

Automating CIS Benchmark Reporting and Remediation

● JAMF
NATION
LIVE

Agenda

1 | macOS Security

Have a look what Apple has been doing on the security stack and build into the system.

2 | Security Benchmarks

Organisations that provide guidance of the Security standard depending on industry and/or geo-location.

3 | Scripts

How we can use the CIS-Script to help you to audit, remediate and report based on the Benchmark rules.

4 | Implementation

See how easy it is to deploy the CIS script in your environment.

Business is changing

● JAMF NATION LIVE



Employee mobility Work anywhere

● JAMF NATION LIVE





Protecting Corporate & Customer Data

Security & Compliance

● JAMF NATION LIVE

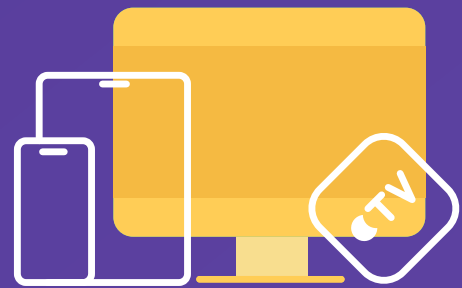


AEM Platform

Manage your Devices Apple Ecosystem Management	Connect your Users Identity & Access Control	Protect your Data Endpoint Security	Complete your Solution Value-Added Workflows
<p>ENTERPRISE</p> <p>Jamf Pro</p> <p>SMB</p> <p>Jamf Now</p> <p>EDUCATION</p> <p>Jamf School</p> <p>DATA POLICY</p> <p>Jamf Data Policy</p>	<p>MAC ACCOUNT & SECURE AUTHENTICATION</p> <p>Jamf Connect</p> <p>ZTNA NETWORK ACCESS</p> <p>Jamf Private Access</p>	<p>macOS THREAT DETECT & PREVENTION</p> <p>Jamf Protect</p> <p>iOS DEVICE THREAT DETECT & PREVENTION</p> <p>Jamf Threat Defence</p>	<p>EDUCATION</p> <ul style="list-style-type: none">▶ Teacher▶ Student▶ Parent <p>HEALTHCARE</p> <ul style="list-style-type: none">▶ Patient Experience▶ Clinical Communication▶ Virtual Visits <p>X-INDUSTRY</p> <ul style="list-style-type: none">▶ Set-up and Reset for Shared Devices and workflow



Connect your Users



Manage your Devices

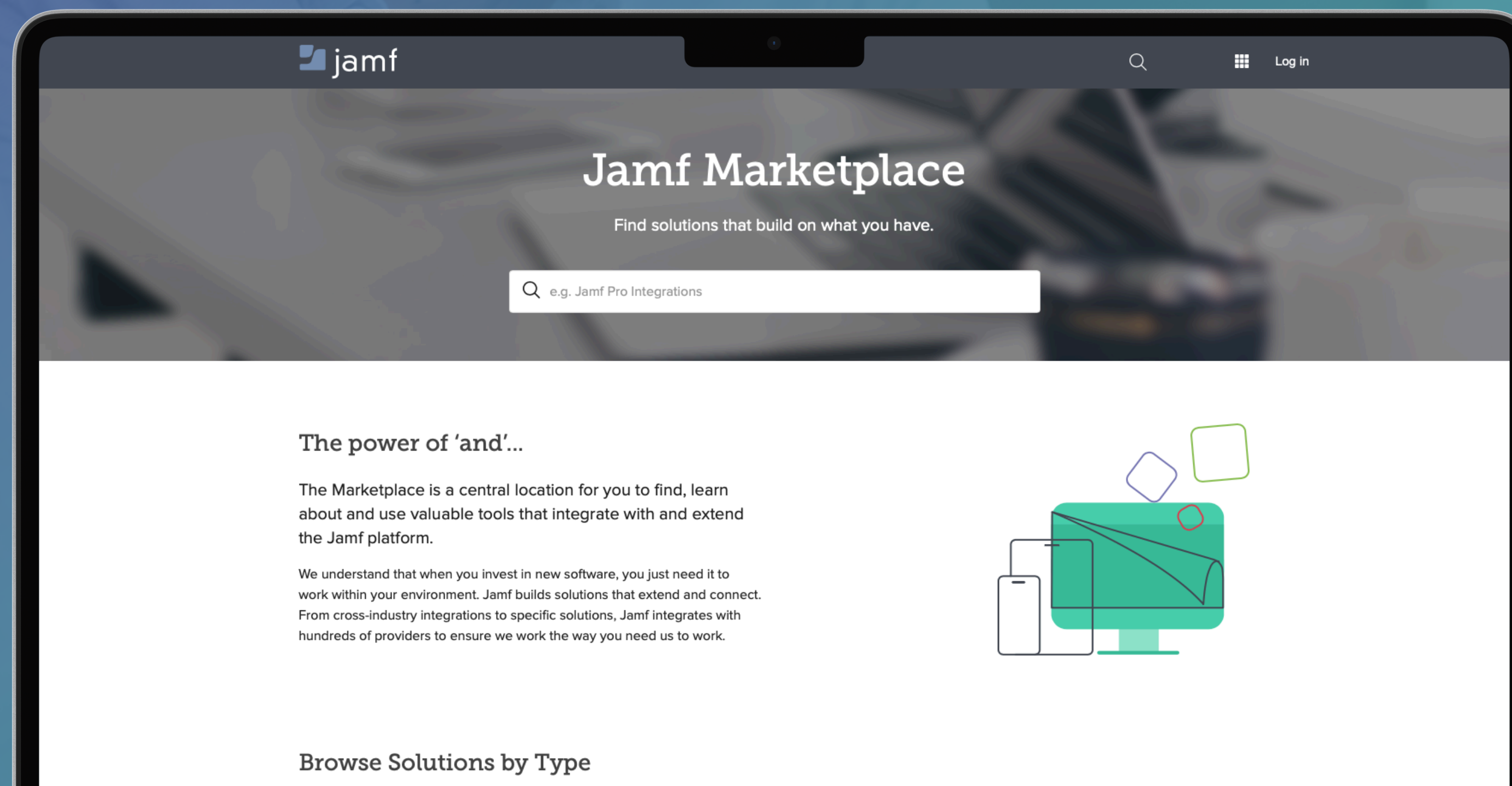


Protect your Data

Amplify the power of Jamf with integrations,
apps and open-source tools

Jamf Marketplace

Expanded Ecosystem and Support Strengthen the
Jamf Platform and Improve Jamf Efficiency



● JAMF NATION LIVE

macOS Security



**Enterprise-grade security
that's built right in.**

UNIX Apple File System Mobile Device Management Password Protection Secure Enclave

Malware Removal Tool Secure Authentication Runtime Protection FileVault Access Rights

Configuration Enforcement Mandatory Access Controls Encrypted Disk Images Touch ID

