CIS. Center for Internet Security®

CIS Benchmarks™

CIS Apple macOS 13.0 Ventura Cloud-tailored Benchmark

v1.1.0 - 10-30-2024

Terms of Use

Please see the below link for our current terms of use:

https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/

For information on referencing and/or citing CIS Benchmarks in 3rd party documentation (including using portions of Benchmark Recommendations) please contact CIS Legal (CISLegal@cisecurity.org) and request guidance on copyright usage.

NOTE: It is ***NEVER*** acceptable to host a CIS Benchmark in ***ANY*** format (PDF, etc.) on a 3rd party (non-CIS owned) site.

Table of Contents

Overview

All CIS Benchmarks™ focus on technical configuration settings used to maintain and/or increase the security of the addressed technology, and they should be used in **conjunction** with other essential cyber hygiene tasks like:

- Monitoring the base operating system and applications for vulnerabilities and quickly updating with the latest security patches.
- End-point protection (Antivirus software, Endpoint Detection and Response (EDR), etc.).
- Logging and monitoring user and system activity.

In the end, the CIS Benchmarks™ are designed to be a key **component** of a comprehensive cybersecurity program.

Important Usage Information

All CIS Benchmarks™ are available free for non-commercial use from the CIS Website. They can be used to ***manually*** assess and remediate systems and applications. In lieu of manual assessment and remediation, there are several tools available to assist with assessment:

- CIS Configuration Assessment Tool (CIS-CAT® Pro Assessor)
- CIS Benchmarks™ Certified 3rd Party Tooling

These tools make the hardening process much more scalable for large numbers of systems and applications.

> **NOTE**: Some tooling focuses only on the CIS Benchmarks™ Recommendations that can be fully automated (skipping ones marked **Manual**). It is important that ***ALL*** Recommendations (**Automated** and **Manual**) be addressed, since all are important for properly securing systems and are typically in scope for audits.

In addition, CIS has developed CIS Build Kits for some common technologies to assist in applying CIS Benchmarks™ Recommendations.

When remediating systems (changing configuration settings on deployed systems as per the CIS Benchmarks™ Recommendations), please approach this with caution and test thoroughly.

The following is a reasonable remediation approach to follow:

1. **NEVER** deploy a CIS Build Kit, or any internally developed remediation method, to production systems without proper testing.
2. Proper testing consists of the following:

a. Understand the configuration (including installed applications) of the targeted systems.
b. Read the Impact section of the given Recommendation to help determine if there might be an issue with the targeted systems.
c. Test the configuration changes on representative lab system(s). This way if there is some issue it can be resolved prior to deploying to any production systems.
d. When confident, initially deploy to a small sub-set of users and monitor closely for issues. This way if there is some issue it can be resolved prior to deploying more broadly.
e. When confident, iteratively deploy to additional groups and monitor closely for issues until deployment is complete. This way if there is some issue it can be resolved prior to continuing deployment.

NOTE: CIS and the CIS Benchmarks™ development communities in CIS WorkBench do their best to test and have high confidence in the Recommendations, but they cannot test potential conflicts with all possible system deployments. Known potential issues identified during CIS Benchmarks™ development are documented in the Impact section of each Recommendation.

By using CIS and/or CIS Benchmarks™ Certified tools, and being careful with remediation deployment, it is possible to harden large numbers of deployed systems in a cost effective, efficient, and safe manner.

NOTE: As previously stated, the PDF versions of the CIS Benchmarks™ are available for free, non-commercial use on the CIS Website. All other formats of the CIS Benchmarks™ (MS Word, Excel, and Build Kits) are available for CIS SecureSuite® members.

CIS-CAT® Pro is also available to CIS SecureSuite® members.

Target Technology Details

This document, CIS Apple macOS 13.0 Ventura Cloud-tailored Benchmark, provides prescriptive guidance for establishing a secure configuration posture for Apple macOS 13.0 Ventura running on a cloud platform. This guide was tested against Apple macOS 13.0 Ventura. To obtain the latest version of this guide, please visit http://benchmarks.cisecurity.org. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

Intended Audience

This document is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate Apple macOS 13.0 Ventura.

Consensus Guidance

This CIS Benchmark™ was created using a consensus review process comprised of a global community of subject matter experts. The process combines real world experience with data-based information to create technology specific guidance to assist users to secure their environments. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS Benchmark undergoes two phases of consensus review. The first phase occurs during initial Benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the Benchmark. This discussion occurs until consensus has been reached on Benchmark recommendations. The second phase begins after the Benchmark has been published. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the Benchmark. If you are interested in participating in the consensus process, please visit https://workbench.cisecurity.org/.

Typographical Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
`Stylized Monospace font`	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
`Monospace font`	Used for inline code, commands, UI/Menu selections or examples. Text should be interpreted exactly as presented.
`<Monospace font in brackets>`	Text set in angle brackets denote a variable requiring substitution for a real value.
Italic font	Used to reference other relevant settings, CIS Benchmarks and/or Benchmark Communities. Also, used to denote the title of a book, article, or other publication.
Bold font	Additional information or caveats things like **Notes**, **Warnings**, or **Cautions** (usually just the word itself and the rest of the text normal).

Recommendation Definitions

The following defines the various components included in a CIS recommendation as applicable. If any of the components are not applicable it will be noted or the component will not be included in the recommendation.

Title

Concise description for the recommendation's intended configuration.

Assessment Status

An assessment status is included for every recommendation. The assessment status indicates whether the given recommendation can be automated or requires manual steps to implement. Both statuses are equally important and are determined and supported as defined below:

Automated

Represents recommendations for which assessment of a technical control can be fully automated and validated to a pass/fail state. Recommendations will include the necessary information to implement automation.

Manual

Represents recommendations for which assessment of a technical control cannot be fully automated and requires all or some manual steps to validate that the configured state is set as expected. The expected state can vary depending on the environment.

Profile

A collection of recommendations for securing a technology or a supporting platform. Most benchmarks include at least a Level 1 and Level 2 Profile. Level 2 extends Level 1 recommendations and is not a standalone profile. The Profile Definitions section in the benchmark provides the definitions as they pertain to the recommendations included for the technology.

Description

Detailed information pertaining to the setting with which the recommendation is concerned. In some cases, the description will include the recommended value.

Rationale Statement

Detailed reasoning for the recommendation to provide the user a clear and concise understanding on the importance of the recommendation.

Impact Statement

Any security, functionality, or operational consequences that can result from following the recommendation.

Audit Procedure

Systematic instructions for determining if the target system complies with the recommendation.

Remediation Procedure

Systematic instructions for applying recommendations to the target system to bring it into compliance according to the recommendation.

Default Value

Default value for the given setting in this recommendation, if known. If not known, either not configured or not defined will be applied.

References

Additional documentation relative to the recommendation.

CIS Critical Security Controls® (CIS Controls®)

The mapping between a recommendation and the CIS Controls is organized by CIS Controls version, Safeguard, and Implementation Group (IG). The Benchmark in its entirety addresses the CIS Controls safeguards of (v7) “5.1 - Establish Secure Configurations” and (v8) '4.1 - Establish and Maintain a Secure Configuration Process” so individual recommendations will not be mapped to these safeguards.

Additional Information

Supplementary information that does not correspond to any other field but may be useful to the user.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1**

  Items in this profile intend to:

  - be practical and prudent;
  - provide a clear security benefit; and
  - not inhibit the utility of the technology beyond acceptable means.

- **Level 2**

  This profile extends the "Level 1" profile. Items in this profile exhibit one or more of the following characteristics:

  - are intended for environments or use cases where security is paramount
  - acts as defense in depth measure
  - may negatively inhibit the utility or performance of the technology.

Acknowledgements

This Benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

Author
Ron Colvin

Contributor
William Harrison
Mark Andersen
Ben Montour
Sara Archacki
Hao Shu
Jeffrey Compton
Jorge Escobar
Tim Harrison CISSP, ICP, KMP, Center for Internet Security, New York
Laura Gardner
Michael Scarborough
Mauro Faccenda
Jason Olsen BSCS, Comerica Bank
Mischa van der Bent
Bob Gendler
Dan Brodjieski
Allen Golbig
Jason Blake
Isaac Ordonez , Mann Consulting
Joe Goerlich , Siemens AG
Kari Byrd
John Mahlman
Henry Stamerjohann CISSP, CCSP
Ron Colvin, Ron Colvin
Matt Durante

Editor
Eric Pinnell
Edward Byrd , Center for Internet Security, New York

Recommendations

1 Install Updates, Patches and Additional Security Software

Install Updates, Patches and Additional Security Software

1.1 Ensure All Apple-provided Software Is Current (Automated)

Profile Applicability:

- Level 1

Description:

Software vendors release security patches and software updates for their products when security vulnerabilities are discovered. There is no simple way to complete this action without a network connection to an Apple software repository. Please ensure appropriate access for this control. This check is only for what Apple provides through software update.

Software updates should be run at minimum every 30 days. Run the following command to verify when software update was previously run:

`$ /usr/bin/sudo defaults read /Library/Preferences/com.apple.SoftwareUpdate | grep -e LastFullSuccessfulDate`.

The response should be in the last 30 days (*Example*): `LastFullSuccessfulDate = "2020-07-30 12:45:25 +0000";`

Rationale:

It is important that these updates be applied in a timely manner to prevent unauthorized persons from exploiting the identified vulnerabilities.

Impact:

Installation of updates can be disruptive to the users especially if a restart is required. Major updates need to be applied after creating an organizational patch policy. It is also advised to run updates and forced restarts during system downtime and not while in active use.

Audit:

Run the following command to verify there are no software updates:

```
% /usr/bin/sudo /usr/sbin/softwareupdate -l

Software Update Tool

Finding available software
No new software available.
```

Note: If you are running a previous version of macOS, the output will say that the current version is available. As long as the system is on the current point release of macOS, it is compliant. It is recommended that your organization moves to the current version of macOS once a .1 version is released. Be aware that old macOS versions will stop receiving any updates.

Remediation:

Run the following command to verify what packages need to be installed:

```
% /usr/bin/sudo /usr/sbin/softwareupdate -l
```

The output will include the following:
`Software Update found the following new or updated software:`
Run the following command to install all the packages that need to be updated:
To install all updates run the command:

```
% /usr/bin/sudo /usr/sbin/softwareupdate -i -a
```

Or run the following command to install individual packages:

```
% /usr/bin/sudo /usr/sbin/softwareupdate -i '<package name>'
```

Note: If one of the software updates listed includes `Action: restart`, then you must attach the `-R` flag to force a system restart. If the system update is complete but no restart occurs, then the system is in an unknown state that requires a future restart. It is advised to run updates and forced restarts during system downtime and not while in active use.
example:

```
% /usr/bin/sudo /usr/sbin/softwareupdate -l

Software Update Tool

Finding available software
Software Update found the following new or updated software:
* Label: ProVideoFormats-2.2.7
        Title: Pro Video Formats, Version: 2.2.7, Size: 9693KiB, Recommended: 
YES,
* Label: Command Line Tools for Xcode-15.0
        Title: Command Line Tools for Xcode, Version: 15.0, Size: 721962KiB, 
Recommended: YES,

% /usr/bin/sudo /usr/sbin/softwareupdate -i 'ProVideoFormats-2.2.7'

Software Update Tool

Finding available software
Attempting to quit apps: (
    "com.apple.Compressor"
)
Waiting for user to quit any relevant apps
Successfully quit all apps

Downloaded Pro Video Formats
Installing Pro Video Formats
Done with Pro Video Formats
Done.
```

In the above example, if a restart was required, the command to remediate would be
`/usr/bin/sudo /usr/sbin/softwareupdate -i 'ProVideoFormats-2.2.7' -R`

References:

1. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r4.pdf

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.3 Perform Automated Operating System Patch Management Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v8	7.4 Perform Automated Application Patch Management Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v7	3.4 Deploy Automated Operating System Patch Management Tools Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.	●	●	●
v7	3.5 Deploy Automated Software Patch Management Tools Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.	●	●	●

1.2 Ensure Auto Update Is Enabled (Automated)

Profile Applicability:

- Level 1

Description:

Auto Update verifies that your system has the newest security patches and software updates. If "Automatically check for updates" is not selected, background updates for new malware definition files from Apple for XProtect and Gatekeeper will not occur.

http://macops.ca/os-x-admins-your-clients-are-not-getting-background-security-updates/

https://derflounder.wordpress.com/2014/12/17/forcing-xprotect-blacklist-updates-on-mavericks-and-yosemite/

Rationale:

It is important that a system has the newest updates applied so as to prevent unauthorized persons from exploiting identified vulnerabilities.

Impact:

Without automatic update, updates may not be made in a timely manner and the system will be exposed to additional risk.

Audit:

Run the following command to verify that software updates are automatically checked:

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

true
```

Remediation:

Run the following command to enable auto update:

```
% /usr/bin/sudo /usr/bin/defaults write
/Library/Preferences/com.apple.SoftwareUpdate AutomaticCheckEnabled -bool
true
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.3 Perform Automated Operating System Patch Management Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v8	7.4 Perform Automated Application Patch Management Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v7	3.4 Deploy Automated Operating System Patch Management Tools Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.	●	●	●
v7	3.5 Deploy Automated Software Patch Management Tools Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.	●	●	●

1.3 Ensure Download New Updates When Available Is Enabled (Automated)

Profile Applicability:

- Level 1

Description:

In the GUI, both "Install macOS updates" and "Install app updates from the App Store" are dependent on whether "Download new updates when available" is selected.

