmarks Level 2 Report	6
Site	
Site to add the advanced computer search to None •	
Save this search	J



- 7. Click Criteria.
- 8. Click Add.



9. Click Show Advanced Criteria.



10. Find Operating System Version and click Choose.

Operating System Version	Choose
operating system version	Clique

- 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

	Computers : Advanced Computer Search ← New Advanced Computer S	earch	
	Search Criteria Display Reports		
	Compliance - Exemptions		
15	Compliance - Failed Result List		
15—	Compliance - Failed Results Count		
	Compliance - Version		
	Controller Chip Type - T1 or T2		
	Current Logged in User		
	Days since last reboot		
	Default Web Browser	en den soorte den soorte den soorte de	
	Deployment Type	8	a 1
	Dockutil Installed	Cancel	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.

X Filter Results	1 - 2 of 2				+ New
AME		TE 🜵 LAST CHECK-IN	I IP ADDRESS	COMPLIANCE - FAILED RESULT LIST	
Keith Macbook Pr	o 4 minutes ago	5 minutes ago	24.44.131.89	icloud_sync_disable os_airdrop_	disable os_bonj
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

		Existing project	
		Create new project	3
2	maces iOS/iPadOS visionOS		

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

	n the list:				
4 —	ios 18	\bigcirc	Cancel	Create	<u> </u>

- 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)



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

10.Click Save

Please select where to save the mSCP direct	Q Search	
Name	Size	Kind
New Folder	Cancel	Save

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

	Please select a Security Benchmark from the list:		
10—	CIS Benchmark - Level 2 BYOD 📀	Cancel	— 11

13.Click Create Guidance.

•••	Jamf Compliance Editor	Qr Search				
CIS Benchmark - Level 2 BYOD IOS/IPadOS 18.0	Rules 25 Rules, 25 included, 25 found Sort - ID S					
Sections	✓ 2.2.1.3 Ensure Managed Apps Storing Data in iCloud is S					
All Sections	✓ 2.2.1.10 Ensure Treat AirDrop as unmanaged destination i					
	2.2.1.8 Ensure Allow documents from managed sources i					
iCloud	2.2.1.9 Ensure Allow documents from unmanaged source					
iOS						
	2.2.1.12 Disable Sending Diagnostic and Usage Data to A					
Password Policy	✓ 2.2.1.7 Ensure Force automatic date and time is set to En					
	2.2.1.4 Ensure Force Encrypted Backups is Enabled					
Supplemental	✓ 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					
	2.3.3.1.2 Ensure Allow Ciri while device is lealed is eat to D					
CIS Benchmark - Level 2 BYOD 📀 ၇	+ - Show All		Jamf Pro Upload	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.

•••	Jamf Compliance Editor	Q~ Search				
CIS Benchmark - Level 2 BYOD iOS/iPadOS 18.0	Rules 25 Rules, 25 included, 25 found Sort - ID					
Sections	✓ 2.2.1.3 Ensure Managed Apps Storing Data in iCloud is S					
All Sections	2.2.1.10 Ensure Treat AirDrop as unmanaged destination i					
	2.2.1.8 Ensure Allow documents from managed sources i					
iCloud	2.2.1.9 Ensure Allow documents from unmanaged source					
ios	2.2.1.13 Ensure Force Apple Watch wrist detection is set					
	2.2.1.12 Disable Sending Diagnostic and Usage Data to A					
Password Policy	2.2.1.7 Ensure Force automatic date and time is set to En					
	2.2.1.4 Ensure Force Encrypted Backups is Enabled					
Supplemental	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 Ciri while device is leaked is set to D					
CIS Benchmark - Level 2 BYOD 📀 🕐	+ - Show All	Jamf Pro Upload Create Guidance				



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.

