



macOS Security Compliance

macOS 14.0

Security Configuration - SystemSettingsRules

Sonoma Guidance, Revision 2.0 (2024-04-24)

Table of Contents

1. Foreword	1
2. Scope	2
3. Authors	3
4. Acronyms and Definitions	4
5. Applicable Documents	6
5.1. Government Documents	6
5.2. Non-Government Documents	6
6. System Settings	7
6.1. Disable Airplay Receiver	7
6.2. Disable Unattended or Automatic Logon to the System	8
6.3. Enable Bluetooth Menu	9
6.4. Disable Bluetooth Sharing	10
6.5. Disable CD/DVD Sharing	11
6.6. Enforce Critical Security Updates to be Installed	11
6.7. Enforce FileVault	12
6.8. Enable macOS Application Firewall	13
6.9. Enable Firewall Stealth Mode	14
6.10. Disable Guest Access to Shared SMB Folders	15
6.11. Disable the Guest Account	16
6.12. Enforce macOS Updates are Automatically Installed	17
6.13. Disable Internet Sharing	18
6.14. Configure Login Window to Show A Custom Message	19
6.15. Configure Login Window to Prompt for Username and Password	20
6.16. Disable Password Hints	20
6.17. Disable Personalized Advertising	21
6.18. Disable Printer Sharing	22
6.19. Disable Remote Apple Events	23
6.20. Disable Remote Management	24
6.21. Disable Screen Sharing and Apple Remote Desktop	24
6.22. Enforce Session Lock After Screen Saver is Started	25
6.23. Enforce Screen Saver Timeout	26
6.24. Disable Server Message Block Sharing	27
6.25. Enforce Software Update App Update Updates Automatically	28
6.26. Enforce Software Update Downloads Updates Automatically	29
6.27. Enforce Software Update Automatically	30
6.28. Ensure Software Update is Updated and Current	30
6.29. Disable SSH Server for Remote Access Sessions	31
6.30. Require Administrator Password to Modify System-Wide Preferences	32

6.31. Ensure Time Machine Volumes are Encrypted	34
6.32. Configure macOS to Use an Authorized Time Server	35
6.33. Enforce macOS Time Synchronization	36
6.34. Ensure Wake for Network Access Is Disabled	37
6.35. Enable Wifi Menu	38

Chapter 1. Foreword

The macOS Security Compliance Project is an open source effort to provide a programmatic approach to generating security guidance. The configuration settings in this document were derived from National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Security and Privacy Controls for Information Systems and Organizations*, Revision 5.

This project can be used as a resource to easily create customized security baselines of technical security controls by leveraging a library of atomic actions which are mapped to the compliance requirements defined in NIST SP 800-53 (Rev. 5). It can also be used to develop customized guidance to meet the particular cybersecurity needs of any organization.

The objective of this effort was to simplify and radically accelerate the process of producing up-to-date macOS security guidance that is also accessible to any organization and tailorable to meet each organization's specific security needs.

Any and all risk based decisions to tailor the content produced by this project in order to meet the needs of a specific organization shall be approved by the responsible Information System Owner (ISO) and Authorizing Official (AO) and formally documented in their System Security Plan (SSP). While the project attempts to provide settings to meet compliance requirements, it is recommended that each rule be reviewed by your organization's Information System Security Officer (ISSO) prior to implementation.

Chapter 2. Scope

This guide describes the actions to take when securing a macOS 14.0 system against the SystemSettingsRules (Tailored from CIS_LVL1) security baseline.

Chapter 3. Authors

macOS Security Compliance Project

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

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

Chapter 4. Acronyms and Definitions

Table 1. Acronyms and Abbreviations

AES	Advanced Encryption Standard
ABM	Apple Business Manager
AFP	Apple Filing Protocol
ALF	Application Layer Firewall
AO	Authorizing Official
API	Application Programming Interface
ARD	Apple Remote Desktop
CA	Certificate Authority
CIS	Center for Internet Security
CMMC	Cybersecurity Maturity Model Certification
CNSSI	Committee on National Security Systems
CRL	Certificate Revocation List
DISA	Defense Information Systems Agency
DMA	Direct Memory Access
FISMA	Federal Information Security Modernization Act
FPKI	Federal Public Key Infrastructure
IR	Infrared
ISO	Information System Owner
ISSO	Information System Security Officer
MDM	Mobile Device Management
NASA	National Aeronautics and Space Administration
NFS	Network File System
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OCSP	Online Certificate Status Protocol
ODV	Organization Defined Values
OS	Operating System
PF	Packet Filter
PIV	Personal Identity Verification
PIV-M	Personal Identity Verification Mandatory
PKI	Public Key Infrastructure
RBD	Risk Based Decision

SIP	System Integrity Protection
SMB	Server Message Block
SSH	Secure Shell
SSP	System Security Plan
STIG	Security Technical Implementation Guide
UAMDM	User Approved MDM
UUCP	Unix-to-Unix Copy Protocol

Table 2. Definitions

Baseline	A baseline is a predefined set of controls (also referred to as "a catalog" of settings) that address the protection needs of an organization's information systems. A baseline serves as a starting point for the creation of security benchmarks.
Benchmark	Benchmarks are a defined list of settings with values that an organization has defined.