System Integrity Protection Keychains XProtect Automatic Security Updates

Cryptographic Validation Gatekeeper Firewall App Transport Security

ISO Certification System Extensions VPN On-Demand Smart Cards

Digital Signing and Encryption VPN Secure Boot Restrictions Firmware Password

Per-app VPN Remote Wipe Single Sign-On Per-message S/MIME App Code Signing

Sandboxing Internet Recovery AirDrop Security Remote Lock



Security Benchmarks



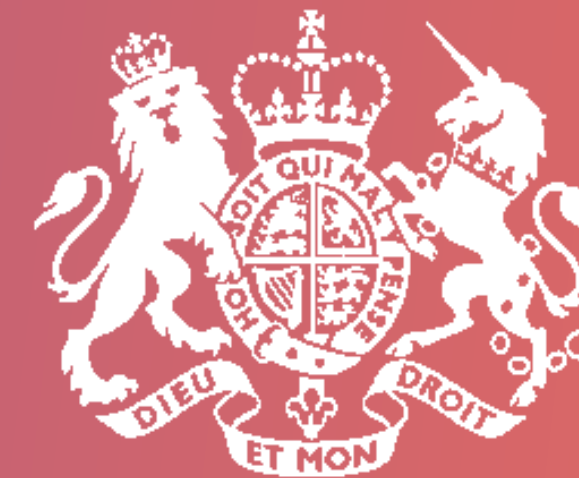
Center for Internet Security



Defense Information Security Agency (US)



National Institute of Standards and Technology (US)




National Cyber Security Centre (UK)



macOS Security Compliance

github.com/usnistgov/macOS_security

file:///Users/mischa/Git/macOS_security-2/build/cis_lvl2/cis_lvl2.html



macOS 12.0

Security Configuration - CIS Benchmarks

Monterey Guidance, Revision 2 (2022-03-16)

Share Comments


Auto-sum Fill Clear Sort & Filter Find & Select Analyse Data Sensitivity

M	N	O
CCI	Modified Rule	CIS
None	customized rule customized references	1.1 Verify all Apple-provided software is current Level 1
None	customized rule customized references	1.2 Enable Auto Update (Automated) Level 1

unsigned

- preferences
- unsigned
 - com.apple.AdLib.mobileconfig
 - com.apple.applicationaccess.mobileconfig
 - com.apple.GlobalPreferences.mobileconfig
 - com.apple.loginwindow.mobileconfig
 - com.apple.ManagedClient.preferences.mobileconfig
 - com.apple.MCX.FileVault2.mobileconfig
 - com.apple.MCX.mobileconfig
 - com.apple.mDNSResponder.mobileconfig
 - com.apple.mDNSResponder.mobileconfig
 - com.apple.mobiledevice.passwordpolicy.mobileconfig
 - com.apple.preferences.sharing.SharingPrefsExtension.mobileconfig
 - com.apple.Safari.mobileconfig
 - com.apple.screensaver.mobileconfig
 - com.apple.security.firewall.mobileconfig
 - com.apple.smb.server.mobileconfig
 - com.apple.SoftwareUpdate.mobileconfig
 - com.apple.SubmitDiagInfo.mobileconfig
 - com.apple.systempolicy.control.mobileconfig
 - com.apple.Terminal.mobileconfig

file:///Users/mischa/Git/macOS_security-2/build/cis_lv12/cis_lv12.html



CIS Benchmarks™

Audit

Remediate

macOS 12.0

Security Configuration - CIS Benchmarks

Monterey Guidance, Revision 2 (2022-03-16)

10.5. Disable Bluetooth When No Devices are Paired

Bluetooth *MUST* be disabled when no devices are paired.

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

```
isPaired=$( /usr/sbin/system_profiler SPBluetoothDataType 2>/dev/null | /usr/bin/grep -c 'Connected: Yes' )
if [[ "$isPaired" = "0" ]] ; then
  poweroff
else
  /bin/
fi
```

Audit

If the result is not 0, this is a finding.

Remediate

Perform the

```
/usr/bin/defaults write /private/var/root/Library/Preferences/com.apple.Bluetooth.plist
defaultPoweredState off
/usr/bin/defaults write /private/var/root/Library/Preferences/com.apple.Bluetooth.plist
```

Remediate

Report

ID

References

800-53r5

- AC-18, AC-18(3)
- SC-8

CIS Benchmark

- 2.1.1 (level 1)

CIS Controls V8

- 4.8, 12.6, 13.9

CCE

- CCE-91126-3

Scripts

main 1 branch 1 tag Go to file Code

Table with 3 columns: File Name, Commit Message, and Commit Date. Rows include .gitignore, 4_Security_Report.sh, Example-Report.numbers, LICENSE, README.md, and Scoring.png.

README.md

CIS-Reporting

Current state of the scripts are: "The scripts is "As is" please be free to give me any feedback

```
INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL I BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
```