	- Pro	
Username		
1		
Required		
Password		
		8
Required		
	Log in	

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

[2	Pro			Q 8
		Co Devices	Mobile Devices Smart Device	e Groups	
2 —	G	Inventory			+ New
	8	Search Inventory	NAME	△ I MEMBERSHIP COUNT	I AUTOMATED MANAGEMENT
	٩	Search Volume Content	All Managed iPads	0	No
		Content Management	All Managed iPhones	1	No
		Configuration Profiles	All Managed iPod touches	0	No
		Software Updates			
		Provisioning Profiles			
		Personal Device Profiles			
		Mobile Device Apps			
		eBooks			
		Groups			
3 —		Smart Device Groups			
l		Static Device Groups			



- 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 Device Group Criteria Automated Management	
Display Name	
Account Driven Liser Enrolled iOS/iPadOS devices running iOS 18	
Site Site to add the smart mobile device group to	
⊙ 🛱	
Cancel Save	

- 6. Click Criteria.
- 7. Click Add.

	Mobile Devic ← Ne	es : Smart Device G Smart N	^{Toups} Mobile De	vice Gr	oup	
6 —	Mobile De	rico Group Criteria	Automated Man	agement		
	AND/OR	CRITERIA	OPERATOR	VALUE		
	No Criteria Sp	ecified				
					+ Ada	• 7

8. Click Show Advanced Criteria.

Mobile Devices : Smart	Device Grou art M	obile Device	Group
Mobile Device Group	Criteria	Automated Management	
NEW CRITERIA			Show Advanced Criteria

9. Scroll down to OS Version and click Choose.

OS Version Choose



10.Configure the following:

- A. Select like for the Operator.
- B. Enter **18** for the Value
- C. Click Add

Mobile Devices : ← New	Smart Device G	Broups Mobile Dev	vice Group		
Mobile Device	Group Criteri	a Automated Manag	ement		
AND/OR	CRITERIA OS Version		VALUE	 • Delete	
2			В	+ Add	c

11. Click Show Advanced Criteria.

Mobile Devices : Smart	Device Grou	obile Device G	roup
Mobile Device Group	Criteria	Automated Management	
NEW CRITERIA			Show Advanced Criteria

12. Select Device Ownership Type and click Choose.

Device Ownership Type	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

Mobile Devices : Smart	Device Groups art Mobile De	evice Group		
Mobile Device Group	Criteria Automated Ma	nagement		
AND/OR	CRITERIA OPER	ATOR	VALUE	
•	OS Version	•	18	 Delete
and 🔹 💌	Device Ownership Type	•	Personal (Account-Driven User Enro	 • Delete
	В —	J	с —	+ Add

14. Click Show Advanced Criteria.

Mobile Devices : Smart	Device Grou	ps obile Device Group	
Mobile Device Group	Criteria	Automated Management	
NEW CRITERIA			Show Advanced Criteria



15. Select Device Ownership Type and click Choose.

Device Owne	ership Type	Choose
Device Owne	arship type	CR

- 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 Device Gro	up Criteria Automat	ed Management Repo	orts			
AND/OR	CRITERIA	OPERATOR	VALUE			
	OS Version	like	• 18		•	Delete
and •	Device Ownership Type	is •	Personal (Account-Driven Use	er Enrollmei	•	Delete
or •	Device Ownership Type	is •	Personal (User Enrollment)) •	Delete
	В-		с			E
			-			

17.Click Previous (←).

Mobile Dev	/ices :	Smart Device Groups
← Ac	cco	unt 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	
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.

		Pro						\$ \$	
	8	C Devices	Mobile Devices Configuration P	rofiles	6				
19—	G	Inventory	C Filter results	1 - 5 of 5		+	- New	oload 📃 🛞	
	8	Search Inventory	21	1.1000					
	Ø	Search Volume Content		III LOGS	III COMPLETE		IN PAILED		
	ø	Content Management	iOS18_cis_lvl2_by	od					
20—		Configuration Profiles	iOS18_cis_lvl2_byod-	View	0	0	0	No scope	
		Software Updates	applicationaccess		Ŭ	Ŭ	Ŭ	defined	
		Provisioning Profiles	iOS18_cis_lvl2_byod-	View	0	0	0	No scope	
		Personal Device Profiles	mail.managed					defined	
		Mobile Device Apps	iOS18_cis_lvl2_byod- mobiledevice.passwordpolicy	View	0	0	0	No scope defined	
		eBooks							

