



# macOS Security Compliance

macOS 15.0

***Security Configuration - CIS\_LVL2-MINIMAL***

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

# 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. macOS .....	7
6.1. Enforce Installation of XProtect Remediator and Gatekeeper Updates Automatically .....	7
6.2. Enable Gatekeeper .....	8
6.3. Ensure Advertising Privacy Protection in Safari Is Enabled .....	9
6.4. Disable Automatic Opening of Safe Files in Safari .....	10
6.5. Ensure Prevent Cross-site Tracking in Safari Is Enabled .....	10
6.6. Ensure Warn When Visiting A Fraudulent Website in Safari Is Enabled .....	11
6.7. Ensure Secure Keyboard Entry Terminal.app is Enabled .....	12
7. Password Policy .....	14
7.1. Limit Consecutive Failed Login Attempts to 5 .....	14
7.2. Set Account Lockout Time to 15 Minutes .....	15
8. System Settings .....	17
8.1. Disable Unattended or Automatic Logon to the System .....	17
8.2. Enable Bluetooth Menu .....	18
8.3. Enforce Critical Security Updates to be Installed .....	19
8.4. Enforce FileVault .....	19
8.5. Enable macOS Application Firewall .....	20
8.6. Enable Firewall Stealth Mode .....	21
8.7. Disable the Guest Account .....	22
8.8. Enforce macOS Updates are Automatically Installed .....	23
8.9. Configure Login Window to Show A Custom Message .....	24
8.10. Configure Login Window to Prompt for Username and Password .....	25
8.11. Disable Password Hints .....	26
8.12. Disable Personalized Advertising .....	27
8.13. Enforce Session Lock After Screen Saver is Started .....	27
8.14. Enforce Screen Saver Timeout .....	28
8.15. Enforce Software Update App Update Updates Automatically .....	29
8.16. Enforce Software Update Downloads Updates Automatically .....	30
8.17. Enforce Software Update Automatically .....	31
8.18. Configure Time Machine for Automatic Backups .....	32
8.19. Configure macOS to Use an Authorized Time Server .....	33

8.20. Enforce macOS Time Synchronization . . . . .	33
8.21. Enable Wifi Menu . . . . .	34

# 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 15.0 system against the CIS\_LVL2-MINIMAL (Tailored from CIS\_LVL2) security baseline.

# Chapter 3. Authors

Security configuration tailored by:

Jayson Kish	macplus.solutions
-------------	-------------------

**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
<a href="#">NIST Special Publication 800-53 Rev 5</a>	<i>NIST Special Publication 800-53 Rev 5.1.1</i>
<a href="#">NIST Special Publication 800-63</a>	<i>NIST Special Publication 800-63</i>
<a href="#">NIST Special Publication 800-171</a>	<i>NIST Special Publication 800-171 Rev 3</i>
<a href="#">NIST Special Publication 800-219</a>	<i>NIST Special Publication 800-219 Rev 1</i>

Table 4. Defense Information Systems Agency (DISA)

Document Number or Descriptor	Document Title
<a href="#">STIG Ver 1, Rel 1</a>	<i>Apple macOS 15 (Sequoia) STIG</i>

Table 5. Cybersecurity Maturity Model Certification (CMMC)

Document Number or Descriptor	Document Title
<a href="#">CMMC Model Overview v2.0</a>	<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
<a href="#">CNSSI No. 1253</a>	<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
<a href="#">Apple Platform Security Guide</a>	<i>Apple Platform Security</i>
<a href="#">Apple Platform Deployment</a>	<i>Apple Platform Deployment</i>
<a href="#">Apple Platform Certifications</a>	<i>Apple Platform Certifications</i>
<a href="#">Profile-Specific Payload Keys</a>	<i>Profile-Specific Payload Keys</i>

Table 8. Center for Internet Security

Document Number or Descriptor	Document Title
<a href="#">Apple macOS 14.0</a>	<i>CIS Apple macOS 14.0 Benchmark version 1.1.0</i>

# Chapter 6. macOS

This section contains the configuration and enforcement of operating system settings.



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

## 6.1. Enforce Installation of XProtect Remediator and Gatekeeper Updates Automatically

Software Update *MUST* be configured to update XProtect Remediator and Gatekeeper automatically.

This setting enforces definition updates for XProtect Remediator and Gatekeeper; with this setting in place, new malware and adware that Apple has added to the list of malware or untrusted software will not execute. These updates do not require the computer to be restarted.