Rationale:

It is important that a system has the newest updates downloaded so that they can be applied.

Impact:

If "Download new updates when available" is not selected, updates may not be made in a timely manner and the system will be exposed to additional risk.

Audit:

Run the following command to verify that software updates are automatically checked:

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

true
```

Remediation:

Run the following command to enable auto update:

```
% /usr/bin/sudo /usr/bin/defaults write
/Library/Preferences/com.apple.SoftwareUpdate AutomaticDownload -bool true
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.3 Perform Automated Operating System Patch Management Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v8	7.4 Perform Automated Application Patch Management Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v7	3.4 Deploy Automated Operating System Patch Management Tools Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.	●	●	●
v7	3.5 Deploy Automated Software Patch Management Tools Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.	●	●	●

1.4 Ensure Install of macOS Updates Is Enabled (Automated)

Profile Applicability:

- Level 1

Description:

Ensure that macOS updates are installed after they are available from Apple. This setting enables macOS updates to be automatically installed. Some environments will want to approve and test updates before they are delivered. It is best practice to test first where updates can and have caused disruptions to operations. Automatic updates should be turned off where changes are tightly controlled and there are mature testing and approval processes. Automatic updates should not be turned off simply to allow the administrator to contact users in order to verify installation. A dependable, repeatable process involving a patch agent or remote management tool should be in place before auto-updates are turned off.

Rationale:

Patches need to be applied in a timely manner to reduce the risk of vulnerabilities being exploited.

Impact:

Unpatched software may be exploited.

Audit:

Run the following command to verify that macOS updates are automatically checked and installed:

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

true
```

Remediation:

Run the following command to to enable automatic checking and installing of macOS updates:

```
% /usr/bin/sudo /usr/bin/defaults write
/Library/Preferences/com.apple.SoftwareUpdate
AutomaticallyInstallMacOSUpdates -bool TRUE
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.3 Perform Automated Operating System Patch Management Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v8	7.4 Perform Automated Application Patch Management Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v7	3.4 Deploy Automated Operating System Patch Management Tools Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.	●	●	●
v7	3.5 Deploy Automated Software Patch Management Tools Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.	●	●	●

1.5 Ensure Install Application Updates from the App Store Is Enabled (Automated)

Profile Applicability:

- Level 1

Description:

Ensure that application updates are installed after they are available from Apple. These updates do not require reboots or administrator privileges for end users.

Rationale:

Patches need to be applied in a timely manner to reduce the risk of vulnerabilities being exploited.

Impact:

Unpatched software may be exploited.

Audit:

Run the following command to verify that App Store updates are auto updating:

```
% /usr/bin/sudo /usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.commerce')\
.objectForKey('AutoUpdate').js
EOS

true
```

Remediation:

Run the following command to turn on App Store auto updating:

```
% /usr/bin/sudo /usr/bin/defaults write
/Library/Preferences/com.apple.commerce AutoUpdate -bool TRUE
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.3 Perform Automated Operating System Patch Management Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v8	7.4 Perform Automated Application Patch Management Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v7	3.4 Deploy Automated Operating System Patch Management Tools Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.	●	●	●
v7	3.5 Deploy Automated Software Patch Management Tools Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.	●	●	●

1.6 Ensure Install Security Responses and System Files Is Enabled (Automated)

Profile Applicability:

- Level 1

Description:

Ensure that system and security updates are installed after they are available from Apple. This setting enables definition updates for XProtect 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 reboots or end user admin rights.

Apple has introduced a security feature that allows for smaller downloads and the installation of security updates when a reboot is not required. This feature is only available when the last regular update has already been applied. This feature emphasizes that a Mac must be up-to-date on patches so that Apple's security tools can be used to quickly patch when a rapid response is necessary.

Rationale:

Patches need to be applied in a timely manner to reduce the risk of vulnerabilities being exploited.

Impact:

Unpatched software may be exploited.

Audit:

Run the following commands to verify that system data files and security updates are automatically checked:

```
% /usr/bin/sudo /usr/bin/osascript -l JavaScript << EOS
function run() {
  let pref1 =
ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.SoftwareUpdat
e')\
  .objectForKey('ConfigDataInstall'))
  let pref2 =
ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.SoftwareUpdat
e')\
  .objectForKey('CriticalUpdateInstall'))
  if ( pref1 == 1 && pref2 == 1 ) {
    return("true")
  } else {
    return("false")
  }
}
EOS

true
```

Remediation:

Run the following commands to enable automatic checking of system data files and security updates:

```
% /usr/bin/sudo  /usr/bin/defaults write
/Library/Preferences/com.apple.SoftwareUpdate ConfigDataInstall -bool true

% /usr/bin/sudo  /usr/bin/defaults write
/Library/Preferences/com.apple.SoftwareUpdate CriticalUpdateInstall -bool
true
```

References:

1. https://eclecticlight.co/2021/10/27/silently-updated-security-data-files-in-monterey/
2. https://support.apple.com/en-us/HT202491
3. https://support.apple.com/guide/security/protecting-against-malware-sec469d47bd8/web
4. https://support.apple.com/guide/deployment/rapid-security-responses-dep93ff7ea78/1/web/1.0

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.3 Perform Automated Operating System Patch Management Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v8	7.4 Perform Automated Application Patch Management Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v8	7.7 Remediate Detected Vulnerabilities Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.		●	●
v7	3.4 Deploy Automated Operating System Patch Management Tools Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.	●	●	●
v7	3.5 Deploy Automated Software Patch Management Tools Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.	●	●	●

2 System Settings

This section contains recommendations related to configurable options in the `System Settings` application.

2.1 Network

The `Network System Settings` pane includes the firewall settings. macOS has a built-in firewall that has two main configuration aspects. Both the Application Layer Firewall (ALF) and the Packet Filter Firewall (PF) can be used to secure running ports and services on a Mac. The Application Firewall is the one accessible in System Preferences under Security. The PF firewall contains many more capabilities than ALF, but also requires a greater understanding of firewall recipes and rule configurations. For standard use cases on a Mac, the PF firewall is not necessary. macOS may expose server services that are reachable remotely, but that is not the primary use case or design. If custom use cases are required, the PF firewall can provide additional security. Macs that are used as mobile desktops do not need to use the PF firewall capabilities unless permanently open ports need to be protected with more granular IP access controls.

Additional information

https://www.muo.com/tag/mac-really-need-firewall/

https://blog.neilsabol.site/post/quickly-easily-adding-pf-packet-filter-firewall-rules-macos-osx/

http://marckerr.com/a-simple-guild-to-the-mac-pf-firewall/

https://blog.scottlowe.org/2013/05/15/using-pf-on-os-x-mountain-lion/

2.1.1 Ensure Firewall Is Enabled (Automated)

Profile Applicability:

- Level 1

Description:

A firewall is a piece of software that blocks unwanted incoming connections to a system.

Rationale:

A firewall minimizes the threat of unauthorized users gaining access to your system while connected to a network or the Internet.

Impact:

The firewall may block legitimate traffic. Applications that are unsigned will require special handling.

Audit:

Run the following command to verify that the firewall is enabled:

```
% /usr/bin/sudo /usr/bin/osascript -l JavaScript << EOS
function run() {
  let firewallstate =
ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.alf')\
.objectForKey('globalstate'))
  if ( ( firewallstate == 1 ) || ( firewallstate == 2 ) ) {
    return("true")
  } else {
    return("false")
  }
}
EOS

true
```

Remediation:

Run the following command to enable the firewall:

```
% /usr/bin/sudo /usr/bin/defaults write /Library/Preferences/com.apple.alf
globalstate -int <value>
```

For the `<value>`, use either `1`, specific services, or `2`, essential services only.

References:

1. https://support.apple.com/en-us/guide/security/seca0e83763f/web
2. http://support.apple.com/en-us/HT201642

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	4.5 Implement and Manage a Firewall on End-User Devices Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v8	13.1 Centralize Security Event Alerting Centralize security event alerting across enterprise assets for log correlation and analysis. Best practice implementation requires the use of a SIEM, which includes vendor-defined event correlation alerts. A log analytics platform configured with security-relevant correlation alerts also satisfies this Safeguard.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v7	9.5 Implement Application Firewalls Place application firewalls in front of any critical servers to verify and validate the traffic going to the server. Any unauthorized traffic should be blocked and logged.			●

2.2 General

2.2.1 Date & Time

This section contains recommendations related to the configurable items under the `Date & Time` panel.

2.2.1.1 Ensure Set Time and Date Automatically Is Enabled (Automated)

Profile Applicability:

- Level 1

Description:

Correct date and time settings are required for authentication protocols, file creation, modification dates, and log entries.

Note: If your organization has internal time servers, enter them here. Enterprise mobile devices may need to use a mix of internal and external time servers. If multiple servers are required, use the Date & Time System Preference with each server separated by a space.

Additional Note: The default Apple time server is time.apple.com. Variations include time.euro.apple.com. While it is certainly more efficient to use internal time servers, there is no reason to block access to global Apple time servers or to add a time.apple.com alias to internal DNS records. There are no reports that Apple gathers any information from NTP synchronization, as the computers already phone home to Apple for Apple services including iCloud use and software updates. Best practice is to allow DNS resolution to an authoritative time service for time.apple.com, preferably to connect to Apple servers, but local servers are acceptable as well.

Rationale:

Kerberos may not operate correctly if the time on the Mac is off by more than 5 minutes. This in turn can affect Apple's single sign-on feature, Active Directory logons, and other features.

Impact:

The `timed` service will periodically synchronize with named time servers and will make the computer time more accurate.

Audit:

Run the following command to ensure that date and time are automatically set:

```
$ /usr/bin/sudo /usr/sbin/systemsetup -getusingnetworktime

Network Time: On
```

Remediation:

Run the following commands to enable the date and time setting automatically:

```
$ /usr/bin/sudo /usr/sbin/systemsetup -setnetworktimeserver
<your.time.server>

setNetworkTimeServer: <your.time.server>

$ /usr/bin/sudo /usr/sbin/systemsetup -setusingnetworktime on

setUsingNetworkTime: On
```

example:

```
$ /usr/bin/sudo /usr/sbin/systemsetup -setnetworktimeserver time.apple.com

setNetworkTimeServer: time.apple.com

$ /usr/bin/sudo /usr/sbin/systemsetup -setusingnetworktime on

setUsingNetworkTime: On
```

Run the following commands if you have not set, or need to set, a new time zone:

```
$ /usr/bin/sudo /usr/sbin/systemsetup -listtimezones

$ /usr/bin/sudo /usr/sbin/systemsetup -settimezone <selected time zone>
```

example:

```
$ /usr/bin/sudo /usr/sbin/systemsetup -listtimezones

Time Zones:
 Africa/Abidjan
 Africa/Accra
 Africa/Addis_Ababa
 ...


$ /usr/bin/sudo /usr/sbin/systemsetup -settimezone America/New_York

Set TimeZone: America/New_York
```

Additional Information:

To learn more about `timed`, read: Has anyone got the time? How High Sierra has changed time synchronisation

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.4 Standardize Time Synchronization Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.		●	●
v7	6.1 Utilize Three Synchronized Time Sources Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.		●	●

2.2.1.2 Ensure the Time Service Is Enabled (Automated)

Profile Applicability:

- Level 1

Description:

In macOS 10.14, Apple replace `ntp` with `timed` for time services, and is used to ensure correct time is kept. Correct date and time settings are required for authentication protocols, file creation, modification dates, and log entries.

Rationale:

Kerberos may not operate correctly if the time on the Mac is off by more than 5 minutes. This in turn can affect Apple's single sign-on feature, Active Directory logons, and other features.

Impact:

Accurate time is required for many computer functions.

Audit:

Terminal Method:
Run the following command to ensure that the timed service is enabled:

```
$ /usr/bin/sudo /bin/launchctl list | /usr/bin/grep -c com.apple.timed

1
```

Remediation:

Terminal Method:
Run the following commands to enable the timed service:

```
$ /usr/bin/sudo /bin/launchctl load -w
/System/Library/LaunchDaemons/com.apple.timed.plist
```

Additional Information:

It is also recommended that time on the computer is within acceptable limits. Truly accurate time is measured within milliseconds.

Run the following commands to verify the time is set within an appropriate limit:

```
$ /usr/bin/sudo /usr/sbin/systemsetup -getnetworktimeserver
```

The output will include `Network Time Server:` and the name of your time server.

example: `Network Time Server: time.apple.com`

```
$ /usr/bin/sudo /usr/bin/sntp <your.time.server>
```

Ensure that the offset result(s) are between -270.x and 270.x seconds.

And to set the time to the correct offset:

```
$ /usr/bin/sudo /usr/bin/sntp -sS <your.time.server>
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.4 Standardize Time Synchronization Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.		●	●
v7	6.1 Utilize Three Synchronized Time Sources Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.		●	●

2.2.2 Sharing

This section contains recommendations related to the configurable items under the `Sharing` panel. The expectation is that no in-bound or out-bound service is directly accessible to the internet. Macs in this environment are expected to be subject to several layers of access control, firewalls, and authorizations to use essential services.