Chapter 5. Applicable Documents

5.1. Government Documents

Table 3. National Institute of Standards and Technology (NIST)

Document Number or Descriptor	Document Title
NIST Special Publication 800-53 Rev 5	<i>NIST Special Publication 800-53 Rev 5</i>
NIST Special Publication 800-63	<i>NIST Special Publication 800-63</i>
NIST Special Publication 800-171	<i>NIST Special Publication 800-171 Rev 2</i>
NIST Special Publication 800-219	<i>NIST Special Publication 800-219 Rev 1</i>

Table 4. Defense Information Systems Agency (DISA)

Document Number or Descriptor	Document Title
STIG Ver 1, Rel 1	<i>Apple macOS 14 (Sonoma) STIG</i>

Table 5. Cybersecurity Maturity Model Certification (CMMC)

Document Number or Descriptor	Document Title
CMMC Model Overview v2.0	<i>Cybersecurity Maturity Model Certification (CMMC) Model Overview v2.0</i>

Table 6. Committee on National Security Systems (CNSS)

Document Number or Descriptor	Document Title
CNSSI No. 1253	<i>Security Categorization and Control Selection for National Security Systems</i>

5.2. Non-Government Documents

Table 7. Apple

Document Number or Descriptor	Document Title
Apple Platform Security Guide	<i>Apple Platform Security</i>
Apple Platform Deployment	<i>Apple Platform Deployment</i>
Apple Platform Certifications	<i>Apple Platform Certifications</i>
Profile-Specific Payload Keys	<i>Profile-Specific Payload Keys</i>

Table 8. Center for Internet Security

Document Number or Descriptor	Document Title
Apple macOS 14.0	<i>CIS Apple macOS 14.0 Benchmark version 1.0.0</i>

Chapter 6. System Settings

This section contains the configuration and enforcement of the settings within the macOS System Settings application.



The check/fix commands outlined in this section *MUST* be run by a user with elevated privileges.

6.1. Disable Airplay Receiver

Airplay Receiver allows you to send content from another Apple device to be displayed on the screen as it's being played from your other device.

Support for Airplay Receiver is non-essential and *MUST* be disabled.

The information system *MUST* be configured to provide only essential capabilities.

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

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\
.objectForKey('allowAirPlayIncomingRequests').js
EOS
```

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

Remediation Description

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

Create a configuration profile containing the following keys in the (com.apple.applicationaccess) payload type:

```
<key>allowAirPlayIncomingRequests</key>
<false/>
```

ID	system_settings_airplay_receiver_disable
----	--

References	800-53r5	<ul style="list-style-type: none">• CM-7, CM-7(1)
	CIS	<ul style="list-style-type: none">• 2.3.1.2 (level 1)
	Benchmark	
	CIS Controls V8	<ul style="list-style-type: none">• 4.1• 4.8
	CCE	<ul style="list-style-type: none">• CCE-92944-8

6.2. Disable Unattended or Automatic Logon to the System

Automatic logon *MUST* be disabled.

When automatic logons are enabled, the default user account is automatically logged on at boot time without prompting the user for a password. Even if the screen is later locked, a malicious user would be able to reboot the computer and find it already logged in. Disabling automatic logons mitigates this risk.

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

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.loginwindow')\
.objectForKey('com.apple.login.mcx.DisableAutoLoginClient').js
EOS
```

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

Remediation Description

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

Create a configuration profile containing the following keys in the (com.apple.loginwindow) payload type:

```
<key>com.apple.login.mcx.DisableAutoLoginClient</key>
<true/>
```

ID	system_settings_automatic_login_disable
----	---

References	800-53r5	<ul style="list-style-type: none">• IA-2• IA-5(13)
	CIS Benchmark	<ul style="list-style-type: none">• 2.12.3 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 4.7
	CCE	<ul style="list-style-type: none">• CCE-92947-1

6.3. Enable Bluetooth Menu

The bluetooth menu *MUST* be enabled.

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

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.controlcenter')\
.objectForKey('Bluetooth').js
EOS
```

If the result is not **18**, this is a finding.

Remediation Description

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

Create a configuration profile containing the following keys in the (com.apple.controlcenter) payload type:

```
<key>Bluetooth</key>
<integer>18</integer>
```

ID	system_settings_bluetooth_menu_enable	
References	800-53r5	<ul style="list-style-type: none">• N/A
	CIS Benchmark	<ul style="list-style-type: none">• 2.4.2 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 4.8• 13.9
	CCE	<ul style="list-style-type: none">• CCE-92950-5

6.4. Disable Bluetooth Sharing

Bluetooth Sharing *MUST* be disabled.

Bluetooth Sharing allows users to wirelessly transmit files between the macOS and Bluetooth-enabled devices, including personally owned cellphones and tablets. A malicious user might introduce viruses or malware onto the system or extract sensitive files via Bluetooth Sharing. When Bluetooth Sharing is disabled, this risk is mitigated.



The check and fix are for the currently logged in user. To get the currently logged in user, run the following.