license Apache-2.0

About No description, website, or topics provided. Readme Apache-2.0 License

Releases 1

v.0.8 Latest on 8 Feb

Packages

No packages published

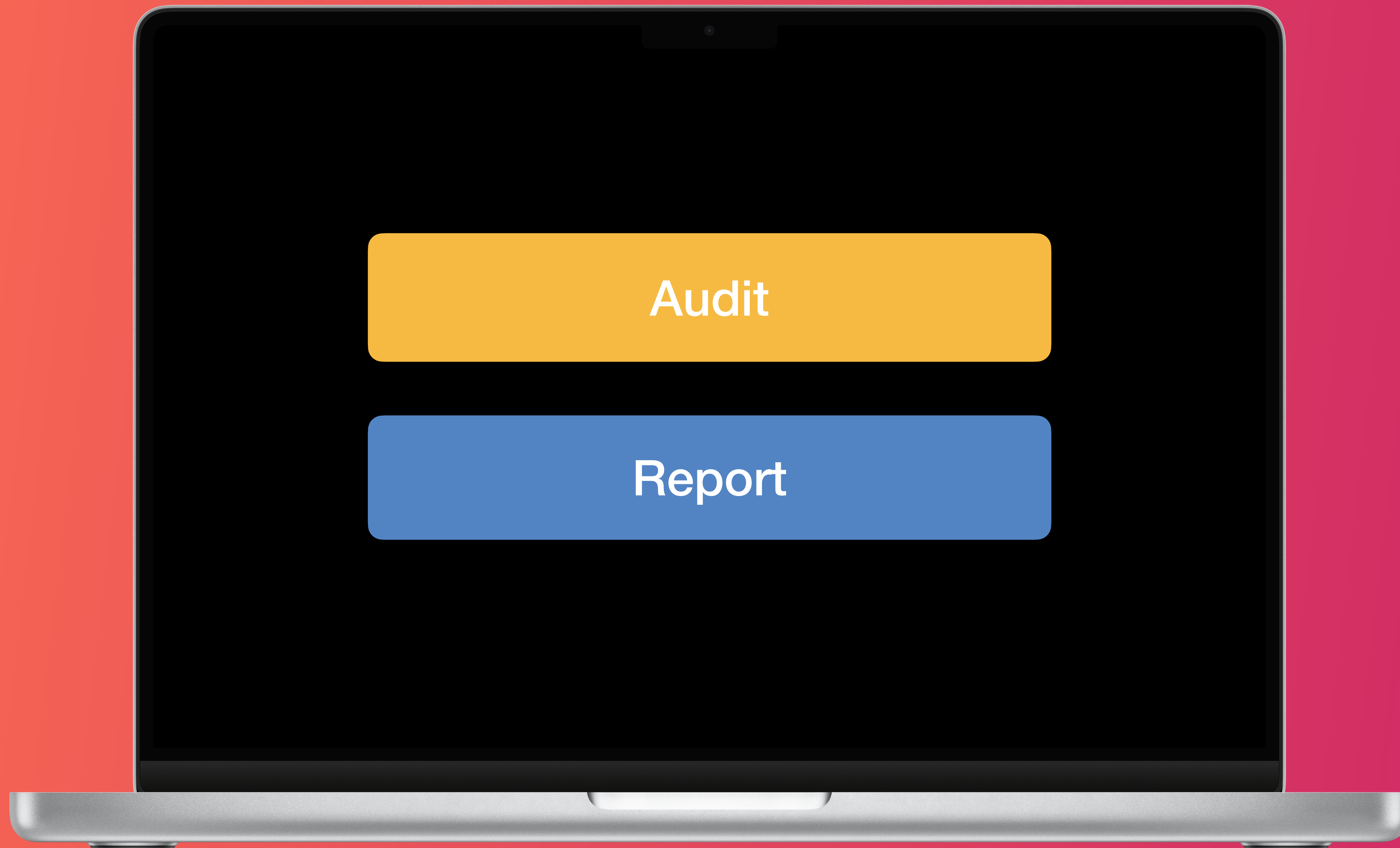
Languages





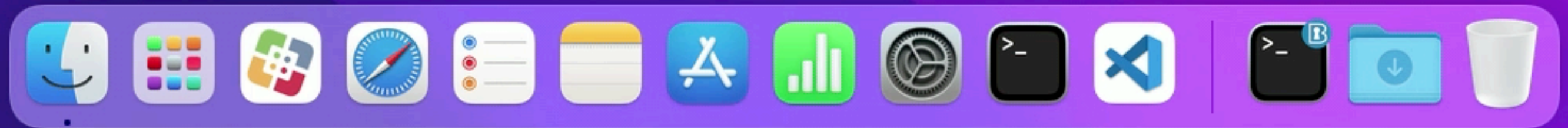
CIS Script

github.com/mvdbent/CIS-Script



Audit

Report

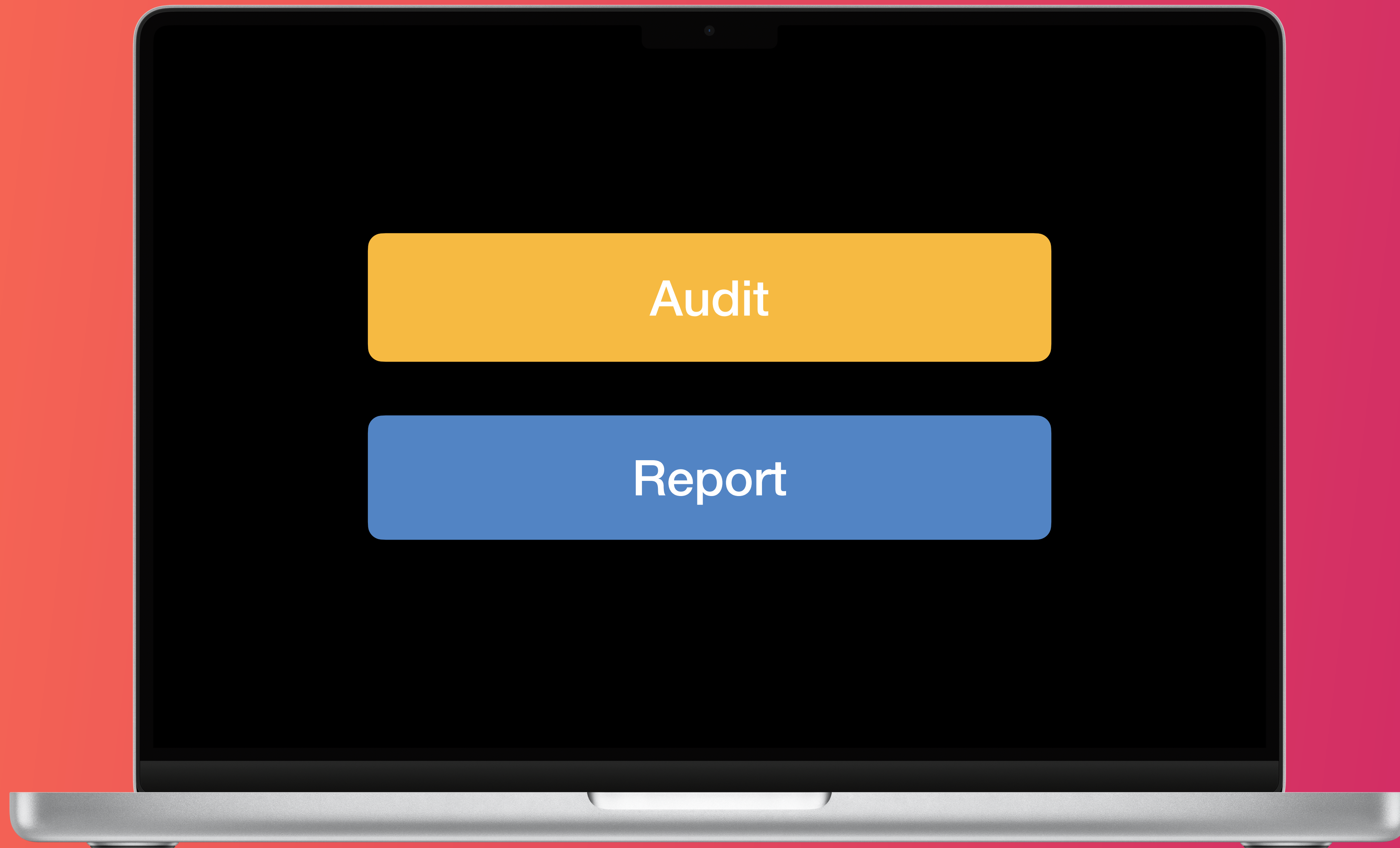


CISBenchmarkReport-Full

Audit Number	Level	Scoring	Result	Managed	Preference domain	Option	Value	Method	Comments	Remediate
1.1 Verify all Apple-provided software is current (Automated)	1		Passed					Script	Apple Software is Current	Script > sudo /usr/sbin/softwareupdate --install --restart --recommended
1.2 Enable Auto Update (Automated)	1		Passed	FALSE	com.apple.SoftwareUpdate	AutomaticCheckEnabled	TRUE	Profile	Auto Update: Enabled	Configuration profile - payload > com.apple.SoftwareUpdate > AutomaticCheckEnabled=true
1.3 Enable Download new updates when available (Automated)	1		Passed	FALSE	com.apple.SoftwareUpdate	AutomaticDownload	TRUE	Profile	Download new updates when available: Enabled	Configuration profile - payload > com.apple.SoftwareUpdate > AutomaticDownload=true
1.4 Enable app update installs (Automated)	1		Passed	FALSE	com.apple.commerce	AutoUpdate	TRUE	Profile	App updates: Enabled	Configuration profile - payload > com.apple.SoftwareUpdate > AutomaticallyInstallAppUpdates=true
1.5 Enable system data files and security updates install (Automated)	1		Failed	FALSE	com.apple.SoftwareUpdate	ConfigDataInstall	None	Profile	System data files and security update installs: Disabled	Configuration profile - payload > com.apple.SoftwareUpdate > ConfigDataInstall=true - CriticalUpdateInstall=true
1.6 Enable macOS update installs (Automated)	1		Passed	FALSE	com.apple.SoftwareUpdate	AutomaticallyInstallMacOSUpdates	TRUE	Profile	macOS update installs: Enabled	Configuration profile - payload > com.apple.SoftwareUpdate > AutomaticallyInstallMacOSUpdates=true
2.1.1 Turn off Bluetooth, if no paired devices exist (Automated)	1		Failed					Script	No Paired Devices	Script - defaults write /Library/Preferences/com.apple.Bluetooth.ControllerPowerState -bool false
2.1.2 Show Bluetooth status in menu bar (Automated)	1		Passed	FALSE	com.apple.controlcenter	NSStatusItem.VisibleBluetooth		Script	Show Bluetooth status in menu bar: Enabled	Script > sudo -u firstuser defaults -currentHost write com.apple.controlcenter.plist Bluetooth -int 18
2.2.1 "Enable Set time and date automatically" (Automated)	1		Failed	FALSE	com.apple.timed	TMAutomaticTimeOnlyEnabled	None	Profile	Time and date automatically: Disabled	Configuration profile - payload > com.apple.timed > TMAutomaticTimeOnlyEnabled=true
2.2.2 Ensure time set is within appropriate limits (Automated)	1		Passed					Script	Network Time Server: time.euro.apple.com	Script > sudo /usr/sbin/systemsetup -setusingnetworktime on && sudo /usr/sbin/systemsetup -setnetworktimeserver time.euro.apple.com
2.3.1 Set an inactivity interval of 20 minutes or less for the screen saver (Automated)	1		Passed	FALSE	com.apple.screensaver	idleTime		Profile	Inactivity interval for the screen saver: 1200	Configuration profile - payload > com.apple.screensaver > idleTime=1200
2.3.2 Secure screen saver corners (Automated)	2		Failed	FALSE	com.apple.dock	wvous-bl-corner, wvous-tl-corner, wvous-tr-corner, wvous-br-corner	None, None, None, None	Profile	Secure screen saver corners: Disabled	Configuration profile - payload > com.apple.dock > wvous-tl-corner=5, wvous-br-corner=10, wvous-bl-corner=13, wvous-tr-corner=0 - 5=Start Screen Saver, 10=Put Display to Sleep, 13=Lock Screen
2.3.3 Familiarize users with screen lock tools or corner to Start Screen Saver (Manual)	1		Passed	FALSE	com.apple.dock			Manual	End-users are familiar with screen lock tools or Hot Corners	Familiarise users with screen lock tools or corner to Start Screen Saver
2.4.1 Disable Remote Apple Events (Automated)	1		Passed					Script	Remote Apple Events: Disabled	Script > sudo /usr/sbin/systemsetup -setremoteappleevents off && sudo launchctl disable system/com.apple.AEServer
2.4.2 Disable Internet Sharing (Automated)	1		Passed					Profile	Internet Sharing: Disabled	Configuration profile - payload > com.apple.MCX > forceInternetSharingOff=true
2.4.3 Disable Screen Sharing (Automated)	1		Passed					Script	Screen Sharing: Disabled	Script > sudo launchctl disable system/com.apple.screensharing
2.4.4 Disable Printer Sharing (Automated)	1		Passed					Script	Printer Sharing: Disabled	Script > sudo /usr/sbin/cupsctl --no-share-printers
2.4.5 Disable Remote Login (Automated)	1		Passed					Script	Remote Login: Disabled	Script > sudo /usr/sbin/systemsetup -setremotelogin off
2.4.6 Disable DVD or CD Sharing (Automated)	1		Passed					Script	DVD or CD Sharing: Disabled	Script > sudo launchctl unload -w /System/Library/LaunchDaemons/com.apple.ODSAgent.plist
2.4.7 Disable Bluetooth Sharing (Automated)	1		Passed	FALSE	com.apple.Bluetooth	PrefKeyServicesEnabled		Script	Bluetooth Sharing: Disabled	Script > sudo -u 'CURRENT_USER' defaults -currentHost write com.apple.Bluetooth.PrefKeyServicesEnabled -bool false
2.4.8 Disable File Sharing (Automated)	1		Passed					Script	File Sharing: Disabled	Script > sudo launchctl disable system/com.apple.smbd
2.4.9 Disable Remote Management (Automated)	1		Passed					Script	Remote Management: Disabled	Script > sudo /System/Library/CoreServices/RemoteManagement/ARDAgent.app/Contents/Resources/kickstart -deactivate -stop
2.4.10 Disable Content Caching (Automated)	2		Passed	FALSE	com.apple.applicationaccess	allowContentCaching	None	Profile	Content Caching: Disabled	Configuration profile - payload > com.apple.applicationaccess > allowContentCaching=false
2.4.11 Disable Media Sharing (Automated)	1		Failed	FALSE	com.apple.preferences.sharing.SharingPrefsExtension	homeSharingUIStatus, legacySharingUIStatus, mediaSharingUIStatus	None, None, None	Profile	Media Sharing: Enabled	Configuration profile - payload > com.apple.preferences.sharing.SharingPrefsExtension > homeSharingUIStatus=0 > legacySharingUIStatus=0 > mediaSharingUIStatus=0
2.5.1.1 Enable FileVault (Automated)	1		Passed	FALSE	com.apple.MCX.FileVault2	Enable	None	Profile	FileVault: Enabled	Configuration profile - payload > com.apple.MCX.FileVault2 > Enable=On
2.5.1.2 Ensure all user storage APFS volumes are encrypted (Manual)	1		Passed					Manual	Startup Volume: Encrypted	Manual - Ensure all user storage APFS Volumes are encrypted
2.5.1.3 Ensure all user storage CoreStorage volumes are encrypted (Manual)	1		Not applicable					Manual	Volumes: APFS	Manual - Ensure all user CoreStorage volumes encrypted
2.5.2.1 Enable Gatekeeper (Automated)	1		Passed	FALSE	com.apple.systempolicy.control	EnableAssessment	None	Profile	Gatekeeper: Enabled	Configuration profile - payload > com.apple.systempolicy.control > EnableAssessment=true