- 23. Select Scope.
- 24. Click Edit.

ns Scope 2	3		Show in Jan	if Pro Dash	board
Targets	Limitatio	ons	Ex	clusions	
arget Mobile Devices	Target Users				
Mobile devices to assign the profile to. Does not apply to personally owned devices	Users to distribute to	the profile			
Specific Mobile Dev 🔹	Specific Users	Ŧ			
RGET	т	YPE			
Targets					
	o D	ė	¢	ŵ	ø



25.Click Add.

Options Scope		
Targets	Limitations	Exclusions
Target Mobile Devices Mobile devices to assign the profile to. Does not apply to personally owned devices	Target Users Users to distribute the profile to	
Specific Mobile Devices •	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

Add Deployment Targets Done Mobile Devices Mobile Device Groups Users User Groups Buildings Departments	Options Scope			
Mobile Devices Mobile Device Groups Users User Groups Buildings Departments	Add Deployment Targets	— A		Done
Buildings Departments	Mobile Devices	Mobile Device Groups	Users	User Groups
	Building	gs	Departr	nents
Q account driven 1 - 1 of 1	Q account driven 1 - 1 o	f1		

27.Click Done.

ions Scope			
Targets	Limitation	3	Exclusions
Add Deployment Targets			Done
Add Deployment Targets	Mobile Device Groups	Users	User Groups



28.Click Save.

Targets	Limitations		Exclusions	
Target Mobile Devices	Target Users			
Mobile devices to assign the profile to. Does not apply to personally owned devices	Users to distribute the profile to			
Specific Mobile Devices	Specific Users	•]		
Selected Deployment Targets			+	Add
Selected Deployment Targets		ТҮРЕ	+	Add
Selected Deployment Targets ARGET Account Driven User Enrolled iOS/IPadOS	devices running iOS 18	TYPE Smart Mobile D	+ evice Group Res	Add

29.Click Previous (\leftarrow).



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_IvI2_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.



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.

Favorites	Please select your mSCP directory.
 Recents Applicati 	<> III • III • III • Content • Conte
 Desktop Documents Downloads 	□ Jamf Compliance Editor - macOS Sequoia → □ macOs_security-sequoia → □ t ↓
Locations	
Tags Red	
Yellow	Cancel Open

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

	Please select a Se	curity Bench	mark from the list:		
6 —	CIS Benchmark - Level 2	\bigcirc	Cancel	ок	 7



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

Save As:	Local-Audit-Keith-MBA.csv	•	15
Tags:			
Where:	📄 Desktop 📀	~ •	16
	Cancel	Save	17

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





O 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

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

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.

	Please select a Sec	curity Benchm	nark from the list:	
6 —	CIS Benchmark - Level 2	٢	Cancel OK	<u> </u>

- 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.

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

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.

•••	Jamf Compliance Edit	or
		Existing project
		Create new project
macOS iOS/iPadOS visionOS)	

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

Favorites	Please select your mSCP directory.	
ecents	K > IIII v IIII v IIII macos_security-sequoia Q Search	
🙏 Applicati		
E Desktop	늘 Jamf Compliance Editor - macOS Sequoia > 📋 macos_security-sequoia >	📄 ba
Documents		🚞 bi
Downloads		bu 📄
Loostions		C
iCloud Dri		— cu
		G
Tags		G
Red		🚞 in
Orange		1.1.1
• Yellow	Cancel	Open


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

	Please select a Se	rk from the list:		
6—	CIS Benchmark - Level 2	٢	Cancel	<u> </u>

- 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 Transitional and the provincial and the provincit