```
CURRENT_USER=$( /usr/sbin/scutil <<< "show State:/Users/ConsoleUser" |  
/usr/bin/awk '/Name :/ && ! /loginwindow/ { print $3 }' )
```

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

```
/usr/bin/sudo -u "$CURRENT_USER" /usr/bin/defaults -currentHost read  
com.apple.Bluetooth PrefKeyServicesEnabled
```

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

Remediation Description

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

```
/usr/bin/sudo -u "$CURRENT_USER" /usr/bin/defaults -currentHost write  
com.apple.Bluetooth PrefKeyServicesEnabled -bool false
```

ID	system_settings_bluetooth_sharing_disable	
References	800-53r5	<ul style="list-style-type: none">AC-18(4)AC-3CM-7, CM-7(1)
	CIS Benchmark	<ul style="list-style-type: none">2.3.3.11 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">3.34.1
	CCE	<ul style="list-style-type: none">CCE-92952-1

6.5. Disable CD/DVD Sharing

CD/DVD Sharing *MUST* be disabled.

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

```
/usr/bin/pgrep -q ODSSAgent; /bin/echo $?
```

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

Remediation Description

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

```
/bin/launchctl unload /System/Library/LaunchDaemons/com.apple.ODSSAgent.plist
```

ID	system_settings_cd_dvd_sharing_disable	
References	800-53r5	• CM-7, CM-7(1)
	CIS Benchmark	• 2.3.3.1 (level 1)
	CIS Controls V8	• 4.1
		• 4.8
	CCE	• CCE-92953-9

6.6. Enforce Critical Security Updates to be Installed

Ensure that security updates are installed as soon as they are available from Apple.

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

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.SoftwareUpdate')\
.objectForKey('CriticalUpdateInstall').js
EOS
```

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

Remediation Description

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

Create a configuration profile containing the following keys in the (com.apple.SoftwareUpdate) payload type:

```
<key>CriticalUpdateInstall</key>
<true/>
```

ID	system_settings_critical_update_install_enforce	
References	800-53r5	• SI-2
	CIS Benchmark	• 1.6 (level 1)
	CIS Controls V8	• 7.3
		• 7.4
		• 7.7
	CCE	• CCE-92955-4

6.7. Enforce FileVault

FileVault *MUST* be enforced.

The information system implements cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.

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

```
dontAllowDisable=$(/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.MCX')\
.objectForKey('dontAllowFEDisable').js
EOS
)
fileVault=$(/usr/bin/fdesetup status | /usr/bin/grep -c "FileVault is On.")
if [[ "$dontAllowDisable" == "true" ]] && [[ "$fileVault" == 1 ]]; then
    echo "1"
else
    echo "0"
fi
```

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

Remediation Description

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

Create a configuration profile containing the following keys in the (com.apple.MCX) payload

type:

```
<key>dontAllowFDEDisable</key>
<true/>
```

ID	system_settings_filevault_enforce	
References	800-53r5	• SC-28, SC-28(1)
	CIS Benchmark	• 2.6.6 (level 1)
	CIS Controls V8	• 3.6
		• 3.11
	CCE	• CCE-92957-0

6.8. Enable macOS Application Firewall

The macOS Application Firewall is the built-in firewall that comes with macOS, and it *MUST* be enabled.

When the macOS Application Firewall is enabled, the flow of information within the information system and between interconnected systems will be controlled by approved authorizations.

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

```
profile="$(/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.security.firewall')\
.objectForKey('EnableFirewall').js
EOS
)"

plist="$(/usr/bin/defaults read /Library/Preferences/com.apple.alf globalstate
2>/dev/null)"

if [[ "$profile" == "true" ]] && [[ "$plist" =~ [1,2] ]]; then
    echo "true"
else
    echo "false"
fi
```

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

Remediation Description

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

Create a configuration profile containing the following keys in the (com.apple.security.firewall) payload type:

```
<key>EnableFirewall</key>
<true/>
```

ID	system_settings_firewall_enable	
References	800-53r5	<ul style="list-style-type: none">• AC-4• CM-7, CM-7(1)• SC-7, SC-7(12)
	CIS Benchmark	<ul style="list-style-type: none">• 2.2.1 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 4.1• 4.5• 13.1
	CCE	<ul style="list-style-type: none">• CCE-92959-6

6.9. Enable Firewall Stealth Mode

Firewall Stealth Mode *MUST* be enabled.

When stealth mode is enabled, the Mac will not respond to any probing requests, and only requests from authorized applications will still be authorized.



Enabling firewall stealth mode may prevent certain remote mechanisms used for maintenance and compliance scanning from properly functioning. Information System Security Officers (ISSOs) are advised to first fully weigh the potential risks posed to their organization before opting not to enable stealth mode.

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

```
profile="$(/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.security.firewall')\
.objectForKey('EnableStealthMode').js
EOS
)"

plist=$(/usr/bin/defaults read /Library/Preferences/com.apple.alf stealthenabled
2>/dev/null)

if [[ "$profile" == "true" ]] && [[ $plist == 1 ]]; then
  echo "true"
```

```
else
  echo "false"
fi
```

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

Remediation Description

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

Create a configuration profile containing the following keys in the (com.apple.security.firewall) payload type:

```
<key>EnableStealthMode</key>
<true/>
<key>EnableFirewall</key>
<true/>
```

ID	system_settings_firewall_stealth_mode_enable	
References	800-53r5	<ul style="list-style-type: none">• CM-7, CM-7(1)• SC-7, SC-7(16)
	CIS Benchmark	<ul style="list-style-type: none">• 2.2.2 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 4.1• 4.5• 4.8
	CCE	<ul style="list-style-type: none">• CCE-92960-4

6.10. Disable Guest Access to Shared SMB Folders

Guest access to shared Server Message Block (SMB) folders *MUST* be disabled.