2.5.2.2 Enable Firewall (Automated)	1		Failed	FALSE	com.apple.security.firewall	EnableFirewall	None	Profile	Firewall: Disabled	Configuration profile - payload > com.apple.security.firewall > EnableFirewall=true
2.5.2.3 Enable Firewall Stealth Mode (Automated)	1		Passed	FALSE	com.apple.security.firewall	EnableStealthMode	None	Profile	Firewall Stealth Mode: Enabled	Configuration profile - payload > com.apple.security.firewall > EnableStealthMode=true
2.5.3 Review Application Firewall Rules (Manual)	1		Passed					Profile	Application Firewall Rules: Application Managed	Configuration profile - payload > com.apple.security.firewall > Applications > Array > BundleID=com.apple.app > Allowed=false
2.5.4 Enable Location Services (Automated)	2		Passed					Script	Location Services: Enabled	Script > sudo /usr/bin/defaults write /var/db/locationd/Library/Preferences/ByHost/com.apple.locationd.LocationServicesApplications -bool true && sudo /bin/launchctl kickstart -k system/com.apple.locationd
2.5.5 Monitor Location Services Access (Manual)	2		Notice					Manual	3 applications can accessing location services	Manual - Disable unnecessary applications from accessing location services
2.5.6 Disable sending diagnostic and usage data to Apple (Automated)	2		Passed	FALSE	com.apple.SubmitDiagInfo	AutoSubmit	None	Profile	Sending diagnostic and usage data to Apple: Disabled	Configuration profile - payload > com.apple.SubmitDiagInfo > AutoSubmit=false - payload > com.apple.applicationaccess > allowDiagnosticSubmission=false
2.5.7 Limit Ad tracking and personalized Ads (Automated)	1		Passed	FALSE	com.apple.AdLib	allowApplePersonalizedAdvertising		Profile	Limited Ad Tracking: Disabled	Configuration profile - payload > com.apple.AdLib > allowApplePersonalizedAdvertising=false
2.6.1 iCloud configuration (Manual)	2		Passed					Manual	no iCloud account(s) configured	Manual - Use a profile to disable services where organizationally required
2.6.2 iCloud keychain (Manual)	2		Failed	FALSE	com.apple.applicationaccess	allowCloudKeychainSync	None	Profile	iCloud keychain: Enabled	Configuration profile - payload > com.apple.applicationaccess > allowCloudKeychainSync=false
2.6.3 iCloud Drive (Manual)	2		Failed	FALSE	com.apple.applicationaccess	allowCloudDocumentSync	None	Profile	iCloud Drive: Enabled	Configuration profile - payload > com.apple.applicationaccess > allowCloudDocumentSync=false
2.6.4 iCloud Drive Document and Desktop sync (Manual)	2		Failed	FALSE	com.apple.applicationaccess	allowCloudDesktopAndDocuments	None	Profile	iCloud Drive Document and Desktop sync: Enabled	Configuration profile - payload > com.apple.applicationaccess > allowCloudDesktopAndDocuments=false
2.7.1 Time Machine Auto-Backup (Automated)	2		Passed					Script	Time Machine Auto-Backup: Enabled	Script > sudo defaults write /Library/Preferences/com.apple.TimeMachine.plist AutoBackup 1
2.7.2 Time Machine Volumes Are Encrypted (Automated)	1		Passed					Manual	No Time Machine Volumes available	Manual > Set encryption through Disk Utility or diskutil in terminal
2.8 Disable Wake for network access (Automated)	1		Passed					Script	Wake for network access: Disabled	Script > sudo /usr/bin/pmset -a womp 0
2.9 Disable Power Nap (Automated)	1		Passed					Script	Power Nap: Enabled	Script > sudo /usr/bin/pmset -a powernap 0
2.10 Enable Secure Keyboard Entry in terminal.app (Automated)	1		Failed	FALSE	com.apple.Terminal	SecureKeyboardEntry	None	Profile	Secure Keyboard Entry in terminal.app: Disabled	Configuration profile - payload > com.apple.Terminal > SecureKeyboardEntry=true
2.11 Ensure EFI version is valid and being regularly checked (Automated)	1		Not applicable						EFI Firmware Integrity is not supported by this Mac. T2 Chip found.	
3.1 Enable security auditing (Automated)	1		Passed					Script	Security auditing: Enabled	Script > sudo launchctl load -w /System/Library/LaunchDaemons/com.apple.auditd.plist
3.2 Configure Security Auditing Flags per local organizational requirements (Manual)	2		Passed					Script	Security Auditing Flags: Enabled	Script > sudo /usr/bin/sed -i.bak '/flags/ s/\$,ad/ /etc/security/audit_control /usr/sbin/audit -s
3.3 Retain install.log for 365 or more days with no maximum size (Automated)	1		Failed					Script	Retain install.log: Less than 365 days	Script > add 'ttl=365' to /etc/asl/com.apple.install
3.4 Ensure security auditing retention (Automated)	1		Failed					Script	Security auditing retention: Unconfigured	Script > add 'expire-after:60d OR 1G' to /etc/security/audit_control
3.5 Control access to audit records (Automated)	1		Passed					Script	Control access to audit records: Correct ownership	Script > sudo chown -R root /var/audit
3.6 Ensure Firewall is configured to log (Automated)	1		Passed					Script	Firewall logging: Enabled	Script > sudo /usr/libexec/ApplicationFirewall/socketfilterfw --setloggingmode on
4.1 Disable Bonjour advertising service (Automated)	2		Failed	FALSE	com.apple.mDNSResponder	NoMulticastAdvertisements	None	Profile	Bonjour advertising service: Enabled	Configuration profile - payload > com.apple.mDNSResponder > NoMulticastAdvertisements=true
4.2 Enable "Show Wi-Fi status in menu bar" (Automated)	1		Passed		com.apple.controlcenter	NSStatusItem.VisibleWiFi	TRUE	Script	Wi-Fi status in menu bar: Enabled	Script > sudo -u <username> defaults -currentHost write com.apple.controlcenter.plist WiFi -int 18
4.4 Ensure http server is not running (Automated)	1		Passed					Script	HTTP server service: Disabled	Script > sudo launchctl disable system/org.apache.httpd
4.5 Ensure nfs server is not running. (Automated)	1		Passed					Script	NFS server service: Disabled	Script > sudo launchctl disable system/com.apple.nfsd && sudo rm /etc/exports
5.1.1 Secure Home Folders (Automated)	1		Passed					Script	Home Folders: Secure	Script > sudo chmod og-rwx 'HomeFolders'
5.1.2 Check System Wide Applications for appropriate permissions (Automated)	1		Passed					Script	All System Wide Applications have appropriate permissions	Script > sudo chmod -R o-w /Applications/<applicationname>
5.1.3 Check System folder for world writable files (Automated)	1		Passed					Script	All System folder for world are not writable files	Script > sudo chmod -R o-w /Path/<baddirectory>
5.1.4 Check Library folder for world writable files (Automated)	2		Passed					Script	All Library folder for world are not writable files	Script > sudo chmod -R o-w /System/Volumes/Data/Library/<baddirectory>
5.3 Reduce the sudo timeout period (Automated)	1		Passed					Script	The sudo timeout period is reduced	Script > echo "Defaults timestamp_timeout=0" >> /etc/sudoers
5.4 Automatically lock the login keychain for inactivity (Manual)	2		Passed					Script	Automatically lock the login keychain for inactivity: Enabled	Script > sudo -i <username> security set-keychain-settings -t 21600 /Users/<username>/Library/Keychains/login.keychain