Services like `Remote Login`, `Screen Sharing`, and `Remote Management (ARD)` that are normally disabled in the CIS macOS Benchmarks are services that may be required for standard usage in a cloud platform environment.

2.2.2.1 Ensure Remote Apple Events Is Disabled (Automated)

Profile Applicability:

- Level 1

Description:

Apple Events is a technology that allows one program to communicate with other programs. Remote Apple Events allows a program on one computer to communicate with a program on a different computer.

Rationale:

Disabling Remote Apple Events mitigates the risk of an unauthorized program gaining access to the system.

Impact:

With remote Apple events turned on, an AppleScript program running on another Mac can interact with the local computer.

Audit:

Run the following commands to verify that Remote Apple Events is not set

```
% /usr/bin/sudo /usr/sbin/systemsetup -getremoteappleevents

Remote Apple Events: Off
```

Remediation:

Run the following commands to set Remote Apple Events to Off:

```
% /usr/bin/sudo /usr/sbin/systemsetup -setremoteappleevents off

setremoteappleevents: Off
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

2.2.2.2 Ensure Content Caching Is Disabled (Automated)

Profile Applicability:

- Level 2

Description:

Starting with 10.13 (macOS High Sierra), Apple introduced a service to make it easier to deploy data from Apple, including software updates, where there are bandwidth constraints to the Internet and fewer constraints or greater bandwidth exist on the local subnet. This capability can be very valuable for organizations that have throttled and possibly metered Internet connections. In heterogeneous enterprise networks with multiple subnets, the effectiveness of this capability would be determined by how many Macs were on each subnet at the time new, large updates were made available upstream. This capability requires the use of mac OS clients as P2P nodes for updated Apple content. Unless there is a business requirement to manage operational Internet connectivity and bandwidth, user endpoints should not store content and act as a cluster to provision data.

Content types supported by Content Caching in macOS

Rationale:

The main use case for Mac computers is as mobile user endpoints. P2P sharing services should not be enabled on laptops that are using untrusted networks. Content Caching can allow a computer to be a server for local nodes on an untrusted network. While there are certainly logical controls that could be used to mitigate risk, they add to the management complexity. Since the value of the service is in specific use cases, organizations with the use case described above can accept risk as necessary.

Impact:

This setting will adversely affect bandwidth usage between local subnets and the Internet.

Audit:

Run the following command to verify that Content Caching is not enabled:

```
% /usr/bin/sudo /usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.AssetCache')\
.objectForKey('Activated').js
EOS

false
```

Remediation:

Run the following command to disable Content Caching:

```
% /usr/bin/sudo /usr/bin/AssetCacheManagerUtil deactivate
```

The output will include `Content caching deactivated`

References:

1. https://support.apple.com/guide/mac-help/about-content-caching-mchl9388ba1b/
2. https://support.apple.com/guide/mac-help/set-up-content-caching-on-mac-mchl3b6c3720/

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

2.3 Privacy & Security

This section contains recommendations for configurable options under the `Privacy & Security` panel.

Additional privacy preference information from Apple

If the computer is present in an area where there are privacy concerns or sensitive activity is taking place, the Mac should be configured appropriately for the sensitive area.

Camera: If the computer is present in an area where there are privacy concerns or sensitive activity is taking place, the camera should be covered at those times. A permanent cover or alteration may be required when the computer is always located in a confidential area.

Microphone: If the computer is present in an area where there are privacy concerns or sensitive activity is taking place, the microphone input should be set to zero in the input tab of the Sound preference pane at those times. Individual management of applications with access to the microphone may be managed in the Security & Privacy Preference Pane under Microphone.

WiFi and Bluetooth Some organizations have comprehensive rules that cover the use of wireless technologies in order to implement operational security. There are often specific policies governing the use of both Bluetooth and Wi-Fi (802.11) that may include disabling the wireless capability in either software or hardware or both. Wireless access is part of the feature set required for mobile computers and is considered essential for most users.

Malware is continuously discovered that circumvents the privacy controls of the built-in video, audio or network capabilities. No computer has perfect security, and even if all the drivers are disabled or removed, working drivers can be reintroduced by a determined attacker. Additional info Apple Pays $100.5K Bug Bounty for Mac Webcam Hack

Mac users, update Zoom now — your microphone may be spying on you

Recommended settings for Wi-Fi routers and access points

Control access to the microphone on Mac

Bluetooth security

2.3.1 Ensure Sending Diagnostic and Usage Data to Apple Is Disabled (Automated)

Profile Applicability:

- Level 2

Description:

Apple provides a mechanism to send diagnostic and analytics data back to Apple to help them improve the platform. Information sent to Apple may contain internal organizational information that should be controlled and not available for processing by Apple. Turn off all Analytics and Improvements sharing.

Share Mac Analytics (Share with App Developers dependent on Mac Analytic sharing)

- Includes diagnostics, usage and location data

Share iCloud Analytics

- Includes iCloud data and usage information

Rationale:

Organizations should have knowledge of what is shared with the vendor and that this setting automatically forwards information to Apple.

Audit:

Run the following command to verify that sending diagnostic and usage data to Apple is disabled:

```
% /usr/bin/sudo /usr/bin/defaults read /Library/Application\
Support/CrashReporter/DiagnosticMessagesHistory.plist AutoSubmit

0

% /usr/bin/sudo /usr/bin/defaults read /Library/Application\
Support/CrashReporter/DiagnosticMessagesHistory.plist ThirdPartyDataSubmit

0

% /usr/bin/sudo -u <username> /usr/bin/defaults read
/Users/<username>/Library/Preferences/com.apple.assistant.support "Siri Data
Sharing Opt-In Status"

2
```

Remediation:

Run the following commands to disable the sending of diagnostic data to Apple:

```
% /usr/bin/sudo /usr/bin/defaults write /Library/Application\
Support/CrashReporter/DiagnosticMessagesHistory.plist AutoSubmit -bool false

/usr/bin/sudo /usr/bin/defaults write /Library/Application\
Support/CrashReporter/DiagnosticMessagesHistory.plist ThirdPartyDataSubmit -
bool false

% /usr/bin/sudo /bin/chmod 644 /Library/Application\
Support/CrashReporter/DiagnosticMessagesHistory.plist

% /usr/bin/sudo /usr/bin/chgrp admin /Library/Application\
Support/CrashReporter/DiagnosticMessagesHistory.plist

% /usr/bin/sudo -u <username> /usr/bin/defaults write
/Users/<username>/Library/Preferences/com.apple.assistant.support "Siri Data
Sharing Opt-In Status" -int 2
```

References:

1. https://support.apple.com/en-ca/guide/mac-help/mh27990/mac

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

2.3.2 Ensure Limit Ad Tracking Is Enabled (Automated)

Profile Applicability:

- Level 1

Description:

Apple provides a framework that allows advertisers to target Apple users and end-users with advertisements. While many people prefer to see advertising that is relevant to them and their interests, the detailed information that is collected, correlated, and available to advertisers in repositories via data mining is often disconcerting. This information is valuable to both advertisers and attackers, and has been used with other metadata to reveal users' identities.

Organizations should manage advertising settings on computers rather than allow users to configure the settings.

Apple Information

Ad tracking should be limited on 10.15 and prior.

Rationale:

Organizations should manage user privacy settings on managed devices to align with organizational policies and user data protection requirements.

Impact:

Uses will see generic advertising rather than targeted advertising. Apple warns that this will reduce the number of relevant ads.

Audit:

For each user, run the following command to verify that ad tracking is limited:

```
% /usr/bin/sudo -u <username> /usr/bin/defaults read
/Users/<username>/Library/Preferences/com.apple.AdLib.plist
allowApplePersonalizedAdvertising

0
```

Remediation:

For each needed user, run the following command to enable limited ad tracking:

```
% /usr/bin/sudo -u <username> /usr/bin/defaults write
/Users/<username>/Library/Preferences/com.apple.Adlib.plist
allowApplePersonalizedAdvertising -bool false
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

2.3.3 Ensure Gatekeeper Is Enabled (Automated)

Profile Applicability:

- Level 1

Description:

Gatekeeper is Apple’s application that utilizes allowlisting to restrict downloaded applications from launching. It functions as a control to limit applications from unverified sources from running without authorization. In an update to Gatekeeper in macOS 13 Ventura, Gatekeeper checks every application on every launch, not just quarantined apps.

Rationale:

Disallowing unsigned software will reduce the risk of unauthorized or malicious applications from running on the system.

Audit:

Run the following command to verify that Gatekeeper is enabled:

```
% /usr/bin/sudo /usr/sbin/spctl --status

assessments enabled
```

Remediation:

Run the following command to enable Gatekeeper to allow applications from App Store and identified developers:

```
% /usr/bin/sudo /usr/sbin/spctl --global-enable
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●
v8	10.2 Configure Automatic Anti-Malware Signature Updates Configure automatic updates for anti-malware signature files on all enterprise assets.	●	●	●
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	8.2 Ensure Anti-Malware Software and Signatures are Updated Ensure that the organization's anti-malware software updates its scanning engine and signature database on a regular basis.	●	●	●
v7	8.4 Configure Anti-Malware Scanning of Removable Devices Configure devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected.	●	●	●

2.4 Lock Screen

2.4.1 Ensure an Inactivity Interval of 20 Minutes Or Less for the Screen Saver Is Enabled (Automated)

Profile Applicability:

- Level 1

Description:

A locking screen saver is one of the standard security controls to limit access to a computer and the current user's session when the computer is temporarily unused or unattended. In macOS, the screen saver starts after a value is selected in the drop-down menu. 20 minutes or less is an acceptable value. Any value can be selected through the command line or script, but a number that is not reflected in the GUI can be problematic. 20 minutes is the default for new accounts.

Rationale:

Setting an inactivity interval for the screen saver prevents unauthorized persons from viewing a system left unattended for an extensive period of time.

Impact:

If the screen saver is not set, users may leave the computer available for an unauthorized person to access information.

Audit:

Run this script to verify the idle times for all users:

```
UUID=`ioreg -rd1 -c IOPlatformExpertDevice | grep "IOPlatformUUID" | sed -e
's/^.* "\(.*\)"$/\1/'`

for i in $(find /Users -type d -maxdepth 1)
do
  PREF=$i/Library/Preferences/ByHost/com.apple.screensaver.$UUID
  if [ -e $PREF.plist ]
  then
  echo -n "Checking User: '$i': "
  defaults read $PREF.plist idleTime 2>&1
  fi
done
```

Note: If the output of the script includes `The domain/default pair of (com.apple.screensaver, idleTime) does not exist` for any user, then the setting has not been changed from the default. Follow the remediation instructions to set the idle time to match your organization's policy.

Remediation:

Run the following command to verify that the idle time of the screen saver to 20 minutes of less (≤1200)

```
% sudo -u <username> defaults -currentHost write com.apple.screensaver
idleTime -int <value ≤1200>
```

Note: Issues arise if the command line is used to make the setting something other than what is available in the GUI Menu. The GUI allows the options of 1 (60), 2 (120), 5 (300), 10 (600), or 20 (120) minutes, so use one of those values to avoid any issues.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 Configure Automatic Session Locking on Enterprise Assets Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	●	●	●
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

2.4.2 Ensure Require Password After Screen Saver Begins or Display Is Turned Off Is Enabled for 5 Seconds or Immediately (Automated)

Profile Applicability:

- Level 1

Description:

Sleep and screen saver modes are low power modes that reduce electrical consumption while the system is not in use.

Rationale:

Prompting for a password when waking from sleep or screen saver mode mitigates the threat of an unauthorized person gaining access to a system in the user's absence.

Impact:

Without a screenlock in place, anyone with physical access to the computer would be logged in and able to use the active user's session.

Audit:

Run the following command to verify that a password is required to wake the computer from sleep or from the screen saver after 5 seconds of less:

```
% /usr/bin/sudo /usr/sbin/sysadminctl -screenLock status
```

The output should include either `screenLock delay is immediate` or `screenLock delay is 5 seconds`.

Remediation:

Run the following command to require a password to unlock the computer after the screen saver engages or the computer sleeps:

```
% /usr/bin/sudo /usr/sbin/sysadminctl -screenLock immediate -password
<administrator password>
```

or

```
% /usr/bin/sudo /usr/sbin/sysadminctl -screenLock 5 seconds -password
<administrator password>
```

References:

1. https://blog.kolide.com/screensaver-security-on-macos-10-13-is-broken-a385726e2ae2
2. https://github.com/rtrouton/profiles/blob/master/SetDefaultScreensaver/SetDefaultScreensaver.mobileconfig

Additional Information:

This only protects the system when the screen saver is running.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.7 Manage Default Accounts on Enterprise Assets and Software Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.	●	●	●
v7	4.2 Change Default Passwords Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.	●	●	●

2.4.3 Ensure a Custom Message for the Login Screen Is Enabled (Automated)

Profile Applicability:

- Level 1

Description:

An access warning informs the user that the system is reserved for authorized use only, and that the use of the system may be monitored.

Rationale:

An access warning may reduce a casual attacker's tendency to target the system. Access warnings may also aid in the prosecution of an attacker by evincing the attacker's knowledge of the system's private status, acceptable use policy, and authorization requirements.

Impact:

If users are not informed of their responsibilities, unapproved activities may occur. Users that are not approved for access may take the lack of a warning banner as implied consent to access.

Audit:

Run the following command to verify that a custom message on the login screen is configured:

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

The output should be a message that is configured to your organization's required text.

Remediation:

Run the following command to enable a custom login screen message:

```
% /usr/bin/sudo /usr/bin/defaults write
/Library/Preferences/com.apple.loginwindow LoginwindowText -string "<custom
message>"
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

2.4.4 Ensure Login Window Displays as Name and Password Is Enabled (Automated)

Profile Applicability:

- Level 1

Description:

The login window prompts a user for his/her credentials, verifies their authorization level, and then allows or denies the user access to the system.