Turning off guest access prevents anonymous users from accessing files shared via SMB.

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

```
/usr/bin/defaults read /Library/Preferences/SystemConfiguration/com.apple.smb.server
AllowGuestAccess
```

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

Remediation Description

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

```
/usr/sbin/sysadminctl -smbGuestAccess off
```

ID	system_settings_guest_access_smb_disable	
References	800-53r5	• AC-2, AC-2(9)
	CIS Benchmark	• 2.12.2 (level 1)
	CIS Controls V8	• 3.3
	CCE	• CCE-92963-8

6.11. Disable the Guest Account

Guest access *MUST* be disabled.

Turning off guest access prevents anonymous users from accessing files.

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

```
/usr/bin/osascript -l JavaScript << EOS
function run() {
  let pref1 = ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.MCX')\
.objectForKey('DisableGuestAccount'))
  let pref2 = ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.MCX')\
.objectForKey('EnableGuestAccount'))
  if ( pref1 == true && pref2 == false ) {
    return("true")
  } else {
    return("false")
  }
}
EOS
```

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

Remediation Description

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

Create a configuration profile containing the following keys in the (com.apple.MCX) payload

type:

```
<key>DisableGuestAccount</key>
<true/>
<key>EnableGuestAccount</key>
<false/>
```

ID	system_settings_guest_account_disable	
References	800-53r5	• AC-2, AC-2(9)
	CIS Benchmark	• 2.12.1 (level 1)
	CIS Controls V8	• 5.2
		• 6.2
		• 6.8
	CCE	• CCE-92964-6

6.12. Enforce macOS Updates are Automatically Installed

Software Update *MUST* be configured to enforce automatic installation of macOS updates is enabled.

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

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.SoftwareUpdate')\
.objectForKey('AutomaticallyInstallMacOSUpdates').js
EOS
```

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

Remediation Description

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

Create a configuration profile containing the following keys in the (com.apple.SoftwareUpdate) payload type:

```
<key>AutomaticallyInstallMacOSUpdates</key>
<true/>
```

ID	system_settings_install_macos_updates_enforce	
References	800-53r5	<ul style="list-style-type: none">• N/A
	CIS Benchmark	<ul style="list-style-type: none">• 1.4 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 7.3• 7.4
	CCE	<ul style="list-style-type: none">• CCE-92968-7

6.13. Disable Internet Sharing

If the system does not require Internet sharing, support for it is non-essential and *MUST* be disabled.

The information system *MUST* be configured to provide only essential capabilities. Disabling Internet sharing helps prevent the unauthorized connection of devices, unauthorized transfer of information, and unauthorized tunneling.

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

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.MCX')\
.objectForKey('forceInternetSharingOff').js
EOS
```

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

Remediation Description

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

Create a configuration profile containing the following keys in the (com.apple.MCX) payload type:

```
<key>forceInternetSharingOff</key>
<true/>
```

ID	system_settings_internet_sharing_disable
----	--

References	800-53r5	<ul style="list-style-type: none">• AC-20• AC-4
	CIS Benchmark	<ul style="list-style-type: none">• 2.3.3.8 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 4.1• 4.8
	CCE	<ul style="list-style-type: none">• CCE-92971-1

6.14. Configure Login Window to Show A Custom Message

The login window *MUST* be configured to show a custom access warning message.

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

```
/usr/bin/osascript -l JavaScript << EOS | /usr/bin/base64
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.loginwindow')\
.objectForKey('LoginwindowText').js
EOS
```

If the result is not **Center for Internet Security Test Message**, this is a finding.

Remediation Description

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

Create a configuration profile containing the following keys in the (com.apple.loginwindow) payload type:

```
<key>LoginwindowText</key>
<string>Center for Internet Security Test Message</string>
```

ID	system_settings_loginwindow_loginwindowtext_enable	
References	800-53r5	<ul style="list-style-type: none">• N/A
	CIS Benchmark	<ul style="list-style-type: none">• 2.10.3 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 4.1
	CCE	<ul style="list-style-type: none">• CCE-92975-2

6.15. Configure Login Window to Prompt for Username and Password

The login window *MUST* be configured to prompt all users for both a username and a password.

By default, the system displays a list of known users on the login window, which can make it easier for a malicious user to gain access to someone else’s account. Requiring users to type in both their username and password mitigates the risk of unauthorized users gaining access to the information system.