Audit Number	Level	Scoring	Result	Managed	Preference domain	Option
1.1 Verify all Apple-provided software is current (Automated)	1		Passed			
1.2 Enable Auto Update (Automated)	1		Passed	FALSE	com.apple.SoftwareUpdate	AutomaticCheckEnabled
1.3 Enable Download new updates when available (Automated)	1		Passed	FALSE	com.apple.SoftwareUpdate	AutomaticDownload
1.4 Enable app update installs (Automated)	1		Passed	FALSE	com.apple.commerce	AutoUpdate
1.5 Enable system data files and security updates install (Automated)	1		Failed	FALSE	com.apple.SoftwareUpdate	ConfigDataInstall
1.6 Enable macOS update installs (Automated)	1		Passed	FALSE	com.apple.SoftwareUpdate	AutomaticallyInstallMacOS
2.1.1 Turn off Bluetooth, if no paired devices exist (Automated)	1		Failed			
2.1.2 Show Bluetooth status in menu bar (Automated)	1		Passed	FALSE	com.apple.controlcenter	NSStatusItem Visible Bluetooth
2.2.1 "Enable Set time and date automatically" (Automated)	1		Failed	FALSE	com.apple.timed	TMAutomaticTimeOnlyEnabled
2.2.2 Ensure time set is within appropriate limits (Automated)	1		Passed			
2.3.1 Set an inactivity interval of 20 minutes or less for the screen saver (Automated)	1		Passed	FALSE	com.apple.screensaver	idleTime
2.3.2 Secure screen saver corners (Automated)	2		Failed	FALSE	com.apple.dock	wvous-bl-corner, wvous-bl-corner
2.3.3 Familiarize users with screen lock tools or corner to Start Screen Saver (Manual)	1		Passed	FALSE	com.apple.dock	
2.4.1 Disable Remote Apple Events (Automated)	1		Passed			
2.4.2 Disable Internet Sharing (Automated)	1		Passed			
2.4.3 Disable Screen Sharing (Automated)	1		Passed			
2.4.4 Disable Printer Sharing (Automated)	1		Passed			
2.4.5 Disable Remote Login (Automated)	1		Passed			
2.4.6 Disable DVD or CD Sharing (Automated)	1		Passed			
2.4.7 Disable Bluetooth Sharing (Automated)	1		Passed	FALSE	com.apple.Bluetooth	PrefKeyServicesEnabled
2.4.8 Disable File Sharing (Automated)	1		Passed			
2.4.9 Disable Remote Management (Automated)	1		Passed			