Rationale:

Prompting the user to enter both their username and password makes it twice as hard for unauthorized users to gain access to the system since they must discover two attributes.

Audit:

Run the following command to verify the login window displays name and password:

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

true
```

Remediation:

Run the following command to enable the login window to display name and password:

```
% /usr/bin/sudo /usr/bin/defaults write
/Library/Preferences/com.apple.loginwindow SHOWFULLNAME -bool true
```

Note: The GUI will not display the updated setting until the current user(s) logs out.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

2.4.5 Ensure Show Password Hints Is Disabled (Automated)

Profile Applicability:

- Level 1

Description:

Password hints are user-created text displayed when an incorrect password is used for an account.

Rationale:

Password hints make it easier for unauthorized persons to gain access to systems by displaying information provided by the user to assist in remembering the password. This info could include the password itself or other information that might be readily discerned with basic knowledge of the end user.

Impact:

The user can set the hint to any value, including the password itself or clues that allow trivial social engineering attacks.

Audit:

Run the following command to verify that password hints are not displayed:

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

0
```

Note: The default setting is not auditable through the command line. Please run the Terminal command for the remediation to set an initial value.

Remediation:

Run the following command to disable password hints:

```
% /usr/bin/sudo /usr/bin/defaults write
/Library/Preferences/com.apple.loginwindow RetriesUntilHint -int 0
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

2.5 Login Password

The `Touch ID & Password` `System Settings` pane is named `Login Password` on Macs that do not have Touch ID and does not contain any details about Touch ID.

2.5.1 Ensure Users' Accounts Do Not Have a Password Hint (Automated)

Profile Applicability:

- Level 1

Description:

Password hints help the user recall their passwords for various systems and/or accounts. In most cases, password hints are simple and closely related to the user's password.

Rationale:

Password hints that are closely related to the user's password are a security vulnerability, especially in the social media age. Unauthorized users are more likely to guess a user's password if there is a password hint. The password hint is very susceptible to social engineering attacks and information exposure on social media networks.

Audit:

Run the following command to verify that no users have a password hint:

```
% /usr/bin/sudo /usr/bin/dscl . -list /Users hint
```

The output will list all users. If there are any text listed with the user, then the machine is not compliant.
example:

```
% /usr/bin/sudo /usr/bin/dscl . -list /Users hint . -list /Users hint

firstuser    passwordhint
seconduser   passwordhint2
thirduser
fourthuser
Guest
```

Remediation:

Run the following command to remove a user's password hint:

```
% /usr/bin/sudo /usr/bin/dscl . -list /Users hint . -delete /Users/<username>
hint
```

example:

```
% /usr/bin/sudo /usr/bin/dscl . -list /Users hint . -delete /Users/firstuser
hint

% /usr/bin/sudo /usr/bin/dscl . -list /Users hint . -delete /Users/seconduser
hint
```

Additional Information:

Organizations might consider entering an organizational help desk phone number or other text (such as a warning to the user). A help desk number is only appropriate for organizations with trained help desk personnel that are validating user identities for password resets.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

2.6 Users & Groups

Account management is a central part of security for any computer system, including macOS. General practices should be followed to ensure that all accounts on a system are still needed, and that default accounts have been removed. Users with administrator roles should have distinct accounts for both administrator functions as well as day-to-day work where the passwords are different and known only by the user assigned to the account. Accounts with elevated privileges should not be easily discerned from the account name from standard accounts.

When any computer system is added to a directory system there are additional controls available, including user account management, that are not available in a standalone computer. One of the drawbacks is the local computer is no longer in control of the accounts that can access or manage it if given permission. For macOS, if the computer is connected to a directory, any standard user can now log into the computer at console, which by default may be desirable or not depending on the use case. If an administrator group is allowed to administer the local computer, the membership of that group is controlled completely in the directory.

macOS computers connected to a directory should be configured so that the risk is appropriate for the mission use of the computer. Only those accounts that require local authentication should be allowed, and only required administrator accounts should be in the local administrator group. Authenticated users for console access and domain admins for administration may be too broad or too limited.

2.6.1 Ensure Guest Account Is Disabled (Automated)

Profile Applicability:

- Level 1

Description:

The guest account allows users access to the system without having to create an account or password. Guest users are unable to make setting changes and cannot remotely login to the system. All files, caches, and passwords created by the guest user are deleted upon logging out.

Rationale:

Disabling the guest account mitigates the risk of an untrusted user doing basic reconnaissance and possibly using privilege escalation attacks to take control of the system.

Impact:

A guest user can use that access to find out additional information about the system and might be able to use privilege escalation vulnerabilities to establish greater access.

Audit:

Run the following command to verify if the guest account is enabled:

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

false
```

Remediation:

Run the following command to disable the guest account:

```
% /usr/bin/sudo /usr/bin/defaults write
/Library/Preferences/com.apple.loginwindow GuestEnabled -bool false
```

Additional Information:

By default, the guest account is enabled for access to sharing services but is not allowed to log into the computer.

The guest account does not need a password when it is enabled to log into the computer.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v8	6.2 Establish an Access Revoking Process Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.	●	●	●
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

2.6.2 Ensure Guest Access to Shared Folders Is Disabled (Automated)

Profile Applicability:

- Level 1

Description:

Allowing guests to connect to shared folders enables users to access selected shared folders and their contents from different computers on a network.

Rationale:

Not allowing guests to connect to shared folders mitigates the risk of an untrusted user doing basic reconnaissance and possibly using privilege escalation attacks to take control of the system.

Impact:

Unauthorized users could access shared files on the system.

Audit:

Run the following commands to verify that shared folders are not accessible to guest users:

```
% /usr/bin/sudo /usr/sbin/sysadminctl -smbGuestAccess status
```

The output should include `SMB guest access disabled`.

Remediation:

Run the following commands to verify that shared folders are not accessible to guest users:

```
% /usr/bin/sudo /usr/sbin/sysadminctl -smbGuestAccess off
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

2.6.3 Ensure Automatic Login Is Disabled (Automated)

Profile Applicability:

- Level 1

Description:

The automatic login feature saves a user's system access credentials and bypasses the login screen. Instead, the system automatically loads to the user's desktop screen.

Rationale:

Disabling automatic login decreases the likelihood of an unauthorized person gaining access to a system.

Impact:

If automatic login is not disabled, an unauthorized user could gain access to the system without supplying any credentials.

Audit:

Run the following command to verify that automatic login has not been enabled:

```
% /usr/bin/sudo /usr/bin/osascript -l JavaScript << EOS
function run() {
  let pref1 =
ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.loginwindow')
\
  .objectForKey('autoLoginUser'))
  if ( pref1 ==  null ) {
    return("true")
  } else {
    return("false")
  }
}
EOS

true
```

Remediation:

Run the following command to disable automatic login:

```
% /usr/bin/sudo /usr/bin/defaults delete
/Library/Preferences/com.apple.loginwindow autoLoginUser
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.7 Manage Default Accounts on Enterprise Assets and Software Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.	●	●	●
v7	4.2 Change Default Passwords Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.	●	●	●

3 Logging and Auditing

This section provides guidance on configuring the logging and auditing facilities available in macOS. Starting with macOS 10.12, Apple introduced unified logging. This capability replaces the previous logging methodology with centralized, system-wide common controls. A full explanation of macOS logging behavior is beyond the scope of this Benchmark. These changes impact previous logging controls from macOS Benchmarks. At this point, many of the syslog controls have been or are being removed since the old logging methods have been deprecated. Controls that still appear useful will be retained. Some legacy controls have been removed for this release.

More info:

- https://developer.apple.com/documentation/os/logging
- https://eclecticlight.co/2018/03/19/macos-unified-log-1-why-what-and-how/

3.1 Ensure Security Auditing Is Enabled (Automated)

Profile Applicability:

- Level 1

Description:

macOS's audit facility, `auditd`, receives notifications from the kernel when certain system calls, such as `open`, `fork`, and `exit`, are made. These notifications are captured and written to an audit log.

Apple has deprecated `auditd` as of macOS 11.0 Big Sur. In macOS 14.0 Sonoma it is no longer enabled by default and it is suggested to use an application that integrates with the EndpointSecurity API. These applications are 3rd party and not built into the macOS. Until `auditd` is removed from macOS completely, running the binary is the best way to collect logging in macOS and the only one that is part of the OS.

Rationale:

Logs generated by `auditd` may be useful when investigating a security incident as they may help reveal the vulnerable application and the actions taken by a malicious actor.

Audit:

Run the following command to verify auditd:

```
% /usr/bin/sudo /bin/launchctl list | /usr/bin/grep -i auditd

-       0       com.apple.auditd
```

Remediation:

Run the following command to load auditd:

```
% /usr/bin/sudo /bin/launchctl load -w
/System/Library/LaunchDaemons/com.apple.auditd.plist
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	4.9 Log and Alert on Unsuccessful Administrative Account Login Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

3.2 Ensure Security Auditing Flags For User-Attributable Events Are Configured Per Local Organizational Requirements (Automated)

Profile Applicability:

- Level 2

Description:

Auditing is the capture and maintenance of information about security-related events. Auditable events often depend on differing organizational requirements.

Rationale:

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises or attacks that have occurred, have begun, or are about to begin. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised.

Depending on the governing authority, organizations can have vastly different auditing requirements. In this control we have selected a minimal set of audit flags that should be a part of any organizational requirements. The flags selected below may not adequately meet organizational requirements for users of this benchmark. The auditing checks for the flags proposed here will not impact additional flags that are selected.

Audit:

Run the following command to verify the Security Auditing Flags that are enabled:

```
% /usr/bin/sudo /usr/bin/grep -e "^flags:" /etc/security/audit_control
```

The output should include the following flags:

- `-fm` - audit failed file attribute modification events
- `ad` - audit successful/failed administrative events
- `-ex` - audit failed program execution
- `aa` - audit all authorization and authentication events
- `-fr` - audit all failed read actions where enforcement stops a read of a file
- `lo` - audit successful/failed login/logout events
- `-fw` - audit all failed write actions where enforcement stopped a file write

The `-all` flag will capture all failed events across all audit classes and can be used to supersede the individual flags for failed events.
Note: Excluding potentially noisy audit events may be ideal, depending on your use-case.
Note: Historical audit flags are listed below as preliminary guidance.

Remediation:

Perform the following to set the required Security Auditing Flags:
Edit the `/etc/security/audit_control` file and add `-fm`, `ad`, `-ex`, `aa`, `-fr`, `lo`, and `-fw` to `flags`. You can also substitute `-all` for `-fm`, `-ex`, `-fr`, and `-fw`.

References:

1. https://derflounder.wordpress.com/2012/01/30/openbsm-auditing-on-mac-os-x/
2. https://csrc.nist.gov/CSRC/media/Publications/sp/800-179/rev-1/draft/documents/sp800-179r1-draft.pdf
3. https://www.scip.ch/en/?labs.20150108
4. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf
5. https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-31-Improving-the-Federal-Governments-Investigative-and-Remediation-Capabilities-Related-to-Cybersecurity-Incidents.pdf

Additional Information:

Flag settings are currently based on the guidance provided by the NIST through the macOS Security guidance they are providing in their GitHub repository. You can find that guidance here.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.14 Log Sensitive Data Access Log sensitive data access, including modification and disposal.			●
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	14.9 Enforce Detail Logging for Access or Changes to Sensitive Data Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring).			●

3.3 Ensure install.log Is Retained for 365 or More Days and No Maximum Size (Automated)

Profile Applicability:

- Level 1

Description:

macOS writes information pertaining to system-related events to the file `/var/log/install.log` and has a configurable retention policy for this file. The default logging setting limits the file size of the logs and the maximum size for all logs. The default allows for an errant application to fill the log files and does not enforce sufficient log retention. The Benchmark recommends a value based on standard use cases. The value should align with local requirements within the organization.

The default value has an "all_max" file limitation, no reference to a minimum retention, and a less precise rotation argument.

The all_max flag control will remove old log entries based only on the size of the log files. Log size can vary widely depending on how verbose installing applications are in their log entries. The decision here is to ensure that logs go back a year, and depending on the applications a size restriction could compromise the ability to store a full year.

While this Benchmark is not scoring for a rotation flag, the default rotation is sequential rather than using a timestamp. Auditors may prefer timestamps in order to simply review specific dates where event information is desired.

Please review the File Rotation section in the man page for more information.