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

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.loginwindow')\
.objectForKey('SHOWFULLNAME').js
EOS
```

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

Remediation Description

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

Create a configuration profile containing the following keys in the (com.apple.loginwindow) payload type:

```
<key>SHOWFULLNAME</key>
<true/>
```

ID	system_settings_loginwindow_prompt_username_password_enforce	
References	800-53r5	• IA-2
	CIS Benchmark	• 2.10.4 (level 1)
	CIS Controls V8	• 4.1
	CCE	• CCE-92976-0

6.16. Disable Password Hints

Password hints *MUST* be disabled.

Password hints leak information about passwords that are currently in use and can lead to loss of confidentiality.

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

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.loginwindow')\
.objectForKey('RetriesUntilHint').js
EOS
```

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

Remediation Description

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

Create a configuration profile containing the following keys in the (com.apple.loginwindow) payload type:

```
<key>RetriesUntilHint</key>
<integer>0</integer>
```

ID	system_settings_password_hints_disable	
References	800-53r5	• IA-6
	CIS Benchmark	• 2.10.5 (level 1)
	CIS Controls V8	• 4.1
	CCE	• CCE-92978-6

6.17. Disable Personalized Advertising

Ad tracking and targeted ads *MUST* be disabled.

The information system *MUST* be configured to provide only essential capabilities. Disabling ad tracking ensures that applications and advertisers are unable to track users' interests and deliver targeted advertisements.

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

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\
.objectForKey('allowApplePersonalizedAdvertising').js
EOS
```

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

Remediation Description

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

Create a configuration profile containing the following keys in the (com.apple.applicationaccess) payload type:

```
<key>allowApplePersonalizedAdvertising</key>
<false/>
```

ID	system_settings_personalized_advertising_disable	
References	800-53r5	<ul style="list-style-type: none">• AC-20• CM-7, CM-7(1)• SC-7(10)
	CIS Benchmark	<ul style="list-style-type: none">• 2.6.4 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 4.8
	CCE	<ul style="list-style-type: none">• CCE-92979-4

6.18. Disable Printer Sharing

Printer Sharing *MUST* be disabled.

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

```
/usr/sbin/cupsctl | /usr/bin/grep -c "_share_printers=0"
```

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

Remediation Description

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

```
/usr/sbin/cupsctl --no-share-printers
/usr/bin/lpstat -p | awk '{print $2}' | /usr/bin/xargs -I{} lpadmin -p {} -o
printer-is-shared=false
```

ID	system_settings_printer_sharing_disable
----	---

References	800-53r5	<ul style="list-style-type: none">• CM-7, CM-7(1)
	CIS Benchmark	<ul style="list-style-type: none">• 2.3.3.4 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 4.1• 4.8
	CCE	<ul style="list-style-type: none">• CCE-92980-2

6.19. Disable Remote Apple Events

If the system does not require Remote Apple Events, support for Apple Remote Events is non-essential and *MUST* be disabled.

The information system *MUST* be configured to provide only essential capabilities. Disabling Remote Apple Events helps prevent the unauthorized connection of devices, the unauthorized transfer of information, and unauthorized tunneling.

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


```
/bin/launchctl print-disabled system | /usr/bin/grep -c "com.apple.AEServer" =>
disabled'
```

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

Remediation Description

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

```
/usr/sbin/systemsetup -setremoteappleevents off
/bin/launchctl disable system/com.apple.AEServer
```

 Systemsetup with -setremoteappleevents flag will fail unless you grant Full Disk Access to systemsetup or it's parent process. Requires supervision.

ID	system_settings_rae_disable
----	-----------------------------

References	800-53r5	<ul style="list-style-type: none">• AC-17• AC-3
	CIS Benchmark	<ul style="list-style-type: none">• 2.3.3.7 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 4.1• 4.8
	CCE	<ul style="list-style-type: none">• CCE-92981-0

6.20. Disable Remote Management

Remote Management *MUST* be disabled.

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

```
/usr/libexec/mdmclient QuerySecurityInfo | /usr/bin/grep -c "RemoteDesktopEnabled = 0"
```

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

Remediation Description

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

```
/System/Library/CoreServices/RemoteManagement/ARDAgent.app/Contents/Resources/kick  
start -deactivate -stop
```

ID	system_settings_remote_management_disable	
References	800-53r5	<ul style="list-style-type: none">• CM-7, CM-7(1)
	CIS Benchmark	<ul style="list-style-type: none">• 2.3.3.6 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 4.1• 4.8• 5.4
	CCE	<ul style="list-style-type: none">• CCE-92982-8

6.21. Disable Screen Sharing and Apple Remote Desktop

Support for both Screen Sharing and Apple Remote Desktop (ARD) is non-essential and *MUST* be

disabled.

The information system *MUST* be configured to provide only essential capabilities. Disabling screen sharing and ARD helps prevent the unauthorized connection of devices, the unauthorized transfer of information, and unauthorized tunneling.

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

```
/bin/launchctl print-disabled system | /usr/bin/grep -c '"com.apple.screensharing" => disabled'
```

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

Remediation Description

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

```
/bin/launchctl disable system/com.apple.screensharing
```

NOTE - This will apply to the whole system

ID	system_settings_screen_sharing_disable	
References	800-53r5	<ul style="list-style-type: none">• AC-17• AC-3
	CIS Benchmark	<ul style="list-style-type: none">• 2.3.3.2 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 4.1• 4.8
	CCE	<ul style="list-style-type: none">• CCE-92983-6

6.22. Enforce Session Lock After Screen Saver is Started

A screen saver *MUST* be enabled and the system *MUST* be configured to require a password to unlock once the screensaver has been on for a maximum of 5 seconds.

An unattended system with an excessive grace period is vulnerable to a malicious user.

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