Timeout set to 5 minutes. The original value was 0

- 16.Click Done
- 17.Click Create Guidance

•••	Jamf Compliance Editor		Q~ odv	•
CIS Benchmark - Level 2 macOS 15.0	Rules 114 Rules, 114 included, 17 found	Sort - ID	Rule Details	Revert Done 1
Sections	3.4 Configure Audit Retention to \$ODV		ID:	
All Sections	3.3 Configure Install.log Retention to \$ODV		os_sudo_timeout_configure	
	5.8 Display Policy Banner at Login Window		Title:	Show
Auditing	1.7 Ensure Software Update Deferment Is Less The	an or Equal to \$0	Discussion:	Hide
iCloud	☑ 5.4 Configure Sudo Timeout Period to \$ODV	М	MODIFIED RULE Timeout set to 5 minutes. The original	value was 0
loiduu	✓ 5.7 Disable Login to Other User's Active and Lock	ed Sessions	The file /etc/sudoers MUST include a	
macOS	✓ 5.2.1 Limit Consecutive Failed Login Attempts to \$	ODV	Check:	Show
	5.2.1 Set Account Lockout Time to \$ODV Minutes		Result:	Show
Password Policy	✓ 5.2.6 Require Passwords to Match the Defined Cu	stom Regular Exp	Fix:	Show
System Settings	5.2.8 Prohibit Password Reuse for a Minimum of \$	ODV Generations	References: Add New	Show
System Settings	✓ 5.2.7 Restrict Maximum Password Lifetime to \$OD	V Days	Organization Defined Value:	Hide
Supplemental	✓ 5.2.2 Require a Minimum Password Length of \$OD	V Characters	5	mao
	5.2.5 Require Passwords Contain a Minimum of Or	ne Special Charac		
	2.10.3 Configure Login Window to Show A Custom	Message	Tags:	Show
	2.10.2 Enforce Session Lock After Screen Saver is	Started	Mobileconfig:	Show
	2.10.1 Enforce Screen Saver Timeout			
	2.3.2.1 Configure macOS to Use an Authorized Tin	ne Server		
CIS Benchmark - Level 2	? + - Show All		Audit Jamf Pro Upload	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.

<	$ ightarrow $ cis2-hcs_modified_odv_gu $arepsilon \equiv \diamondsuit$
	Name
sh	cis2-hcs_modified_odv_guidance_compliance.sh
	cis2-hcs_modified_odv_guidance.adoc
0	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.



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

23.Click the highlighted page.

•	cis2-hcs_modified Page 3 of 120	í	Q	€	Û	<u>/</u> ~	ŕ	» Q~ sudo timeout	22
Sort By:	Search Rank Page Or	der						Found on 2 pages () Done	
	8.27. Ensure Sleep and I 8.28. Ensure Software U 8.29. Configure Sudo To	Display Sl pdate De Log Ever	leep Is I fermen nts.	Enable it Is Le	d on A ss Tha	pple Silicon I n or Equal to	evices. 30 Days	50 5	
	8.30. Configure Sudo II 8.31. Configure Sudoers 8.32. Ensure Appropriat	Timestar e Permis	mp Typ sions A	e re Ena	bled fo	or System Wie	le Appli		23



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. Co	nfigure Su	do Timeout Period to 5
MODIFIED RU include a time	ILE Timeout set to estamp_timeout of	o 5 minutes. The original value was 0 The file /etc/sudoers MUS7 5.
To check the s	tate of the system,	, run the following command(s):
/usr/bin/su 5.0 minutes	do /usr/bin/sudo "	-V /usr/bin/grep -c "Authentication timestamp timeout:
If the result is	not 1 , this is a find	ting.
Perform the /usr/bin/	following to conf /find /etc/sudoer Defaults times	<pre>igure the system to meet the requirements: s* -type f -exec sed -i '' '/timestamp_timeout/d' '{}' \; tamp_timeout=5" >> /etc/sudoers.d/mscp</pre>
ID	os_sudo_timeout	:_configure
ID References	os_sudo_timeout 800-53r5 CIS Bonchmark	t_configure • N/A • 5.4 (level 1)
ID References	os_sudo_timeout 800-53r5 CIS Benchmark CIS Controls V8	• N/A • 5.4 (level 1) • 4.3

This completes the guide.