```
man asl.conf
```

- The maximum file size limitation string should be removed "all_max="
- An organization-appropriate retention should be added "ttl="
- The rotation should be set with timestamps "rotate=utc" or "rotate=local"

Rationale:

Archiving and retaining `install.log` for at least a year is beneficial in the event of an incident, as it will allow the user to view the various changes to the system along with the date and time they occurred.

Impact:

Without log files system maintenance and security, forensics cannot be properly performed.

Audit:

Run the following command to verify that log files are retained for at least 365 days with no maximum size:

```
% /usr/bin/sudo /usr/bin/grep -i ttl /etc/asl/com.apple.install
```

The output must include `ttl≥365`

```
% /usr/bin/sudo /usr/bin/grep -i all_max= /etc/asl/com.apple.install
```

No results should be returned.

Remediation:

Perform the following to ensure that install logs are retained for at least 365 days:
Edit the `/etc/asl/com.apple.install` file and add or modify the `ttl` value to `365` or greater on the `file` line. Also, remove the `all_max=` setting and value from the `file` line.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.1 Establish and Maintain an Audit Log Management Process Establish and maintain an audit log management process that defines the enterprise's logging requirements. At a minimum, address the collection, review, and retention of audit logs for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	8.3 Ensure Adequate Audit Log Storage Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	●	●	●
v7	6.4 Ensure adequate storage for logs Ensure that all systems that store logs have adequate storage space for the logs generated.		●	●
v7	6.7 Regularly Review Logs On a regular basis, review logs to identify anomalies or abnormal events.		●	●

3.4 Ensure Security Auditing Retention Is Enabled (Automated)

Profile Applicability:

- Level 1

Description:

The macOS audit capability contains important information to investigate security or operational issues. This resource is only completely useful if it is retained long enough to allow technical staff to find the root cause of anomalies in the records.

Retention can be set to respect both size and longevity. To retain as much as possible under a certain size, the recommendation is to use the following:

`expire-after:60d OR 5G`

This recomendation is based on minimum storage for review and investigation. When a third party tool is in use to allow remote logging or the store and forwarding of logs, this local storage requirement is not required.

Rationale:

The audit records need to be retained long enough to be reviewed as necessary.

Impact:

The recommendation is that at least 60 days or 5 gigabytes of audit records are retained. Systems that have very little remaining disk space may have issues retaining sufficient data.

Audit:

Run the following command to verify audit retention:

```
% /usr/bin/sudo /usr/bin/grep -e "^expire-after" /etc/security/audit_control
```

The output value for `expire-after:` should be ≥ `60d OR 5G`
Note: If your organization is offloading your security logs, we recommend following the same guidance (at minimum) for your off-site log storage. Your local storage limit (or time frame) may fail if they are set to lower in this case, but are following the guidance.

Remediation:

Perform the following to set the audit retention length:
Edit the `/etc/security/audit_control` file so that `expire-after:` is at least `60d OR 5G`

Default Value:

More info in the man page. To reference the man page use the command `$ man audit_control`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.1 Establish and Maintain an Audit Log Management Process Establish and maintain an audit log management process that defines the enterprise's logging requirements. At a minimum, address the collection, review, and retention of audit logs for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	8.3 Ensure Adequate Audit Log Storage Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	●	●	●
v7	6.4 Ensure adequate storage for logs Ensure that all systems that store logs have adequate storage space for the logs generated.		●	●
v7	6.7 Regularly Review Logs On a regular basis, review logs to identify anomalies or abnormal events.		●	●

3.5 Ensure Access to Audit Records Is Controlled (Automated)

Profile Applicability:

- Level 1

Description:

The audit system on macOS writes important operational and security information that can be both useful for an attacker and a place for an attacker to attempt to obfuscate unwanted changes that were recorded. As part of defense-in-depth, the /etc/security/audit_control configuration and the files in /var/audit should be owned only by root with group wheel with read-only rights and no other access allowed. macOS ACLs should not be used for these files.

The default folder for storing logs is `/var/audit`, but it can be changed. This recommendation will ensure that any target directory has appropriate access control in place even if the target directory is not the default of `/var/audit`.

Rationale:

Audit records should never be changed except by the system daemon posting events. Records may be viewed or extracts manipulated, but the authoritative files should be protected from unauthorized changes.

Impact:

This control is only checking the default configuration to ensure that unwanted access to audit records is not available.

Audit:

Run the following commands to check file access rights:

```
% /usr/bin/sudo /bin/ls -n $(/usr/bin/sudo /usr/bin/grep '^dir'
/etc/security/audit_control | /usr/bin/awk -F: '{print $2}') | /usr/bin/awk
'{s+=$3} END {print s}'

0

% /usr/bin/sudo /bin/ls -n $(/usr/bin/sudo /usr/bin/grep '^dir'
/etc/security/audit_control | /usr/bin/awk -F: '{print $2}') | /usr/bin/awk
'{s+=$4} END {print s}'

0

% /usr/bin/sudo /bin/ls -l $(/usr/bin/sudo /usr/bin/grep '^dir'
/etc/security/audit_control | /usr/bin/awk -F: '{print $2}') | /usr/bin/awk
'!/-r--r-----|current|total/{print $1}' | /usr/bin/wc -l | /usr/bin/tr -d ' '

0

% /usr/bin/sudo /bin/ls -n $(/usr/bin/sudo /usr/bin/grep '^dir' /var/audit/ |
/usr/bin/awk -F: '{print $2}') | /usr/bin/awk '{s+=$3} END {print s}'

0

% /usr/bin/sudo /bin/ls -n $(/usr/bin/sudo /usr/bin/grep '^dir' /var/audit/ |
/usr/bin/awk -F: '{print $2}') | /usr/bin/awk '{s+=$4} END {print s}'

0

% /usr/bin/sudo /bin/ls -l $(/usr/bin/sudo /usr/bin/grep '^dir' /var/audit/ |
/usr/bin/awk -F: '{print $2}') | /usr/bin/awk '!/-r--r-----
|current|total/{print $1}' | /usr/bin/wc -l | /usr/bin/tr -d ' '

0
```

Remediation:

Terminal Method:
Run the following to commands to set the audit records to the root user and wheel group:

```
% /usr/bin/sudo /usr/sbin/chown -R root:wheel /etc/security/audit_control

% /usr/bin/sudo /bin/chmod -R og-rw /etc/security/audit_control

% /usr/bin/sudo /usr/sbin/chown -R root:wheel $(/usr/bin/sudo /usr/bin/grep
'^dir' /etc/security/audit_control | /usr/bin/awk -F: '{print $2}')

% /usr/bin/sudo /bin/chmod -R og-rw $(/usr/bin/sudo /usr/bin/grep '^dir'
/etc/security/audit_control | /usr/bin/awk -F: '{print $2}')
```

Note: It is recommended to do a thorough verification process on why the audit logs have been changed before following the remediation steps. If the system has different access controls on the audit logs, and the changes cannot be traced, a new install may be prudent. Check for signs of file tampering as well as unapproved OS changes.
Note: In macOS 14, and versions going forward, Apple disabled `auditd` by default. Since that is the default, the `/etc/security/audit_control` does not exist. If this remediation is ran without copying the `/etc/security/audit_control.example` to `/etc/security/audit_control` then it can cause a recursive permissions issue and can cause an unsupported state (undesired results) and booting anomalies.

Additional Information:

From ls man page

```
-e      Print the Access Control List (ACL) associated with the file, if
             present, in long (-l) output.
```

More info:

https://www.techrepublic.com/blog/apple-in-the-enterprise/introduction-to-os-x-access-control-lists-acls/

http://ahaack.net/technology/OS-X-Access-Control-Lists-ACL.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user’s need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

3.6 Ensure Firewall Logging Is Enabled and Configured (Automated)

Profile Applicability:

- Level 1

Description:

The socketfilter Firewall is what is used when the Firewall is turned on in the Security & Privacy Preference Pane. In order to appropriately monitor what access is allowed and denied, logging must be enabled. The logging level must be set to "detailed" to be useful in monitoring connection attempts that the firewall detects. Throttled login is not sufficient for examining Firewall connection attempts.

In-depth log monitoring on macOS may require changes to the "Enable-Private-Data" key in SystemLogging.System to ensure more complete logging.

Reviewing macOS Unified Logs

Rationale:

In order to troubleshoot the successes and failures of a Firewall, detailed logging should be enabled.

Impact:

Detailed logging may result in excessive storage.

Audit:

Run the following command to verify that the Firewall log is enabled:

```
% /usr/bin/sudo /usr/bin/osascript -l JavaScript << EOS
function run() {
  let pref1 = $.NSUserDefaults.alloc.initWithSuiteName('com.apple.alf')\
  .objectForKey('loggingenabled').js
  let pref2 = $.NSUserDefaults.alloc.initWithSuiteName('com.apple.alf')\
  .objectForKey('loggingoption').js
  if ( pref1 == 1 && pref2 == 2 ) {
    return("true")
  } else {
    return("false")
  }
}
EOS

true
```

Remediation:

Run the following command to enable logging of the firewall:

```
% /usr/bin/sudo /usr/libexec/ApplicationFirewall/socketfilterfw --
setloggingmode on

Turning on log mode

% /usr/bin/sudo /usr/libexec/ApplicationFirewall/socketfilterfw --
setloggingopt detail

Setting detail log option
```

References:

1. https://developer.apple.com/documentation/devicemanagement/firewall?language=objc

Additional Information:

More info http://krypted.com/tag/socketfilterfw/

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.5 Implement and Manage a Firewall on End-User Devices Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

4 Network Configurations

This section contains guidance on configuring the networking-related aspects of macOS that have been removed from `System Settings` but still can be set through `Terminal`.

4.1 Ensure Bonjour Advertising Services Is Disabled (Automated)

Profile Applicability:

- Level 2

Description:

Bonjour is an auto-discovery mechanism for TCP/IP devices which enumerates devices and services within a local subnet. DNS on macOS is integrated with Bonjour and should not be turned off, but the Bonjour advertising service can be disabled.

Rationale:

Bonjour can simplify device discovery from an internal rogue or compromised host. An attacker could use Bonjour's multicast DNS feature to discover a vulnerable or poorly-configured service or additional information to aid a targeted attack. Implementing this control disables the continuous broadcasting of "I'm here!" messages. Typical end-user endpoints should not have to advertise services to other computers. This setting does not stop the computer from sending out service discovery messages when looking for services on an internal subnet, if the computer is looking for a printer or server and using service discovery. To block all Bonjour traffic except to approved devices, the pf or other firewall would be needed.

Impact:

Some applications may not operate properly if the `mDNSResponder` is turned off. This will also affect AirDrop functionality.

Audit:

Run the following command to verify that Bonjour Advertising is not enabled:

```
% /usr/bin/sudo /usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.mDNSResponder')\
.objectForKey('NoMulticastAdvertisements').js
EOS

true
```

Remediation:

Run the following command to disable Bonjour Advertising services:

```
% /usr/bin/sudo /usr/bin/defaults write
/Library/Preferences/com.apple.mDNSResponder.plist NoMulticastAdvertisements
-bool true
```

Additional Information:

Anything Bonjour discovers is already available on the network and probably discoverable with network scanning tools. The security benefit of disabling Bonjour for that reason is minimal.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

4.2 Ensure HTTP Server Is Disabled (Automated)

Profile Applicability:

- Level 1

Description:

macOS used to have a graphical front-end to the embedded Apache web server in the Operating System. Personal web sharing could be enabled to allow someone on another computer to download files or information from the user's computer. Personal web sharing from a user endpoint has long been considered questionable, and Apple has removed that capability from the GUI. Apache, however, is still part of the Operating System and can be easily turned on to share files and provide remote connectivity to an end-user computer. Web sharing should only be done through hardened web servers and appropriate cloud services.

Rationale:

Web serving should not be done from a user desktop. Dedicated webservers or appropriate cloud storage should be used. Open ports make it easier to exploit the computer.

Impact:

The web server is both a point of attack for the system and a means for unauthorized file transfers.

Audit:

Run the following command to verify that the HTTP server services are not currently enabled. This check does not reflect any auto-start settings, only whether the web server is currently enabled:

```
% /usr/bin/sudo /bin/launchctl list | /usr/bin/grep -c "org.apache.httpd"

0
```

Remediation:

Run the following command to disable the HTTP server services:

```
% /usr/bin/sudo /usr/sbin/apachectl stop

% /usr/bin/sudo /bin/launchctl unload -w
/System/Library/LaunchDaemons/org.apache.httpd.plist
```

References:

1. https://www.stigviewer.com/stig/apple_macos_11_big_sur/2021-06-16/finding/V-230793
2. https://httpd.apache.org/security/vulnerabilities_24.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

4.3 Ensure NFS Server Is Disabled (Automated)

Profile Applicability:

- Level 1

Description:

macOS can act as an NFS fileserver. NFS sharing could be enabled to allow someone on another computer to mount shares and gain access to information from the user's computer. File sharing from a user endpoint has long been considered questionable, and Apple has removed that capability from the GUI. NFSD is still part of the Operating System and can be easily turned on to export shares and provide remote connectivity to an end-user computer.

The etc/exports file contains the list of NFS shared directories. If the file exists, it is likely that NFS sharing has been enabled in the past or may be available periodically. As an additional check, the audit verifies that there is no /etc/exports file.

Rationale:

File serving should not be done from a user desktop. Dedicated servers should be used. Open ports make it easier to exploit the computer.

Impact:

The nfs server is both a point of attack for the system and a means for unauthorized file transfers.

Audit:

Run the following commands to verify that the NFS fileserver service is not enabled:

```
% /usr/bin/sudo /bin/launchctl list | /usr/bin/grep -c com.apple.nfsd

0

% /usr/bin/sudo /bin/cat /etc/exports

cat: /etc/exports: No such file or directory
```

Remediation:

Run the following command to disable the nfsd fileserver services:

```
% /usr/bin/sudo /sbin/nfsd stop

% /usr/bin/sudo /bin/launchctl disable system/com.apple.nfsd
```

Remove the exported Directory listing.