```
/usr/bin/osascript -l JavaScript << EOS
function run() {
```

```

let delay = ObjC.unwrap(
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.screensaver')\
.objectForKey('askForPasswordDelay'))
if ( delay <= 5 ) {
    return("true")
} else {
    return("false")
}
}
EOS

```

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

Remediation Description

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

Create a configuration profile containing the following keys in the (com.apple.screensaver) payload type:

```

<key>askForPasswordDelay</key>
<integer>5</integer>

```

ID	system_settings_screensaver_ask_for_password_delay_enforce	
References	800-53r5	<ul style="list-style-type: none"> • AC-11
	CIS Benchmark	<ul style="list-style-type: none"> • 2.10.2 (level 1)
	CIS Controls V8	<ul style="list-style-type: none"> • 4.7
	CCE	<ul style="list-style-type: none"> • CCE-92984-4

6.23. Enforce Screen Saver Timeout

The screen saver timeout *MUST* be set to 1200 seconds or a shorter length of time.

This rule ensures that a full session lock is triggered within no more than 1200 seconds of inactivity.

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

```

/usr/bin/osascript -l JavaScript << EOS
function run() {
    let timeout = ObjC.unwrap(
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.screensaver')\
.objectForKey('idleTime'))

```

```
if ( timeout <= 1200 ) {  
    return("true")  
} else {  
    return("false")  
}  
}  
EOS
```

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

Remediation Description

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

Create a configuration profile containing the following keys in the (com.apple.screensaver) payload type:

```
<key>idleTime</key>  
<integer>1200</integer>
```

ID	system_settings_screensaver_timeout_enforce	
References	800-53r5	<ul style="list-style-type: none">• AC-11• IA-11
	CIS Benchmark	<ul style="list-style-type: none">• 2.10.1 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 4.3
	CCE	<ul style="list-style-type: none">• CCE-92986-9

6.24. Disable Server Message Block Sharing

Support for Server Message Block (SMB) file sharing is non-essential and *MUST* be disabled.

The information system *MUST* be configured to provide only essential capabilities.

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

```
/bin/launchctl print-disabled system | /usr/bin/grep -c '"com.apple.smbd" => disabled'
```

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

Remediation Description

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

```
/bin/launchctl disable system/com.apple.smbd
```

The system may need to be restarted for the update to take effect.

ID	system_settings_smbd_disable	
References	800-53r5	<ul style="list-style-type: none">• AC-17• AC-3
	CIS Benchmark	<ul style="list-style-type: none">• 2.3.3.3 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 4.1• 4.8• 5.4
	CCE	<ul style="list-style-type: none">• CCE-92989-3

6.25. Enforce Software Update App Update Updates Automatically

Software Update *MUST* be configured to enforce automatic updates of App Updates is enabled.

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

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.SoftwareUpdate')\
.objectForKey('AutomaticallyInstallAppUpdates').js
EOS
```

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

Remediation Description

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

Create a configuration profile containing the following keys in the (com.apple.SoftwareUpdate) payload type:

```
<key>AutomaticallyInstallAppUpdates</key>
<true/>
```

ID	system_settings_software_update_app_update_enforce	
References	800-53r5	<ul style="list-style-type: none">• N/A
	CIS Benchmark	<ul style="list-style-type: none">• 1.5 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 7.3• 7.4
	CCE	<ul style="list-style-type: none">• CCE-92990-1

6.26. Enforce Software Update Downloads Updates Automatically

Software Update *MUST* be configured to enforce automatic downloads of updates is enabled.

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

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.SoftwareUpdate')\
.objectForKey('AutomaticDownload').js
EOS
```

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

Remediation Description

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

Create a configuration profile containing the following keys in the (com.apple.SoftwareUpdate) payload type:

```
<key>AutomaticDownload</key>
<true/>
```

ID	system_settings_software_update_download_enforce	
References	800-53r5	<ul style="list-style-type: none">• N/A
	CIS Benchmark	<ul style="list-style-type: none">• 1.3 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 7.3• 7.4
	CCE	<ul style="list-style-type: none">• CCE-92991-9

6.27. Enforce Software Update Automatically

Software Update *MUST* be configured to enforce automatic update is enabled.

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

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.SoftwareUpdate')\
.objectForKey('AutomaticCheckEnabled').js
EOS
```

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

Remediation Description

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

Create a configuration profile containing the following keys in the (com.apple.SoftwareUpdate) payload type:

```
<key>AutomaticCheckEnabled</key>
<true/>
```

ID	system_settings_software_update_enforce	
References	800-53r5	• SI-2(5)
	CIS Benchmark	• 1.2 (level 1)
	CIS Controls V8	• 7.3
		• 7.4
	CCE	• CCE-92992-7

6.28. Ensure Software Update is Updated and Current

Make sure Software Update is updated and current.



Automatic fix can cause unplanned restarts and may lose work.