<https://support.apple.com/en-us/HT207005>



Software update will automatically update XProtect Remediator and Gatekeeper by default in the macOS.

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('ConfigDataInstall').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>ConfigDataInstall</key>
<true/>
```

ID	os_config_data_install_enforce
----	--------------------------------

References	800-53r5	<ul style="list-style-type: none"><li>• SI-2(5)</li><li>• SI-3</li></ul>
	CIS Benchmark	<ul style="list-style-type: none"><li>• 1.6 (level 1)</li></ul>
	CIS Controls V8	<ul style="list-style-type: none"><li>• 7.3</li><li>• 7.4</li><li>• 7.7</li></ul>
	CCE	<ul style="list-style-type: none"><li>• CCE-94176-5</li></ul>

## 6.2. Enable Gatekeeper

Gatekeeper *MUST* be enabled.

Gatekeeper is a security feature that ensures that applications are digitally signed by an Apple-issued certificate before they are permitted to run. Digital signatures allow the macOS host to verify that the application has not been modified by a malicious third party.

Administrator users will still have the option to override these settings on a case-by-case basis.

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

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.systempolicy.control')\
.objectForKey('EnableAssessment').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.systempolicy.control) payload type:

```
<key>EnableAssessment</key>
<true/>
```

ID	os_gatekeeper_enable
----	----------------------

References	800-53r5	<ul style="list-style-type: none"><li>• CM-14</li><li>• CM-5</li><li>• SI-3</li><li>• SI-7(1), SI-7(15)</li></ul>
	CIS Benchmark	<ul style="list-style-type: none"><li>• 2.6.5 (level 1)</li></ul>
	CIS Controls V8	<ul style="list-style-type: none"><li>• 10.1</li><li>• 10.2</li><li>• 10.5</li></ul>
	CCE	<ul style="list-style-type: none"><li>• CCE-94195-5</li></ul>

### 6.3. Ensure Advertising Privacy Protection in Safari Is Enabled

Allow privacy-preserving measurement of ad effectiveness *MUST* be enabled in Safari.

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

```
/usr/bin/profiles -P -o stdout | /usr/bin/grep -c  
'"WebKitPreferences.privateClickMeasurementEnabled" = 1' | /usr/bin/awk '{ if ($1 >=  
1) {print "1"} else {print "0"}}'
```

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.Safari) payload type:

```
<key>WebKitPreferences.privateClickMeasurementEnabled</key>  
<true/>
```

ID	os_safari_advertising_privacy_protection_enable
----	---

References	800-53r5	<ul style="list-style-type: none"><li>• N/A</li></ul>
	CIS Benchmark	<ul style="list-style-type: none"><li>• 6.3.6 (level 1)</li></ul>
	CIS Controls V8	<ul style="list-style-type: none"><li>• 9.1</li></ul>
	CCE	<ul style="list-style-type: none"><li>• CCE-94280-5</li></ul>

## 6.4. Disable Automatic Opening of Safe Files in Safari

Open "safe" files after downloading *MUST* be disabled in Safari.

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

```
/usr/bin/profiles -P -o stdout | /usr/bin/grep -c 'AutoOpenSafeDownloads = 0' |  
/usr/bin/awk '{ if ($1 >= 1) {print "1"} else {print "0"}}'
```

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.Safari) payload type:

```
<key>AutoOpenSafeDownloads</key>  
<false/>
```

ID	os_safari_open_safe_downloads_disable	
References	800-53r5	<ul style="list-style-type: none"><li>• N/A</li></ul>
	CIS Benchmark	<ul style="list-style-type: none"><li>• 6.3.1 (level 1)</li></ul>
	CIS Controls V8	<ul style="list-style-type: none"><li>• 9.1</li><li>• 9.6</li></ul>
	CCE	<ul style="list-style-type: none"><li>• CCE-94281-3</li></ul>

## 6.5. Ensure Prevent Cross-site Tracking in Safari Is Enabled

Prevent cross-site tracking *MUST* be enabled in Safari.

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

```
/usr/bin/profiles -P -o stdout | /usr/bin/grep -cE
'"WebKitPreferences.storageBlockingPolicy" = 1|"WebKitStorageBlockingPolicy" =
1|"BlockStoragePolicy" =2' | /usr/bin/awk '{ if ($1 >= 1) {print "1"} else {print
"0"}}'
```

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.Safari) payload type:

```
<key>WebKitPreferences.storageBlockingPolicy</key>
<integer>1</integer>
<key>WebKitStorageBlockingPolicy</key>
<integer>1</integer>
<key>BlockStoragePolicy</key>
<integer>2</integer>
```

ID	os_safari_prevent_cross-site_tracking_enable	
References	800-53r5	• N/A
	CIS Benchmark	• 6.3.4 (level 1)
	CIS Controls V8	• 9.1 • 9.3
	CCE	• CCE-94282-1

## 6.6. Ensure Warn When Visiting A Fraudulent Website in Safari Is Enabled

Warn when visiting a fraudulent website *MUST* be enabled in Safari.

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

```
/usr/bin/profiles -P -o stdout | /usr/bin/grep -c 'WarnAboutFraudulentWebsites = 1' |
/usr/bin/awk '{ if ($1 >= 1) {print "1"} else {print "0"}}'
```

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.Safari) payload type:

```
<key>WarnAboutFraudulentWebsites</key>
<true/>
```

ID	os_safari_warn_fraudulent_website_enable	
References	800-53r5	• N/A
	CIS Benchmark	• 6.3.3 (level 1)
	CIS Controls V8	• 9.1
		• 9.3
	CCE	• CCE-94285-4

## 6.7. Ensure Secure Keyboard Entry Terminal.app is Enabled

Secure keyboard entry *MUST* be enabled in Terminal.app.

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

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.Terminal')\
.objectForKey('SecureKeyboardEntry').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.Terminal) payload type:

```
<key>SecureKeyboardEntry</key>
<true/>
```

<b>ID</b>	os_terminal_secure_keyboard_enable	
<b>References</b>	<div>800-53r5</div> <div>CIS Benchmark</div> <div>CIS Controls V8</div> <div>CCE</div>	<ul style="list-style-type: none"> <li>• N/A</li> <li>• 6.4.1 (level 1)</li> <li>• 4.8</li> <li>• CCE-94315-9</li> </ul>



# Chapter 7. Password Policy

This section contains the configuration and enforcement of settings pertaining to password policies in macOS.



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



The password policy recommendations in the NIST 800-53 (Rev 5) and NIST 800-63B state that complexity rules should be organizationally defined. The values defined are based off of common complexity values. But your organization may define its own password complexity rules.



The settings outlined in this section adhere to the recommendations provided in this document for systems that utilize passwords for local accounts. If systems are integrated with a directory service, local password policies should align with domain password policies to the fullest extent feasible.

## 7.1. Limit Consecutive Failed Login Attempts to 5

The macOS *MUST* be configured to limit the number of failed login attempts to a maximum of 5. When the maximum number of failed attempts is reached, the account *MUST* be locked for a period of time after.

This rule protects against malicious users attempting to gain access to the system via brute-force hacking methods.

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

```
/usr/bin/pwpolicy -getaccountpolicies 2> /dev/null | /usr/bin/tail +2 |  
/usr/bin/xmllint --xpath  
'//dict/key[text()="policyAttributeMaximumFailedAuthentications"]/following-  
sibling::integer[1]/text()' - | /usr/bin/awk '{ if ($1 <= 5) {print "yes"} else {print  
"no"}}' | /usr/bin/uniq
```

If the result is not **yes**, 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.mobiledevice.passwordpolicy) payload type:

```
<key>maxFailedAttempts</key>
```

```
<integer>5</integer>
```

ID	pwpolicy_account_lockout_enforce	
References	800-53r5	• AC-7
	CIS Benchmark	• 5.2.1 (level 1)
	CIS Controls V8	• 6.2
	CCE	• CCE-94331-6

## 7.2. Set Account Lockout Time to 15 Minutes

The macOS *MUST* be configured to enforce a lockout time period of at least 15 minutes when the maximum number of failed logon attempts is reached.

This rule protects against malicious users attempting to gain access to the system via brute-force hacking methods.

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

```
/usr/bin/pwpolicy -getaccountpolicies 2> /dev/null | /usr/bin/tail +2 |  
/usr/bin/xmllint --xpath '//dict/key[text()="autoEnableInSeconds"]/following-  
sibling::integer[1]/text()' - | /usr/bin/awk '{ if ($1/60 >= 15 ) {print "yes"} else  
{print "no"}}' | /usr/bin/uniq
```

If the result is not **yes**, 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.mobiledevice.passwordpolicy) payload type:

```
<key>minutesUntilFailedLoginReset</key>  
<integer>15</integer>
```

ID	pwpolicy_account_lockout_timeout_enforce
----	--

<b>References</b>	<b>800-53r5</b>	<ul style="list-style-type: none"> <li>• AC-7</li> </ul>
	<b>CIS Benchmark</b>	<ul style="list-style-type: none"> <li>• 5.2.1 (level 1)</li> </ul>
	<b>CIS Controls V8</b>	<ul style="list-style-type: none"> <li>• 6.2</li> </ul>
	<b>CCE</b>	<ul style="list-style-type: none"> <li>• CCE-94332-4</li> </ul>

# Chapter 8. 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.

## 8.1. 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"><li>• IA-2</li><li>• IA-5(13)</li></ul>
	CIS Benchmark	<ul style="list-style-type: none"><li>• 2.12.3 (level 1)</li></ul>
	CIS Controls V8	<ul style="list-style-type: none"><li>• 4.7</li></ul>
	CCE	<ul style="list-style-type: none"><li>• CCE-94350-6</li></ul>

## 8.2. 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"><li>• N/A</li></ul>
	CIS Benchmark	<ul style="list-style-type: none"><li>• 2.4.2 (level 1)</li></ul>
	CIS Controls V8	<ul style="list-style-type: none"><li>• 4.8</li><li>• 13.9</li></ul>
	CCE	<ul style="list-style-type: none"><li>• CCE-94353-0</li></ul>

### 8.3. 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-94358-9

### 8.4. 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
```

```
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.MCX')\
.objectForKey('dontAllowFDEDisable').js
EOS
)
fileVault=$(/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/>
```

<b>ID</b>	system_settings_filevault_enforce	
<b>References</b>	<b>800-53r5</b>	<ul style="list-style-type: none"> <li>• SC-28, SC-28(1)</li> </ul>
	<b>CIS Benchmark</b>	<ul style="list-style-type: none"> <li>• 2.6.6 (level 1)</li> </ul>
	<b>CIS Controls V8</b>	<ul style="list-style-type: none"> <li>• 3.6</li> <li>• 3.11</li> </ul>
	<b>CCE</b>	<ul style="list-style-type: none"> <li>• CCE-94360-5</li> </ul>

## 8.5. 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):

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.security.firewall')\
```

```
.objectForKey('EnableFirewall').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.security.firewall) payload type:

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

ID	system_settings_firewall_enable	
References	800-53r5	<ul style="list-style-type: none"><li>• AC-4</li><li>• CM-7, CM-7(1)</li><li>• SC-7, SC-7(12)</li></ul>
	CIS Benchmark	<ul style="list-style-type: none"><li>• 2.2.1 (level 1)</li></ul>
	CIS Controls V8	<ul style="list-style-type: none"><li>• 4.1</li><li>• 4.5</li><li>• 13.1</li></ul>
	CCE	<ul style="list-style-type: none"><li>• CCE-94362-1</li></ul>

## 8.6. 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):

```
/usr/bin/osascript -l JavaScript << EOS
```



```
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.security.firewall')\
.objectForKey('EnableStealthMode').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.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"><li>• CM-7, CM-7(1)</li><li>• SC-7, SC-7(16)</li></ul>
	CIS Benchmark	<ul style="list-style-type: none"><li>• 2.2.2 (level 1)</li></ul>
	CIS Controls V8	<ul style="list-style-type: none"><li>• 4.1</li><li>• 4.5</li><li>• 4.8</li></ul>
	CCE	<ul style="list-style-type: none"><li>• CCE-94363-9</li></ul>

## 8.7. 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-94367-0

## 8.8. 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	• N/A
	CIS Benchmark	• 1.4 (level 1)
	CIS Controls V8	• 7.3
		• 7.4
	CCE	• CCE-94373-8

## 8.9. 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 **kishjayson@macplus.solutions**, 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>kishjayson@macplus.solutions</string>
```

ID	system_settings_loginwindow_loginwindowtext_enable	
References	800-53r5	• N/A
	CIS Benchmark	• 2.10.3 (level 1)
	CIS Controls V8	• 4.1
	CCE	• CCE-94379-5

## 8.10. 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
----	--

<b>References</b>	<b>800-53r5</b>	<ul style="list-style-type: none"><li>• IA-2</li></ul>
	<b>CIS Benchmark</b>	<ul style="list-style-type: none"><li>• 2.10.4 (level 1)</li></ul>
	<b>CIS Controls V8</b>	<ul style="list-style-type: none"><li>• 4.1</li></ul>
	<b>CCE</b>	<ul style="list-style-type: none"><li>• CCE-94380-3</li></ul>