```
% /usr/bin/sudo /bin/rm /etc/exports
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

5 System Access, Authentication, and Authorization

The controls in this section are a combination of hardening controls that are not specifically in a System Preference pane. Many of these controls are only accessible using the Command Line or a Device Profile and not available in the Graphical User Interface. The Benchmark does contain simple, easy to follow instructions for technical staff to audit and implement recommended controls.

FileVault is enabled in the CIS macOS Benchmarks, but in a cloud platform environment FileVault probably does need not be enabled since there is no direct physical access to the system. FileVault may not be needed if the physical environment where the system resides is properly protected and secure.

5.1 File System Permissions and Access Controls

File system permissions have always been part of computer security. There are several principles that are part of best practices for a POSIX-based system which are contained in this section. This section does not contain a complete list of every permission on a macOS System that might be problematic. Developers and use cases differ, and what some administrators who are long in the profession might consider a travesty are issues to which a risk assessor steeped in BYOD trends may not give a second glance. Here we document controls that should point out truly bad practices or anomalies which should be looked at and considered closely. Many of the controls are to mitigate the risk of privilege escalation attacks and data exposure to unauthorized parties.

5.1.1 Ensure Home Folders Are Secure (Automated)

Profile Applicability:

- Level 1

Description:

By default, macOS allows all valid users into the top level of every other user's home folder and restricts access to the Apple default folders within. Another user on the same system can see you have a "Documents" folder but cannot see inside it. This configuration does work for personal file sharing but can expose user files to standard accounts on the system.

The best parallel for Enterprise environments is that everyone who has a Dropbox account can see everything that is at the top level but can't see your pictures. Similarly with macOS, users can see into every new Directory that is created because of the default permissions.

Home folders should be restricted to access only by the user. Sharing should be used on dedicated servers or cloud instances that are managing access controls. Some environments may encounter problems if execute rights are removed as well as read and write. Either no access or execute only for group or others is acceptable.

Rationale:

Allowing all users to view the top level of all networked users' home folder may not be desirable since it may lead to the revelation of sensitive information.

Impact:

If implemented, users will not be able to use the "Public" folders in other users' home folders. "Public" folders with appropriate permissions would need to be set up in the /Shared folder.

Audit:

Run the following command to ensure that all home folders are secure:

```
% /usr/bin/sudo /usr/bin/find /System/Volumes/Data/Users -mindepth 1 -
maxdepth 1 -type d -not -perm 700 | /usr/bin/grep -v "Shared" | /usr/bin/grep
-v "Guest"
```

The output will show what user folders are not secure.

Remediation:

For each user, run the following command to secure all home folders:

```
% /usr/bin/sudo /bin/chmod -R og-rwx /Users/<username>
```

Alternately, run the following command if there needs to be executable access for a home folder:

```
% /usr/bin/sudo /bin/chmod -R og-rw /Users/<username>
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

5.1.2 Ensure Apple Mobile File Integrity (AMFI) Is Enabled (Automated)

Profile Applicability:

- Level 1

Description:

Apple Mobile File Integrity (AMFI) was first released in macOS 10.12. The daemon and service block attempts to run unsigned code. AMFI uses launchd, code signatures, certificates, entitlements, and provisioning profiles to create a filtered entitlement dictionary for an app. AMFI is the macOS kernel module that enforces code-signing and library validation.

Rationale:

Apple Mobile File Integrity validates that application code is validated.

Impact:

Applications could be compromised with malicious code.

Audit:

Run the following command to verify that Apple Mobile File Integrity is enabled:

```
% /usr/bin/sudo /usr/sbin/nvram -p | /usr/bin/grep -c
"amfi_get_out_of_my_way=1"

0
```

Note: AMFI cannot be disabled with SIP enabled, but a change attempt can be made that will appear successful, and report incorrectly as successful. If the AMFI audit fails, and the SIP audit passes, this is still an issue the admin should research.

Remediation:

Run the following command to enable the Apple Mobile File Integrity service:

```
% /usr/bin/sudo /usr/sbin/nvram boot-args=""
```

References:

1. https://eclecticlight.co/2018/12/29/amfi-checking-file-integrity-on-your-mac/
2. https://github.com/usnistgov/macos_security/issues/39
3. https://github.com/usnistgov/macos_security/issues/40
4. https://www.naut.ca/blog/2020/11/13/forbidden-commands-to-liberate-macos/

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.3 Address Unauthorized Software Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.	●	●	●
v8	2.6 Allowlist Authorized Libraries Use technical controls to ensure that only authorized software libraries, such as specific .dll, .ocx, .so, etc., files, are allowed to load into a system process. Block unauthorized libraries from loading into a system process. Reassess bi-annually, or more frequently.		●	●
v7	2.6 Address unapproved software Ensure that unauthorized software is either removed or the inventory is updated in a timely manner	●	●	●

5.1.3 Ensure Signed System Volume (SSV) Is Enabled (Automated)

Profile Applicability:

- Level 1

Description:

Signed System Volume is a security feature introduced in macOS 11.0 Big Sur.

During system installation, a SHA-256 cryptographic hash is calculated for all immutable system files and stored in a Merkle tree which itself is hashed as the Seal. Both are stored in the metadata of the snapshot created of the System volume.

The seal is verified by the boot loader at startup. macOS will not boot if system files have been tampered with. If validation fails, the user will be instructed to reinstall the operating system.

During read operations for files located in the Signed System Volume, a hash is calculated and compared to the value stored in the Merkle tree.

Rationale:

Running without Signed System Volume on a production system could run the risk of Apple software that integrates directly with macOS being modified.

Impact:

Apple Software that integrates with the operating system could become compromised.

Audit:

Run the following command to verify that Signed System Volume is enabled:

```
% /usr/bin/sudo /usr/bin/csrutil authenticated-root status

Authenticated Root status: enabled
```

Remediation:

If SSV has been disabled, assume that the operating system has been compromised. Back up any files, and do a clean install to a known good Operating System.

References:

1. https://developer.apple.com/news/?id=3xpv8r2m
2. https://eclecticlight.co/2020/11/30/is-big-surs-system-volume-sealed/
3. https://eclecticlight.co/2020/06/25/big-surs-signed-system-volume-added-security-protection/
4. https://support.apple.com/guide/security/signed-system-volume-security-secd698747c9/web
5. https://support.apple.com/guide/mac-help/what-is-a-signed-system-volume-mchl0f9af76f/mac

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.6 Encrypt Data on End-User Devices Encrypt data on end-user devices containing sensitive data. Example implementations can include: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.	●	●	●
v8	3.11 Encrypt Sensitive Data at Rest Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		●	●
v7	13.6 Encrypt the Hard Drive of All Mobile Devices. Utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices.	●	●	●
v7	14.8 Encrypt Sensitive Information at Rest Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			●

5.1.4 Ensure Appropriate Permissions Are Enabled for System Wide Applications (Automated)

Profile Applicability:

- Level 1

Description:

Applications in the System Applications Directory (/Applications) should be world-executable since that is their reason to be on the system. They should not be world-writable and allow any process or user to alter them for other processes or users to then execute modified versions.

Rationale:

Unauthorized modifications of applications could lead to the execution of malicious code.

Impact:

Applications changed will no longer be world-writable. Depending on the environment, there will be different risk tolerances on each non-conforming application. Global changes should not be performed where mission-critical applications are misconfigured.

Audit:

Run the following command to verify that all applications have the correct permissions:

```
% /usr/bin/sudo /usr/bin/find /System/Volumes/Data/Applications -iname
"*\.app" -type d -perm -2 -ls | grep -v Xcode.app | /usr/bin/wc -l |
/usr/bin/xargs

0
```

Remediation:

Run the following command to change the permissions for each application that does not meet the requirements:

```
% /usr/bin/sudo IFS=$'\n'
for apps in $( /usr/bin/find /System/Volumes/Data/Applications -iname
"*\.app" -type d -perm -2 | grep -v Xcode.app ); do
  /bin/chmod -R o-w "$apps"
done
```

Note: Global changes should not be performed where mission-critical applications are part of the improperly permissioned applications.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

5.1.5 Ensure No World Writable Folders Exist in the System Folder (Automated)

Profile Applicability:

- Level 1

Description:

Software sometimes insists on being installed in the `/System/Volumes/Data/System` Directory and has inappropriate world-writable permissions.

Macs with writable files in System should be investigated forensically. A file with open writable permissions is a sign of at best a rogue application. It could also be a sign of a computer compromise and a persistent presence on the system.

Rationale:

Folders in `/System/Volumes/Data/System` should not be world-writable. The audit check excludes the `downloadDir` folder that is part of Apple's default user template.

Impact:

Changing file permissions could disrupt the use of applications that rely on files in the System Folder with vulnerable permissions.

Audit:

Run the following command to check for directories in the /System folder that are world-writable:

```
% /usr/bin/sudo /usr/bin/find /System/Volumes/Data/System -type d -perm -2 -
ls | /usr/bin/grep -v "downloadDir" | /usr/bin/wc -l | /usr/bin/xargs

0
```

Remediation:

Run the following command to set permissions so that folders are not world-writable in the /System folder:

```
% /usr/bin/sudo IFS=$'\n'
for sysPermissions in $( /usr/bin/sudo /usr/bin/find
/System/Volumes/Data/System -type d -perm -2 | /usr/bin/grep -v "downloadDir"
); do
  /bin/chmod -R o-w "$sysPermissions"
done
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

5.1.6 Ensure No World Writable Folders Exist in the Library Folder (Automated)

Profile Applicability:

- Level 2

Description:

Software sometimes insists on being installed in the `/System/Volumes/Data/Library Directory` and has inappropriate world-writable permissions.

Rationale:

Folders in `/System/Volumes/Data/Library` should not be world-writable. The audit check excludes the `/System/Volumes/Data/Library/Caches` and `/System/Volumes/Data/Library/Preferences/Audio/Data` folders where the sticky bit is set.

Audit:

Run the following to verify that no directories in the `/System/Volumes/Data/Library` folder are world-writable:

```
% /usr/bin/sudo /usr/bin/find /System/Volumes/Data/Library -type d -perm -2 -
ls | /usr/bin/grep -v Caches | /usr/bin/grep -v /Preferences/Audio/Data |
/usr/bin/wc -l | /usr/bin/xargs

0
```

Remediation:

Run the following command to set permissions so that folders are not world-writable in the `/System/Volumes/Data/Library` folder:

```
% /usr/bin/sudo IFS=$'\n'
for libPermissions in $( /usr/bin/find /System/Volumes/Data/Library -type d -
perm -2 | /usr/bin/grep -v Caches | /usr/bin/grep -v /Preferences/Audio/Data
); do
  /bin/chmod -R o-w "$libPermissions"
done
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user’s need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

5.2 Password Management

Password security is an important part of general IT security where passwords are in use. For macOS, passwords are still much more widely used than other methods for account access. While there are other authentication and authorization methods for access from a macOS computer to organizational services, console access to the Mac is probably done using a password. This section contains password controls.

Apple has provided sufficient security controls to resist password attacks against the locked console, thus the CIS benchmark no longer recommends locking the keychain in addition to locking the console or display.

Recent updates based on research by NIST in SP800-63 call into question traditional password complexity and rotation requirements. Sticky notes are not a password management program, and password vault APIs are under increasing attack. Ideally, the user will remember their important passwords. The new understanding has informed changes to the previous password recommendations.

Length, threshold, and a yearly rotation requirement are the only scored controls below. Other controls will remain as unscored options. Passwords used for macOS are likely to also function as encryption keys for FileVault. Depending on the information confidentiality on FileVault volumes, stronger passwords may be required than are necessary to pass the controls in this Benchmark.

Apple-supported solutions for managing local passwords on macOS are to use either an XML file that contains password rules that are imported with pwpolicy or through the use of a profile. In either case, the controls in this section can be implemented with an organizationally-approved password policy.

Before applying your organization's password policy, the existing password policy should be cleared so there is no outdated or conflicting legacy settings in the password policy. A pre-existing password policly could result in false results. To clear the password policy before applying the newest options, use the command `/usr/bin/sudo /usr/bin/pwpolicy -clearaccountpolicies`

Content is available where security hardening content is available and is native to Management suites and MDM tools.

Content also available here: https://github.com/ronc-LAemigre/macos-sec-config

NIST guidance on passwords starting at 5.1.1.1

https://pages.nist.gov/800-63-3/sp800-63b.html

Additional references:

- https://developer.apple.com/documentation/devicemanagement/passcode
- https://krypted.com/mac-security/programatically-setting-password-policies/
- https://www.macworld.co.uk/news/flaw-mac-t2-chip-passwords-3813616/

Note: The current method of creating and setting password policy is using the `pwpolicy -setglobalpolicy` command. That command has been deprecated by Apple, but is still in use in the current version of macOS. The Benchmark will continue to use this command line method for passwords until Apple removes it from the OS. Setting password policy with mobile configuration profiles is the preferred method going forward.

5.2.1 Ensure Password Account Lockout Threshold Is Configured (Automated)

Profile Applicability:

- Level 1

Description:

The account lockout threshold specifies the amount of times a user can enter an incorrect password before a lockout will occur.

Ensure that a lockout threshold is part of the password policy on the computer.

Rationale:

The account lockout feature mitigates brute-force password attacks on the system.

Impact:

The number of incorrect log on attempts should be reasonably small to minimize the possibility of a successful password attack, while allowing for honest errors made during a normal user log on.

The locked account will auto-unlock after a few minutes when bad password attempts stop. The computer will accept the still-valid password if remembered or recovered.

Audit:

Terminal Method:
Run the following command to verify that the number of failed attempts is less than or equal to 5:

```
$ /usr/bin/sudo /usr/bin/pwpolicy -getaccountpolicies 2> /dev/null |
/usr/bin/tail +2 | /usr/bin/xmllint --xpath
'//dict/key[text()="policyAttributeMaximumFailedAuthentications"]/following-
sibling::integer[1]/text()' -
```

The output should be ≤ 5

Remediation:

Run the following command to set the maximum number of failed login attempts to less than or equal to 5:

```
% /usr/bin/sudo /usr/bin/pwpolicy -n /Local/Default -setglobalpolicy
"maxFailedLoginAttempts=<value≤5>"
```

References:

1. CIS Password Policy - https://workbench.cisecurity.org/communities/113
2. https://support.apple.com/guide/security/passcodes-and-passwords-sec20230a10d/web

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.2 Establish an Access Revoking Process Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.	●	●	●
v7	16.7 Establish Process for Revoking Access Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor . Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.		●	●

5.2.2 Ensure Password Minimum Length Is Configured (Automated)

Profile Applicability:

- Level 1

Description:

A minimum password length is the fewest number of characters a password can contain to meet a system's requirements.

Ensure that a minimum of a 15-character password is part of the password policy on the computer.

Where the confidentiality of encrypted information in FileVault is more of a concern, requiring a longer password or passphrase may be sufficient rather than imposing additional complexity requirements that may be self-defeating.

Rationale:

Information systems that are not protected with strong password schemes including passwords of minimum length provide a greater opportunity for attackers to crack the password and gain access to the system.

Impact:

Short passwords can be easily attacked.

Audit:

Run the following command to verify that the password length is greater than or equal to 15:

```
% /usr/bin/sudo /usr/bin/pwpolicy -getaccountpolicies | /usr/bin/grep -e
"policyAttributePassword matches" | /usr/bin/cut -b 46-53 | /usr/bin/cut -
d',' -f1 | /usr/bin/cut -d'{' -f2
```

The output value should be ≥ `15`

Remediation:

Run the following command to set the password length to greater than or equal to 15:

```
% /usr/bin/sudo /usr/bin/pwpolicy -n /Local/Default -setglobalpolicy
"minChars=<value≥15>"
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

5.2.3 Ensure Complex Password Must Contain Alphabetic Characters Is Configured (Automated)

Profile Applicability:

- Level 2

Description:

Complex passwords contain one character from each of the following classes: English uppercase letters, English lowercase letters, Westernized Arabic numerals, and non-alphanumeric characters.

Ensure that an Alphabetic character is part of the password policy on the computer.

Rationale:

The more complex a password, the more resistant it will be against persons seeking unauthorized access to a system.

Impact:

Password policy should be in effect to reduce the risk of exposed services being compromised easily through dictionary attacks or other social engineering attempts.

Audit:

Run the following command to verify that the password requires at least one letter:

```
% pref=$(/usr/bin/sudo /usr/bin/pwpolicy -getaccountpolicies | /usr/bin/sudo
/usr/bin/grep -A1 minimumLetters | /usr/bin/sudo /usr/bin/tail -1 |
/usr/bin/sudo /usr/bin/cut -d'>' -f2 | /usr/bin/sudo /usr/bin/cut -d '<' -f1)
&& if [[ "$pref" != "" && pref -ge 1 ]]; then echo "true"; else echo "false";
fi

true
```

Remediation:

Terminal Method:
Run the following command to set that passwords must contain at least one letter:

```
% /usr/bin/sudo /usr/bin/pwpolicy -n /Local/Default -setglobalpolicy -
setaccountpolicies "requiresAlpha=<value≥1>"
```

Additional Information:

Note: The CIS macOS community has decided to not require the additional password complexity settings (Recommendations 5.3 - 5.6). Because of that, we have left the complexity recommendations as a manual assessment. Since there are a large amount of admins in the greater macOS world that do need these settings, we include both the guidance for the proper setting as well as probes for CIS-CAT to test.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

5.2.4 Ensure Complex Password Must Contain Numeric Character Is Configured (Automated)

Profile Applicability:

- Level 2

Description:

Complex passwords contain one character from each of the following classes: English uppercase letters, English lowercase letters, Westernized Arabic numerals, and non-alphanumeric characters.

Ensure that a number or numeric value is part of the password policy on the computer.

Rationale:

The more complex a password, the more resistant it will be against persons seeking unauthorized access to a system.

Impact:

Password policy should be in effect to reduce the risk of exposed services being compromised easily through dictionary attacks or other social engineering attempts.

Audit:

Run the following command to verify that passwords require at least one number:

```
% pref=$(/usr/bin/sudo /usr/bin/pwpolicy -getaccountpolicies | /usr/bin/sudo
/usr/bin/grep -A1 minimumNumericCharacters | /usr/bin/sudo /usr/bin/tail -1 |
/usr/bin/sudo /usr/bin/cut -d '>' -f2 | /usr/bin/sudo /usr/bin/cut -d '<' -
f1) && if [[ "$pref" != "" && pref -ge 1 ]]; then echo "true"; else echo
"false"; fi

true
```

Remediation:

Run the following command to set passwords to require at least one number:

```
% /usr/bin/sudo /usr/bin/pwpolicy -n /Local/Default -setglobalpolicy -
setaccountpolicies "requiresNumeric=<value≥1>"
```

Additional Information:

Note: The CIS macOS community has decided to not require the additional password complexity settings (Recommendations `5.3` - `5.6`). Because of that, we have left the complexity recommendations as a manual assessment. Since there are a large amount of admins in the greater macOS world that do need these settings, we include both the guidance for the proper setting as well as probes for CIS-CAT to test.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

5.2.5 Ensure Complex Password Must Contain Special Character Is Configured (Automated)

Profile Applicability:

- Level 2

Description:

Complex passwords contain one character from each of the following classes: English uppercase letters, English lowercase letters, Westernized Arabic numerals, and non-alphanumeric characters. Ensure that a special character is part of the password policy on the computer.

Rationale:

The more complex a password, the more resistant it will be against persons seeking unauthorized access to a system.

Impact:

Password policy should be in effect to reduce the risk of exposed services being compromised easily through dictionary attacks or other social engineering attempts.

Audit:

Run the following command to verify that the password requires at least one special character:

```
% /usr/bin/sudo pref=$(/usr/bin/sudo pwpolicy -getaccountpolicies  |
/usr/bin/sudo /usr/bin/grep -A1 minimumSymbols | /usr/bin/sudo /usr/bin/tail
-1 | /usr/bin/sudo /usr/bin/cut -d '>' -f2 | /usr/bin/sudo /usr/bin/cut -d
'<' -f1) && if [[ "$pref" != "" && pref -ge 1 ]]; then echo "true"; else echo
"false"; fi

true
```

Remediation:

Run the following command to set passwords to require at least one special character:

```
% /usr/bin/sudo /usr/bin/pwpolicy -n /Local/Default -setglobalpolicy -
setaccountpolicies "requiresSymbol=<value≥1>"
```

Additional Information:

Note: The CIS macOS community has decided to not require the additional password complexity settings (Recommendations 5.3 - 5.6). Because of that, we have left the complexity recommendations as a manual assessment. Since there are a large amount of admins in the greater macOS world that do need these settings, we include both the guidance for the proper setting as well as probes for CIS-CAT to test.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

5.2.6 Ensure Complex Password Must Contain Uppercase and Lowercase Characters Is Configured (Automated)

Profile Applicability:

- Level 2

Description:

Complex passwords contain one character from each of the following classes: English uppercase letters, English lowercase letters, Westernized Arabic numerals, and non-alphanumeric characters.

Ensure that both uppercase and lowercase letters are part of the password policy on the computer.

Rationale:

The more complex a password, the more resistant it will be against persons seeking unauthorized access to a system.

Impact:

Password policy should be in effect to reduce the risk of exposed services being compromised easily through dictionary attacks or other social engineering attempts.

Audit:

Run the following command to verify that the password requires an upper and lower case letter:

```
% /usr/bin/sudo pref=$(/usr/bin/pwpolicy -getaccountpolicies | /usr/bin/grep
-A1 minimumMixedCaseCharacters | /usr/bin/tail -1 | /usr/bin/cut -d'>' -f2 |
/usr/bin/cut -d '<' -f1) && if [[ "$pref" != "" && pref -ge 1 ]]; then echo
"true"; else echo "false"; fi

true
```

Remediation:

Run the following command to set passwords to require an upper and lower case letter:

```
% /usr/bin/sudo /usr/bin/pwpolicy -n /Local/Default -setglobalpolicy
"requiresMixedCase=<value≥1>"
```

Additional Information:

Note: The CIS macOS community has decided to not require the additional password complexity settings (Recommendations `5.3` - `5.6`). Because of that, we have left the complexity recommendations as a manual assessment. Since there are a large amount of admins in the greater macOS world that do need these settings, we include both the guidance for the proper setting as well as probes for CIS-CAT to test.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

5.2.7 Ensure Password Age Is Configured (Automated)

Profile Applicability:

- Level 1

Description:

Over time, passwords can be captured by third parties through mistakes, phishing attacks, third-party breaches, or merely brute-force attacks. To reduce the risk of exposure and to decrease the incentives of password reuse (passwords that are not forced to be changed periodically generally are not ever changed), users should reset passwords periodically. This control uses 365 days as the acceptable value. Some organizations may be more or less restrictive. This control mainly exists to mitigate against password reuse of the macOS account password in other realms that may be more prone to compromise. Attackers take advantage of exposed information to attack other accounts.

Rationale:

Passwords should be changed periodically to reduce exposure.

Impact:

Required password changes will lead to some locked computers requiring admin assistance.

Audit:

Run the following command to verify that the password expires after at most 365 days:

```
% /usr/bin/sudo pref=$(/usr/bin/pwpolicy -getaccountpolicies | /usr/bin/grep
-A1 policyAttributeExpiresEveryNDays | /usr/bin/tail -1 | /usr/bin/cut -d'>'
-f2 | /usr/bin/cut -d '<' -f1) && if [[ "$pref" != "" && pref -le 365 ]];
then echo "true"; else echo "false"; fi

true
```

Remediation:

Run the following command to require that passwords expire after at most 365 days:

```
% /usr/bin/sudo /usr/bin/pwpolicy -n /Local/Default -setglobalpolicy
"maxMinutesUntilChangePassword=<value≤525600>"
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.3 Disable Dormant Accounts Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.	●	●	●
v7	16.9 Disable Dormant Accounts Automatically disable dormant accounts after a set period of inactivity.	●	●	●

5.2.8 Ensure Password History Is Configured (Automated)

Profile Applicability:

- Level 1

Description:

Over time, passwords can be captured by third parties through mistakes, phishing attacks, third-party breaches, or merely brute-force attacks. To reduce the risk of exposure and to decrease the incentives of password reuse (passwords that are not forced to be changed periodically generally are not ever changed), users must reset passwords periodically. This control ensures that previous passwords are not reused immediately by keeping a history of previous password hashes. Ensure that password history checks are part of the password policy on the computer. This control checks whether a new password is different than the previous 15. The latest NIST guidance based on exploit research referenced in this section details how one of the greatest risks is password exposure rather than password cracking. Passwords should be changed to a new unique value whenever a password might have been exposed to anyone other than the account holder. Attackers have maintained persistent control based on predictable password change patterns and substantially different patterns should be used in case of a leak.

Rationale:

Old passwords should not be reused.

Impact:

Required password changes will lead to some locked computers requiring admin assistance.

Audit:

Run the following command to verify that the password is required to be different from at least the last 15 passwords:

```
% /usr/bin/sudo pref$=(/usr/bin/pwpolicy -getaccountpolicies | /usr/bin/grep
-A1 policyAttributePasswordHistoryDepth | /usr/bin/tail -1 | /usr/bin/cut -
d'>' -f2 | /usr/bin/cut -d '<' -f1) && if [[ "$pref" != "" && pref -ge 1 ]];
then echo "true"; else echo "false"; fi

true
```

Remediation:

Run the following command to require that the password must be different from at least the last 15 passwords:

```
% /usr/bin/sudo /usr/bin/pwpolicy -n /Local/Default -setglobalpolicy
"usingHistory=<value≥15>"
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

5.3 Ensure the Sudo Timeout Period Is Set to Zero (Automated)

Profile Applicability:

- Level 1

Description:

The sudo command allows the user to run programs as the root user. Working as the root user allows the user an extremely high level of configurability within the system. This control, along with the control to use a separate timestamp for each tty, limits the window where an unauthorized user, process, or attacker could utilize legitimate credentials that are valid for longer than required.