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

```
softwareupdate_date_epoch=$(/bin/date -j -f "%Y-%m-%d" "$( /usr/bin/defaults read /Library/Preferences/com.apple.SoftwareUpdate.plist LastFullSuccessfulDate | /usr/bin/awk '{print $1}' )" "+%s")
```

```
thirty_days_epoch=$(/bin/date -v -30d "+%s")
if [[ $softwareupdate_date_epoch -lt $thirty_days_epoch ]]; then
  /bin/echo "0"
else
  /bin/echo "1"
fi
```

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

Remediation Description

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

```
/usr/sbin/softwareupdate -i -a
```

NOTE - This will apply to the whole system

ID	system_settings_softwareupdate_current	
References	800-53r5	• N/A
	CIS Benchmark	• 1.1 (level 1)
	CIS Controls V8	• 7.3
		• 7.4
	CCE	• CCE-92993-5

6.29. Disable SSH Server for Remote Access Sessions

SSH service *MUST* be disabled for remote access.

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

```
/bin/launchctl print-disabled system | /usr/bin/grep -c '"com.openssh.sshd" => disabled'
```

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

Remediation Description

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

```
/usr/sbin/systemsetup -f -setremotelogin off >/dev/null
```

```
/bin/launchctl disable system/com.openssh.sshd
```



Systemsetup with -setremotelogin flag will fail unless you grant Full Disk Access to systemsetup or it's parent process. Requires supervision.

ID	system_settings_ssh_disable	
References	800-53r5	<ul style="list-style-type: none">• AC-17• CM-7, CM-7(1)
	CIS Benchmark	<ul style="list-style-type: none">• 2.3.3.5 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 4.1• 4.8
	CCE	<ul style="list-style-type: none">• CCE-92994-3

6.30. Require Administrator Password to Modify System-Wide Preferences

The system *MUST* be configured to require an administrator password in order to modify the system-wide preferences in System Settings.

Some Preference Panes in System Settings contain settings that affect the entire system. Requiring a password to unlock these system-wide settings reduces the risk of a non-authorized user modifying system configurations.

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

```
authDBs=("system.preferences" "system.preferences.energysaver"
"system.preferences.network" "system.preferences.printing"
"system.preferences.sharing" "system.preferences.softwareupdate"
"system.preferences.startupdisk" "system.preferences.timemachine")
result="1"
for section in ${authDBs[@]}; do
    if [[ $(/usr/bin/security -q authorizationdb read "$section" | /usr/bin/xmllint
-xpath 'name(//*[contains(text(), "shared")]/following-sibling::*[1])' -) != "false"
]]; then
        result="0"
    fi
    if [[ $(security -q authorizationdb read "$section" | /usr/bin/xmllint -xpath
'//*[contains(text(), "group")]/following-sibling::*[1]/text()' -) != "admin" ]];
then
        result="0"
    fi
    if [[ $(/usr/bin/security -q authorizationdb read "$section" | /usr/bin/xmllint
```

```

-xpath 'name(//*[contains(text(), "authenticate-user")]/following-sibling::*[1])' -)
!= "true" ]]; then
    result="0"
fi
if [[ $(/usr/bin/security -q authorizationdb read "$section" | /usr/bin/xmllint
-xpath 'name(//*[contains(text(), "session-owner")]/following-sibling::*[1])' -) !=
"false" ]]; then
    result="0"
fi
done
echo $result

```

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

Remediation Description

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

```

authDBs=("system.preferences" "system.preferences.energysaver"
"system.preferences.network" "system.preferences.printing"
"system.preferences.sharing" "system.preferences.softwareupdate"
"system.preferences.startupdisk" "system.preferences.timemachine")

for section in ${authDBs[@]}; do
    /usr/bin/security -q authorizationdb read "$section" > "/tmp/$section.plist"

    class_key_value=$(/usr/libexec/PlistBuddy -c "Print :class" "/tmp/$section.plist"
2>&1)
    if [[ "$class_key_value" == *"Does Not Exist"* ]]; then
        /usr/libexec/PlistBuddy -c "Add :class string user" "/tmp/$section.plist"
    else
        /usr/libexec/PlistBuddy -c "Set :class user" "/tmp/$section.plist"
    fi

    key_value=$(/usr/libexec/PlistBuddy -c "Print :shared" "/tmp/$section.plist"
2>&1)
    if [[ "$key_value" == *"Does Not Exist"* ]]; then
        /usr/libexec/PlistBuddy -c "Add :shared bool false" "/tmp/$section.plist"
    else
        /usr/libexec/PlistBuddy -c "Set :shared false" "/tmp/$section.plist"
    fi

    auth_user_key=$(/usr/libexec/PlistBuddy -c "Print :authenticate-user"
"/tmp/$section.plist" 2>&1)
    if [[ "$auth_user_key" == *"Does Not Exist"* ]]; then
        /usr/libexec/PlistBuddy -c "Add :authenticate-user bool true" "/tmp/
$section.plist"
    else
        /usr/libexec/PlistBuddy -c "Set :authenticate-user true" "/tmp/$section.plist"
    fi
done

```

```

fi

session_owner_key=$(/usr/libexec/PlistBuddy -c "Print :session-owner"
/tmp/$section.plist" 2>&1)
if [[ "$session_owner_key" == *"Does Not Exist"* ]]; then
    /usr/libexec/PlistBuddy -c "Add :session-owner bool false" "/tmp/
$section.plist"
else
    /usr/libexec/PlistBuddy -c "Set :session-owner false" "/tmp/$section.plist"
fi

group_key=$(usr/libexec/PlistBuddy -c "Print :group" "/tmp/$section.plist" 2>&1)
if [[ "$group_key" == *"Does Not Exist"* ]]; then
    /usr/libexec/PlistBuddy -c "Add :group string admin" "/tmp/$section.plist"
else
    /usr/libexec/PlistBuddy -c "Set :group admin" "/tmp/$section.plist"
fi

/usr/bin/security -q authorizationdb write "$section" < "/tmp/$section.plist"
done