	Remediate
	Script > sudo /usr/sbin/softwareupdate --install --restart --recommended
	Configuration profile - payload > com.apple.SoftwareUpdate > AutomaticCheckEnabled=true
	Configuration profile - payload > com.apple.SoftwareUpdate > AutomaticDownload=true
	Configuration profile - payload > com.apple.SoftwareUpdate > AutomaticallyInstallAppUpdates=true
oled	Configuration profile - payload > com.apple.SoftwareUpdate > ConfigDataInstall=true - CriticalUpdateInstall=true
	Configuration profile - payload > com.apple.SoftwareUpdate > AutomaticallyInstallMacOSUpdates=true)
	Script - defaults write /Library/Preferences/com.apple.Bluetooth ControllerPowerState -bool false
	Script > sudo -u firstuser defaults -currentHost write com.apple.controlcenter.plist Bluetooth -int 18
	Configuration profile - payload > com.apple.timed > TMAutomaticTimeOnlyEnabled=true
	Script > sudo /usr/sbin/systemsetup -setusingnetworktime on && sudo /usr/sbin/systemsetup -setnetworktimeserver time.euro.apple.com
	Configuration profile - payload > com.apple.screensaver > idleTime=1200
	Configuration profile - payload > com.apple.dock > wvous-tl-corner=5, wvous-br-corner=10, wvous-bl-corner=13, wvous-tr-corner=0 - 5=Start Screen Saver, 10=Put Display to Sleep, 13=Lock Screen
Corners	Familiarise users with screen lock tools or corner to Start Screen Saver
	Script > sudo /usr/sbin/systemsetup -setremoteappleevents off && sudo launchctl disable system/com.apple.AEServer
	Configuration profile - payload > com.apple.MCX > forceInternetSharingOff=true
	Script > sudo launchctl disable system/com.apple.screensharing
	Script > sudo /usr/sbin/cupsctl --no-share-printers
	Script > sudo /usr/sbin/systemsetup -setremotelogin off
	Script > sudo launchctl unload -w /System/Library/LaunchDaemons/com.apple.ODSAgent.plist
	Script > sudo -u 'CURRENT_USER' defaults -currentHost write com.apple.Bluetooth PrefKeyServicesEnabled -bool false
	Script > sudo launchctl disable system/com.apple.smbd
	Script > sudo launchctl disable system/com.apple.smbd



Audit

Report



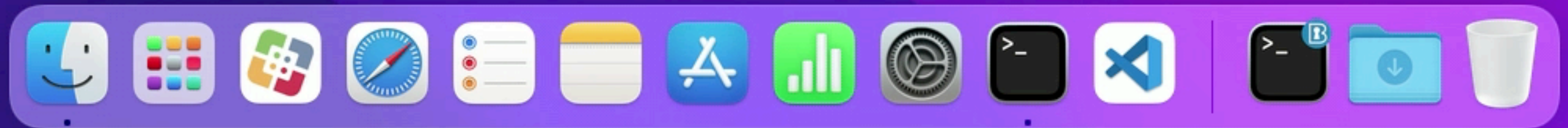
Audit

Remediate

Report

mischa@MBAir CIS-Script %

I



CISBenchmarkReport

Audit Number	Level	Scoring	Result	Managed	Method	Comments
1.1 Verify all Apple-provided software is current (Automated)	1		Passed		Script	Apple Software is Current
1.2 Enable Auto Update (Automated)	1		Passed	FALSE	Profile	Auto Update: Enabled
1.3 Enable Download new updates when available (Automated)	1		Passed	FALSE	Profile	Download new updates when available: Enabled
1.4 Enable app update installs (Automated)	1		Passed	FALSE	Profile	App updates: Enabled
1.5 Enable system data files and security updates install (Automated)	1		Failed	FALSE	Profile	System data files and security update installs: Disabled
1.6 Enable macOS update installs (Automated)	1		Passed	FALSE	Profile	macOS update installs: Enabled
2.1.1 Turn off Bluetooth, if no paired devices exist (Automated)	1		Passed After Remediation		Script	No Paired Devices
2.1.2 Show Bluetooth status in menu bar (Automated)	1		Passed	FALSE	Script	Show Bluetooth status in menu bar: Enabled
2.2.1 "Enable Set time and date automatically" (Automated)	1		Failed	FALSE	Profile	Time and date automatically: Disabled
2.2.2 Ensure time set is within appropriate limits (Automated)	1		Passed		Script	Network Time Server: time.euro.apple.com
2.3.1 Set an inactivity interval of 20 minutes or less for the screen saver (Automated)	1		Passed	FALSE	Profile	Inactivity interval for the screen saver: 1200
2.3.2 Secure screen saver corners (Automated)	2		Failed	FALSE	Profile	Secure screen saver corners: Disabled
2.3.3 Familiarize users with screen lock tools or corner to Start Screen Saver (Manual)	1		Passed	FALSE	Manual	End-users are familiar with screen lock tools or Hot Corners
2.4.1 Disable Remote Apple Events (Automated)	1		Passed		Script	Remote Apple Events: Disabled
2.4.2 Disable Internet Sharing (Automated)	1		Passed		Profile	Internet Sharing: Disabled
2.4.3 Disable Screen Sharing (Automated)	1		Passed		Script	Screen Sharing: Disabled
2.4.4 Disable Printer Sharing (Automated)	1		Passed		Script	Printer Sharing: Disabled
2.4.5 Disable Remote Login (Automated)	1		Passed		Script	Remote Login: Disabled
2.4.6 Disable DVD or CD Sharing (Automated)	1		Passed		Script	DVD or CD Sharing: Disabled
2.4.7 Disable Bluetooth Sharing (Automated)	1		Passed	FALSE	Script	Bluetooth Sharing: Disabled
2.4.8 Disable File Sharing (Automated)	1		Passed		Script	File Sharing: Disabled
2.4.9 Disable Remote Management (Automated)	1		Passed		Script	Remote Management: Disabled
2.4.10 Disable Content Caching (Automated)	2		Passed	FALSE	Profile	Content Caching: Disabled
2.4.11 Disable Media Sharing (Automated)	1		Failed	FALSE	Profile	Media Sharing: Enabled

```
> ./CISBenchmarkScript.sh --help
```

The following options are available:

-f	--fullreport	Print Full Report
-h	--help	Displays this message or details on a specific verb
-r	--remediate	Enable Remediation

EXAMPLES

```
./CISBenchmarkScript.sh  
Run script to print Short Report
```

```
./CISBenchmarkScript.sh -f  
Run script to print Full Report
```








```
./CISBenchmarkScript.sh -r  
Run script with Remediation enabled
```

```
./CISBenchmarkScript.sh -rf  
Run script with Remediation enabled and print Full Report
```

How the script is built



CIS Script

-  Assemble.sh
-  Build
-  **Fragments**
-  Jamf
-  LICENSE
-  README.md
-  Utils



CIS Script

 Assemble.sh

 Build

 **Fragments**

 Jamf

 LICENSE

 README.md

 Utils

 Footer.sh

 Header.json

 Header.sh

 **OrgScores**

 Version.sh

```
#!/bin/zsh
```

```
script_dir=$(dirname ${0:A})  
projectfolder=$(dirname $script_dir)
```

```
source ${projectfolder}/Header.sh
```

```
CISLevel="1"  
audit="2.1.1 Turn off Bluetooth, if no paired devices exist (Automated)"  
orgScore="OrgScore2_1_1"  
emptyVariables
```

```
# Verify organizational score  
runAudit  
# If organizational score is 1 or tr  
if [[ "${auditResult}" == "1" ]]; th  
method="Script"  
remediate="Script - defaults wri
```