## 8.11. 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>
```

<b>ID</b>	system_settings_password_hints_disable	
<b>References</b>	<b>800-53r5</b>	<ul style="list-style-type: none"><li>• IA-6</li></ul>
	<b>CIS Benchmark</b>	<ul style="list-style-type: none"><li>• 2.10.5 (level 1)</li></ul>
	<b>CIS Controls V8</b>	<ul style="list-style-type: none"><li>• 4.1</li></ul>
	<b>CCE</b>	<ul style="list-style-type: none"><li>• CCE-94382-9</li></ul>

# 8.12. 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"><li>• AC-20</li><li>• CM-7, CM-7(1)</li><li>• SC-7(10)</li></ul>
	CIS Benchmark	<ul style="list-style-type: none"><li>• 2.6.4 (level 1)</li></ul>
	CIS Controls V8	<ul style="list-style-type: none"><li>• 4.8</li></ul>
	CCE	<ul style="list-style-type: none"><li>• CCE-94383-7</li></ul>

# 8.13. 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	• AC-11
	CIS Benchmark	• 2.10.2 (level 1)
	CIS Controls V8	• 4.7
	CCE	• CCE-94388-6

## 8.14. 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"><li>• AC-11</li><li>• IA-11</li></ul>
	CIS Benchmark	<ul style="list-style-type: none"><li>• 2.10.1 (level 1)</li></ul>
	CIS Controls V8	<ul style="list-style-type: none"><li>• 4.3</li></ul>
	CCE	<ul style="list-style-type: none"><li>• CCE-94390-2</li></ul>

## 8.15. 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	• N/A
	CIS Benchmark	• 1.5 (level 1)
	CIS Controls V8	• 7.3
		• 7.4
	CCE	• CCE-94395-1

# 8.16. 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	• N/A
	CIS Benchmark	• 1.3 (level 1)
	CIS Controls V8	• 7.3
		• 7.4
	CCE	• CCE-94396-9

## 8.17. 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	<ul style="list-style-type: none"><li>• SI-2(5)</li></ul>
	CIS Benchmark	<ul style="list-style-type: none"><li>• 1.2 (level 1)</li></ul>
	CIS Controls V8	<ul style="list-style-type: none"><li>• 7.3</li><li>• 7.4</li></ul>
	CCE	<ul style="list-style-type: none"><li>• CCE-94397-7</li></ul>

## 8.18. Configure Time Machine for Automatic Backups

Automatic backups *MUST* be enabled when using Time Machine.

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

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.TimeMachine')\
.objectForKey('AutoBackup').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.TimeMachine) payload type:

```
<key>AutoBackup</key>
<true/>
```

ID	system_settings_time_machine_auto_backup_enable	
References	800-53r5	<ul style="list-style-type: none"><li>• N/A</li></ul>
	CIS Benchmark	<ul style="list-style-type: none"><li>• 2.3.4.1 (level 2)</li></ul>
	CIS Controls V8	<ul style="list-style-type: none"><li>• 11.2</li></ul>
	CCE	<ul style="list-style-type: none"><li>• CCE-94402-5</li></ul>

# 8.19. 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"><li>• AU-12(1)</li><li>• SC-45(1)</li></ul>
	CIS Benchmark	<ul style="list-style-type: none"><li>• 2.3.2.1 (level 1)</li></ul>
	CIS Controls V8	<ul style="list-style-type: none"><li>• 8.4</li></ul>
	CCE	<ul style="list-style-type: none"><li>• CCE-94404-1</li></ul>

# 8.20. 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"><li>• AU-12(1)</li><li>• SC-45(1)</li></ul>
	CIS Benchmark	<ul style="list-style-type: none"><li>• 2.3.2.1 (level 1)</li></ul>
	CIS Controls V8	<ul style="list-style-type: none"><li>• 8.4</li></ul>
	CCE	<ul style="list-style-type: none"><li>• CCE-94405-8</li></ul>

## 8.21. 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	<ul style="list-style-type: none"><li>• N/A</li></ul>
	CIS Benchmark	<ul style="list-style-type: none"><li>• 2.4.1 (level 1)</li></ul>
	CIS Controls V8	<ul style="list-style-type: none"><li>• 4.8</li><li>• 12.6</li></ul>
	CCE	<ul style="list-style-type: none"><li>• CCE-94414-0</li></ul>