```

ID	system_settings_system_wide_preferences_configure	
References	800-53r5	<ul style="list-style-type: none"> AC-6, AC-6(1), AC-6(2)
	CIS Benchmark	<ul style="list-style-type: none"> 2.6.8 (level 1)
	CIS Controls V8	<ul style="list-style-type: none"> 4.1
	CCE	<ul style="list-style-type: none"> CCE-92996-8

6.31. Ensure Time Machine Volumes are Encrypted

Time Machine volumes *MUST* be encrypted.

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

```

error_count=0
for tm in $(/usr/bin/tmutil destinationinfo 2>/dev/null | /usr/bin/awk -F': '
'/Name/{print $2}'); do
    tmMounted=$(/usr/sbin/diskutil info "${tm}" 2>/dev/null | /usr/bin/awk
'/Mounted/{print $2}')
    tmEncrypted=$(/usr/sbin/diskutil info "${tm}" 2>/dev/null | /usr/bin/awk
'/FileVault/{print $2}')
    if [[ "$tmMounted" = "Yes" && "$tmEncrypted" = "No" ]]; then
        ((error_count++))
    fi
done

```

```
echo "$error_count"
```

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

Remediation Description

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

1. Go to System Settings → Time Machine
2. Click **Select Disk**
3. Select existing Backup Disk under **Available Disks**
4. Click **Encrypt Backups**
5. Click **Use Disk**

ID	system_settings_time_machine_encrypted_configure	
References	800-53r5	<ul style="list-style-type: none">• N/A
	CIS Benchmark	<ul style="list-style-type: none">• 2.3.4.2 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 3.6• 3.11• 11.3
	CCE	<ul style="list-style-type: none">• CCE-92998-4

6.32. Configure macOS to Use an Authorized Time Server

Approved time server *MUST* be the only server configured for use. As of macOS 10.13 only one time server is supported.

This rule ensures the uniformity of time stamps for information systems with multiple system clocks and systems connected over a network.

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

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.MCX')\
.objectForKey('timeServer').js
EOS
```

If the result is not **time.apple.com**, this is a finding.

Remediation Description

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

Create a configuration profile containing the following keys in the (com.apple.MCX) payload type:

```
<key>timeServer</key>
<string>time.apple.com</string>
```

ID	system_settings_time_server_configure	
References	800-53r5	<ul style="list-style-type: none">• AU-12(1)• SC-45(1)
	CIS Benchmark	<ul style="list-style-type: none">• 2.3.2.1 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 8.4
	CCE	<ul style="list-style-type: none">• CCE-92999-2

6.33. Enforce macOS Time Synchronization

Time synchronization *MUST* be enforced on all networked systems.

This rule ensures the uniformity of time stamps for information systems with multiple system clocks and systems connected over a network.

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

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.timed')\
.objectForKey('TMAutomaticTimeOnlyEnabled').js
EOS
```

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

Remediation Description

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



The following settings are in the (com.apple.ManagedClient.preferences) payload. This payload requires the additional settings to be sub-payloads within, containing their defined payload types.

Create a configuration profile containing the following keys in the (com.apple.timed) payload type:

```
<key>TMAutomaticTimeOnlyEnabled</key>
<true/>
```

ID	system_settings_time_server_enforce	
References	800-53r5	<ul style="list-style-type: none">• AU-12(1)• SC-45(1)
	CIS Benchmark	<ul style="list-style-type: none">• 2.3.2.1 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 8.4
	CCE	<ul style="list-style-type: none">• CCE-93000-8

6.34. Ensure Wake for Network Access Is Disabled

Wake for network access *MUST* be disabled.

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

```
/usr/bin/pmset -g custom | /usr/bin/awk '/womp/ { sum+=$2 } END {print sum}'
```

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

Remediation Description

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

```
/usr/bin/pmset -a womp 0
```

ID	system_settings_wake_network_access_disable	
References	800-53r5	<ul style="list-style-type: none">• N/A
	CIS Benchmark	<ul style="list-style-type: none">• 2.9.3 (level 1)
	CIS Controls V8	<ul style="list-style-type: none">• 4.8
	CCE	<ul style="list-style-type: none">• CCE-93005-7

6.35. Enable Wifi Menu

The WiFi menu *MUST* be enabled.

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

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.controlcenter')\
.objectForKey('WiFi').js
EOS
```

If the result is not **18**, this is a finding.

Remediation Description

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

Create a configuration profile containing the following keys in the (com.apple.controlcenter) payload type:

```
<key>WiFi</key>
<integer>18</integer>
```

ID	system_settings_wifi_menu_enable	
References	800-53r5	• N/A
	CIS Benchmark	• 2.4.1 (level 1)
	CIS Controls V8	• 4.8
		• 12.6
	CCE	• CCE-93010-7