Audit

```
-bool false"
```

```
connectable=$(system_profiler SPBluetoothDataType 2>&1 | grep -c "Connected: Yes")  
bluetoothEnabled=$(system_profiler SPBluetoothDataType 2>&1 | grep -c "State: On")  
comment="Paired Devices: ${conne  
# if [[ "$connectable" == 0 ]] &  
if [[ "$connectable" -gt 0 ]] &&  
result="Passed"  
else  
result="Failed"  
comment="No Paired Devices"
```

Remediate

```
[[ "$bluetoothEnabled" == 0 ]]; then
```

```
# Remediation  
if [[ "${remediateResult}" =  
/usr/bin/defaults write  
killall -HUP bluetoothd
```

Report

```
defaultPoweredState off
```

```
# re-check  
bluetoothEnabled=$(system_profiler SPBluetoothDataType 2>&1 | grep -c "State: On")  
if [[ "$bluetoothEnabled" == 0 ]]; then  
result="Passed After Remediation"  
else  
result="Failed After Remediation"  
fi
```

```
fi
```

```
fi
```

```
fi
```

```
printReport
```

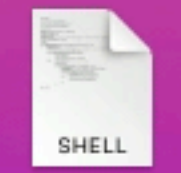


Custom rules

CIS-Script/Fragments/OrgScores

Demo

mischa@MBAir CIS-Script %



OrgScore6_4.sh



```
> ./Assemble.sh --help
```

The following options are available:

```
-h      --help      Displays this message or details on a specific verb
-j      --json      Builds Jamf Pro Custom Schema.json file
-s      --separate  Builds separate CIS Benchmark Script from the fragments
```

EXAMPLES

```
./Assemble.sh
Builds CIS Benchmark Script from the fragments

./Assemble.sh -j
Builds Jamf Pro Custom Schema.json file

./Assemble.sh -s
Builds separate CIS Benchmark Script from the fragments
```



**macOS
Big Sur**



**macOS
Monterey**

Implementation

INVENTORY

- Search Inventory
- Search Volume Content
- Licensed Software

CONTENT MANAGEMENT

- Policies
- Configuration Profiles**
- Restricted Software
- PreStage Imaging
- Mac App Store Apps
- Patch Management
- eBooks

GROUPS

- Smart Computer Groups
- Static Computer Groups
- Classes

ENROLLMENT

- Enrollment Invitations
- PreStage Enrollments

SETTINGS

- Management Settings

Computers
Configuration Profiles

> 🔍 Filter Pr 1 - 75 of 75

+ New Upload ☰ ☱

NAME	LOGS	COMPLETED	PENDING	FAILED	SCOPE
> Certificates					
▼ CIS Benchmark					
CIS Benchmark Settings	View	1	0	0	CIS Benchmark
Disable automatic login	View	1	0	0	CIS Benchmark
Disable Bonjour advertising service	View	1	0	0	CIS Benchmark
Disable Content Caching	View	1	0	0	CIS Benchmark
Disable Fast User Switching	View	1	0	0	CIS Benchmark
Disable Guest Access	View	1	0	0	CIS Benchmark
Disable Internet Sharing	View	1	0	0	CIS Benchmark
Disable Media Sharing	View	1	0	0	CIS Benchmark
Disable Personalized Advertising	View	1	0	0	CIS Benchmark
Disable sending diagnostic and usage data to Apple	View	1	0	0	CIS Benchmark
Disable the automatic run of safe files in Safari	View	1	0	0	CIS Benchmark
Disabled iCloud Functions	View	1	0	0	CIS Benchmark
enable Lock Screen	View	1	0	0	CIS Benchmark
Ensure time set is within appropriate limits	View	0	0	0	No scope defined
Login Window	View	1	0	0	CIS Benchmark
Passcode	View	1	0	0	CIS Benchmark
Passcode Extra	View	1	0	0	CIS Benchmark
Screen Saver	View	1	0	0	CIS Benchmark
Secure Keyboard Entry	View	1	0	0	CIS Benchmark

← CIS-Script

General Script Options Limitations

Script Contents

Shell Dracula

-T T+ Commands

VERSION
10.38.3-t1653338998
MANAGED
Computers: 2
Mobile Devices: 2
UNMANAGED
Computers: 0
Mobile Devices: 1

```

1 #!/bin/zsh
2
3 VERSION="1.1"
4 VERSIONDATE="2021-09-23"
5
6 #####
7 # License information
8 #####
9 #
10 # THE SCRIPTS ARE PROVIDED "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES,
11 # INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY
12 # AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL
13 # I BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY,
14 # OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
15 # SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
16 # INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
17 # CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
18 # ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF
19 # THE POSSIBILITY OF SUCH DAMAGE.
20 #
21 #####
22 #####
23 #
24 # Written by: Mischa van der Bent
25 #
26 # DESCRIPTION
27 # This script is inspired by the CIS Benchmark script of Jamf Professional Services
28 # https://github.com/jamf/CIS-for-macOS-Catalina-CP
29 # And will look for a managed Configuration Profile (com.cis.benchmark.plist) and checks,
30 # remediation (if needend) and report.
31 # The Security Score can be set with the Jamf Pro Custom Schema json file.
32 # Reports are stored in /Library/Security/Reports.
33 #
34 # REQUIREMENTS
35 # Compatible with Big Sure macOS 11.x
36 # Compatible with Monterey macOS 12.x
37 #
38 #####
39 #####
40
41 export PATH=/usr/bin:/bin:/usr/sbin:/sbin
42
43 #####
44 # Directory/Path/Variables
45 #####
46
47 CISBenchmarkReportPath="/Library/Security/Reports"
48 CISBenchmarkReport=${CISBenchmarkReportPath}/CISBenchmarkReport.csv
49 plistlocation="/Library/Managed Preferences/com.cis.benchmark.plist"
50 currentUser=$(scutil <<< "show State:/Users/ConsoleUser" | awk '/Name :/ { print $3 }')
51
52 #####
53 # Functions
54 #####
55
56 function help(){
57 echo
58 echo "The following options are available:"
59 echo
60 echo " -f --fullreport Print Full Report"
61 echo " -h --help Displays this message or details on a specific verb"
62 echo " -r --remediate Enable Remediation"
63 echo
64 echo "EXAMPLES"
65 echo " ./CISBenchmarkScript.sh -f"
66 echo " Run script to print Full Report"
67 echo
68 echo " ./CISBenchmarkScript.sh -r"
69 echo " Run script with Remediation enabled"

```

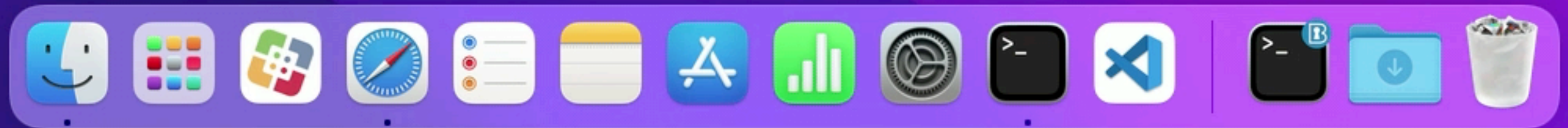


Configure

Jamf Pro Custom Schema.json

Demo

mischa@MBAir CIS-Script %



← Extension Attributes

+ New + New From Template Upload

NAME

- CIS-Script Failed
- CIS-Script Failed - List
- CIS-Script Failed After Remediation
- CIS-Script Failed After Remediation - List
- CIS-Script Not applicable
- CIS-Script Not applicable - List
- CIS-Script Notice
- CIS-Script Notice - List
- CIS-Script Passed
- CIS-Script Passed After Remediation
- CIS-Script Passed After Remediation - List
- CIS-Script Scored

VERSION
10.38.3-t1653338998

MANAGED
Computers: 2
Mobile Devices: 2

UNMANAGED
Computers: 0
Mobile Devices: 1

- INVENTORY
 - Search Inventory
 - Search Volume Content
 - Licensed Software
- CONTENT MANAGEMENT
 - Policies**
 - Configuration Profiles
 - Restricted Software
 - PreStage Imaging
 - Mac App Store Apps
 - Patch Management
 - eBooks
- GROUPS
 - Smart Computer Groups
 - Static Computer Groups
 - Classes
- ENROLLMENT
 - Enrollment Invitations
 - PreStage Enrollments
- SETTINGS
 - Management Settings

- General
- Packages (0 Packages)
- Software Updates (Not Configured)
- Scripts (1 Script)**
- Printers (0 Printers)
- Disk Encryption (Not Configured)
- Dock Items (0 Dock Items)
- Local Accounts (0 Accounts)
- Management Accounts (Not Configured)
- Directory Bindings (0 Bindings)
- EFI Password (Not Configured)
- Restart Options (Not Configured)
- Maintenance (Configured)
- Files and Processes (Not Configured)
- macOS Intune Integration (Not Configured)

General

Display Name Display name for the policy

CIS Benchmark

Enabled

Category Category to add the policy to

CIS Benchmark

Trigger Event(s) to use to initiate the policy

- Startup
When a computer starts up. A startup script that checks for policies must be configured in Jamf Pro for this to work
- Login
When a user logs in to a computer. A login hook that checks for policies must be configured in Jamf Pro for this to work
- Logout
When a user logs out of a computer. A logout hook that checks for policies must be configured in Jamf Pro for this to work
- Network State Change
When a computer's network state changes (e.g., when the network connection changes, when the computer name changes, when the IP address changes)
- Enrollment Complete
Immediately after a computer completes the enrollment process
- Recurring Check-in**
At the recurring check-in frequency configured in Jamf Pro
- Custom
At a custom event

Execution Frequency Frequency at which to run the policy

Once every day

Target Drive The drive on which to run the policy (e.g. "/Volumes/Restore/"). The policy runs on the boot drive by default

/

Server-Side Limitations

Client-Side Limitations

Server-side limitations are enforced based on the settings on the Jamf Pro host server

Activation Date/Time Date/time to make the policy active

-- / -- / ---- at -- : -- --

Expiration Date/Time Date/time to make the policy expire

-- / -- / ---- at -- : -- --

- INVENTORY
 - Search Inventory
 - Search Volume Content
 - Licensed Software
- CONTENT MANAGEMENT
 - Policies
 - Configuration Profiles
 - Restricted Software
 - PreStage Imaging
 - Mac App Store Apps
 - Patch Management
 - eBooks
- GROUPS
 - Smart Computer Groups
 - Static Computer Groups
 - Classes
- ENROLLMENT
 - Enrollment Invitations
 - PreStage Enrollments
- SETTINGS
 - Management Settings

- General CISMACSYSADMIN
- Hardware MacBook Air (Retina, 13-inch, 2019)
- Operating System macOS 11.6.0
- User and Location mischa
- Security
- Purchasing
- Storage 1 Drive
- Extension Attributes
- Disk Encryption Encrypted
- Applications 60 Applications
- Plug-ins 0 Plug-ins
- Profiles 33 Profiles
- Certificates 5 Certificates
- Package Receipts 12 Receipts
- Software Updates 0 Updates
- Local User Accounts 1 Account
- Printers 0 Printers

MDM Capability:	Yes
Enrolled via Automated Device Enrollment:	Yes
User Approved MDM:	Yes
MDM Capable Users:	mischa
Jamf Pro Computer ID:	50
Asset Tag:	
Bar Code 1:	
Bar Code 2:	
Bluetooth Low Energy Capability:	Capable
Supports iOS and iPadOS App Installations:	No
Logged in to the App Store:	Not Active

Extension Attributes

CIS-Script Failed:	0
CIS-Script Failed - List:	
CIS-Script Failed After Remediation:	0
CIS-Script Failed After Remediation - List:	
CIS-Script Not applicable:	2
CIS-Script Not applicable - List:	2.5.1.3 Ensure all user storage CoreStorage volumes are encrypted (Manual) 2.11 Ensure EFI version is valid and being regularly checked (Automated)
CIS-Script Notice:	1
CIS-Script Notice - List:	2.5.5 Monitor Location Services Access (Manual)
CIS-Script Passed:	76
CIS-Script Passed After Remediation:	1
CIS-Script Passed After Remediation - List:	2.1.1 Turn off Bluetooth, if no paired devices exist (Automated)
CIS-Script Scored:	80

INVENTORY

- 🔍 Search Inventory
 - 📄 Search Volume Content
 - 🔑 Licensed Software
- CONTENT MANAGEMENT
- 📄 Policies
 - ⚙️ Configuration Profiles
 - 🛡️ Restricted Software
 - 📄 PreStage Imaging
 - 📄 Mac App Store Apps
 - 📄 Patch Management
 - 📄 eBooks

GROUPS

- 📁 Smart Computer Groups
- 📁 Static Computer Groups
- 👤 Classes

ENROLLMENT

- 📄 Enrollment Invitations
- 📄 PreStage Enrollments

SETTINGS

- ⚙️ Management Settings

Inventory Management History

- 📄 User and Location
mischa
- 🔒 Security
- 🌐 Purchasing
- 💾 Storage
1 Drive
- 📄 Extension Attributes
- 🔒 Disk Encryption
Encrypted
- 📄 Applications
60 Applications
- 🛡️ Plug-ins
0 Plug-ins
- ⚙️ Profiles
33 Profiles
- 📄 Certificates
5 Certificates
- 📄 Package Receipts
12 Receipts
- 🔄 Software Updates
0 Updates
- 👤 Local User Accounts
1 Account
- 🖨️ Printers
0 Printers
- ⚙️ Services
360 Services
- 📎 Attachments
1 Attachment
- 📄 Content Caching

Attachments

📄 Upload

NAME	SIZE	
CISBenchmarkReport.csv	8 KB	Delete



Apple Security Certifications and Compliance Centre

support.apple.com/en-gb/guide/sccc/



macOS Security Compliance

github.com/usnistgov/macOS_security



CIS Script

github.com/mvdbent/CIS-Script



@mvdbent

[#macOS_security_compliance](#) [#security](#)

Recap

1 | macOS Security

Have a look what Apple has been doing on the security stack and build into the system.

2 | Security Benchmarks

Organisations that provide guidance of the Security standard depending on industry and/or geo-location.

3 | Scripts

How we can use the CIS-Script to help you to audit, remediate and report based on the Benchmark rules.

4 | Implementation

See how easy it is to deploy the CIS script in your environment.

A woman in a business setting is shown in profile, focused on her work. She is using a laptop and a tablet. In the background, other people are visible, suggesting a collaborative office environment. The entire image is overlaid with a semi-transparent purple gradient.

Thank You!

Questions?