Rationale:

The `sudo` command stays logged in as the root user for five minutes before timing out and re-requesting a password. This five-minute window should be eliminated since it leaves the system extremely vulnerable. This is especially true if an exploit were to gain access to the system, since they would be able to make changes as a root user.

Impact:

This control has a serious impact where users often have to use sudo. It is even more of an impact where users have to use sudo multiple times in quick succession as part of normal work processes. Organizations with that common use case will likely find this control too onerous and are better to accept the risk of not requiring a 0 grace period.

In some ways the use of sudo -s, which is undesirable, is better than a long grace period since that use does change the hash to show that it is a root shell rather than a normal shell where sudo commands will be implemented without a password.

Audit:

Perform the following to verify the sudo timeout period:

```
% /usr/bin/sudo /usr/bin/sudo -V | /usr/bin/grep -c "Authentication timestamp
timeout: 0.0 minutes"

1
```

Run the following commands to verify that the root is the owner of the `/etc/sudoers.d` folder, and that wheel is the group

```
% /usr/bin/stat /etc/sudoers.d

16777229 19662948 drwxr-xr-x 2 root wheel 0 64 "Jun  7 23:12:24 2022" "May  9
17:30:48 2022" "Jun  7 23:12:24 2022" "May  9 17:30:48 2022" 4096 0 0
/etc/sudoers.d
```

Remediation:

Run the following command to edit the sudo settings:

```
% /usr/bin/sudo /usr/sbin/visudo -f /etc/sudoers.d/<configuration file name>
```

example: `$ /usr/bin/sudo /usr/sbin/visudo -f /etc/sudoers.d/10_cissudoconfiguration`
Note: Unlike other Unix and/or Linux distros, macOS will ignore configuration files in the sudoers.d folder that contain a `.` so do not add a file extension to the configuration file.
Add the line `Defaults timestamp_timeout=0` to the configuration file.
If /etc/sudoers.d/ is not owned by root or in the wheel group, run the following to change ownership and group:

```
% /usr/bin/sudo /usr/sbin/chown -R root:wheel /etc/security/sudoers.d/
```

Additional Information:

In previous iterations and OS versions of the macOS Benchmark, the guidance was to edit the sudoers file directly. While this would properly configure the OS, any update would change the settings back to the default configuration. Creating a configuration file in the `/etc/sudoers.d/` folder will not be modified on an OS update and will keep the proper configuration.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 Configure Automatic Session Locking on Enterprise Assets Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	●	●	●
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

5.4 Ensure a Separate Timestamp Is Enabled for Each User/tty Combo (Automated)

Profile Applicability:

- Level 1

Description:

Using tty tickets ensures that a user must enter the sudo password in each Terminal session.

With sudo versions 1.8 and higher, introduced in 10.12, the default value is to have tty tickets for each interface so that root access is limited to a specific terminal. The default configuration can be overwritten or not configured correctly on earlier versions of macOS.

Rationale:

In combination with removing the sudo timeout grace period, a further mitigation should be in place to reduce the possibility of a background process using elevated rights when a user elevates to root in an explicit context or tty.

Additional mitigation should be in place to reduce the risk of privilege escalation of background processes.

Impact:

This control should have no user impact. Developers or installers may have issues if background processes are spawned with different interfaces than where sudo was executed.

Audit:

Run the following commands to verify that the default sudoers controls are in place with explicit tickets per tty:

```
% /usr/bin/sudo /usr/bin/sudo -V | /usr/bin/grep -c "Type of authentication
timestamp record: tty"

1
```

Remediation:

Run the following command to edit the sudo settings:

```
% /usr/bin/sudo /usr/sbin/visudo -f /etc/sudoers.d/<configuration file name>
```

example: `% /usr/bin/sudo /usr/sbin/visudo -f /etc/sudoers.d/10_cissudoconfiguration`
Note: Unlike other Unix and/or Linux distros, macOS will ignore configuration files in the sudoers.d folder that contain a `.` so do not add a file extension to the configuration file.
Add the line `Defaults timestamp_type=tty` to the configuration file.
Note: The `Defaults timestamp_type=tty` line can be added to an existing configuration file or a new one. That will depend on your organization's preference and works either way.

Default Value:

If no value is set, the default value of tty_tickets enabled will be used.

References:

1. https://github.com/jorangreef/sudo-prompt/issues/33

Additional Information:

In previous iterations and OS versions of the macOS Benchmark, the guidance was to edit the sudoers file directly. While this would properly configure the OS, any update would change the settings back to the default configuration. Creating a configuration file in the `/etc/sudoers.d/` folder will not be modified on an OS update and will keep the proper configuration.

With the configuration file, there is no need to remove the `Defaults !tty_tickets` line from the `visudo` settings. The configuration file will take precedent.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 Configure Automatic Session Locking on Enterprise Assets Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	●	●	●
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

5.5 Ensure the "root" Account Is Disabled (Automated)

Profile Applicability:

- Level 1

Description:

The root account is a superuser account that has access privileges to perform any actions and read/write to any file on the computer. With some versions of Linux, the system administrator may commonly use the root account to perform administrative functions.

Rationale:

Enabling and using the root account puts the system at risk since any successful exploit or mistake while the root account is in use could have unlimited access privileges within the system. Using the `sudo` command allows users to perform functions as a root user while limiting and password protecting the access privileges. By default the root account is not enabled on a macOS computer. An administrator can escalate privileges using the `sudo` command (use `-s` or `-i` to get a root shell).

Impact:

Some legacy POSIX software might expect an available root account.

Audit:

Run the following command to verify the the root user has not been enabled:

```
% /usr/bin/sudo /usr/bin/dscl . -read /Users/root AuthenticationAuthority


No such key: AuthenticationAuthority
```

Remediation:

Run the following command to disable the root user:

```
% /usr/bin/sudo /usr/sbin/dsenableroot -d

username = root
user password:
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	●	●	●
v7	4.3 Ensure the Use of Dedicated Administrative Accounts Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.	●	●	●

5.6 Ensure an Administrator Account Cannot Login to Another User's Active and Locked Session (Automated)

Profile Applicability:

- Level 1

Description:

macOS has a privilege that can be granted to any user that will allow that user to unlock active users' sessions.

Rationale:

Disabling the administrator's and/or user's ability to log into another user's active and locked session prevents unauthorized persons from viewing potentially sensitive and/or personal information.

Impact:

While Fast user switching is a workaround for some lab environments, especially where there is even less of an expectation of privacy, this setting change may impact some maintenance workflows.

Audit:

Run the following command to verify that a user cannot log into another user's active and/or locked session:

```
% /usr/bin/sudo /usr/bin/security authorizationdb read
system.login.screensaver 2>&1 | /usr/bin/grep -c 'authenticate-session-owner'

1
```

Remediation:

Run the following command to disable a user logging into another user's active and/or locked session:

```
% /usr/bin/sudo /usr/bin/security authorizationdb write
system.login.screensaver authenticate-session-owner

YES (0)
```

References:

1. https://derflounder.wordpress.com/2014/02/16/managing-the-authorization-database-in-os-x-mavericks/
2. https://www.jamf.com/jamf-nation/discussions/18195/system-login-screensaver

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 Configure Automatic Session Locking on Enterprise Assets Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	●	●	●
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

5.7 Ensure a Login Window Banner Exists (Automated)

Profile Applicability:

- Level 2

Description:

A Login window banner warning informs the user that the system is reserved for authorized use only. It enforces an acknowledgment by the user that they have been informed of the use policy in the banner if required. The system recognizes either the `.txt` and the `.rtf` formats.

Rationale:

An access warning may reduce a casual attacker's tendency to target the system. Access warnings may also aid in the prosecution of an attacker by evincing the attacker's knowledge of the system's private status, acceptable use policy, and authorization requirements.

Impact:

Users will have to click on the window with the Login text before logging into the computer.

Audit:

Run the following command to verify the login window text:

```
% /usr/bin/sudo /bin/cat /Library/Security/PolicyBanner.*
```

If the output includes `no matches found: /Library/Security/PolicyBanner.*` the system is not compliant.
Run the following to verify permissions of the policy banner file:

```
% /usr/bin/stat -f %A /Library/Security/PolicyBanner.*
```

The output should have `4` as the 3rd digit.
If there is an output, then the policy banner will not display.

example:

```
% /usr/bin/sudo /bin/cat /Library/Security/PolicyBanner.txt

Center for Internet Security Test Message

% /usr/bin/sudo /bin/cat /Library/Security/PolicyBanner.rtf

{\rtf1\ansi\ansicpg1252\cocoartf1561\cocoasubrtf610
{\fonttbl\f0\fswiss\fcharset0 Helvetica;}
{\colortbl;\red255\green255\blue255;}
{\*\expandedcolortbl;;}
\margl1440\margr1440\vieww10800\viewh8400\viewkind0
\pard\tx566\tx1133\tx1700\tx2267\tx2834\tx3401\tx3968\tx4535\tx5102\tx5669\tx
6236\tx6803\pardirnatural\partightenfactor0

\f0\fs24 \cf0 Center for Internet Security Test Message}

% /usr/bin/sudo /bin/cat /Library/Security/PolicyBanner.*

{\rtf1\ansi\ansicpg1252\cocoartf1561\cocoasubrtf610
{\fonttbl\f0\fswiss\fcharset0 Helvetica;}
{\colortbl;\red255\green255\blue255;}
{\*\expandedcolortbl;;}
\margl1440\margr1440\vieww10800\viewh8400\viewkind0
\pard\tx566\tx1133\tx1700\tx2267\tx2834\tx3401\tx3968\tx4535\tx5102\tx5669\tx
6236\tx6803\pardirnatural\partightenfactor0

\f0\fs24 \cf0 Center for Internet Security Test Message}Center for Internet
Security Test Message

% /usr/bin/sudo stat -f %A /Library/Security/PolicyBanner.*

644
```

Remediation:

Run the following commands to create or edit the login window text and set the proper permissions:
Edit (or create) a `PolicyBanner.txt` or `PolicyBanner.rtf` file, in the `/Library/Security/` folder, to include the required login window banner text.
Perform the following to set permissions on the policy banner file:

```
% /usr/bin/sudo /usr/sbin/chown o+r /Library/Security/PolicyBanner.txt

% /usr/bin/sudo /usr/sbin/chown o+r /Library/Security/PolicyBanner.rtf
```

Note: If your organization uses an `.rtfd` file to set the policy banner, run `% /usr/bin/sudo /usr/sbin/chown -R o+rx /Library/Security/PolicyBanner.rtfd` to update the permissions.

References:

1. https://support.apple.com/en-au/HT202277

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

5.8 Ensure the Guest Home Folder Does Not Exist (Automated)

Profile Applicability:

- Level 1

Description:

In the previous two controls, the guest account login has been disabled and sharing to guests has been disabled, as well. There is no need for the legacy Guest home folder to remain in the file system. When normal user accounts are removed, you have the option to archive it, leave it in place, or delete. In the case of the guest folder, the folder remains in place without a GUI option to remove it. If at some point in the future a Guest account is needed, it will be re-created. The presence of the Guest home folder can cause automated audits to fail when looking for compliant settings within all User folders, as well. Rather than ignoring the folder's continued existence, it is best removed.

Rationale:

The Guest home folders are unneeded after the Guest account is disabled and could be used inappropriately.

Impact:

The Guest account should not be necessary after it is disabled, and it will be automatically re-created if the Guest account is re-enabled.

Audit:

Run the following command to verify if the Guest user home folder exists:

```
% /usr/bin/sudo /bin/ls /Users/ | /usr/bin/grep Guest
```

Remediation:

Run the following command to remove the Guest user home folder:

```
% /usr/bin/sudo /bin/rm -R /Users/Guest
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

5.9 Ensure XProtect Is Running and Updated (Automated)

Profile Applicability:

- Level 1

Description:

XProtect is Apple's native signature-based antivirus technology. XProtect both finds and blocks the execution of known malware. There are many AV and Endpoint Threat Detection and Response (ETDR) tools available for Mac OS. The native Apple provisioned tool looks for specific known malware and is completely integrated into the OS. No matter what other tools are being used, XProtect should have the latest signatures available.

Rationale:

Apple creates signatures for known malware that actually affects Macs and that knowledge should be leveraged.

Impact:

Some organizations may have effective Mac OS anti-malware tools that XProtect conflicts with.

Audit:

Run the following command to verify that XProtect is running and up-to-date:

```
% /usr/bin/sudo /bin/launchctl list | /usr/bin/grep -cE
"(com.apple.XprotectFramework.PluginService$|com.apple.XProtect.daemon.scan$)
"

2
```

Note: XProtect can only be disabled while SIP (System Integrity Protection) is disabled. If XProtect is disabled while SIP is enabled, there needs to be a more significant investigation on this system, as it is likely compromised in some way.
To verify the updates to XProtect, run the following command:

```
% /usr/bin/sudo /usr/sbin/system_profiler SPInstallHistoryDataType | grep -A
5 "XProtectPlistConfigData"
```

Remediation:

Run the following command to enable and update XProtect:

```
% /usr/bin/sudo /bin/launchctl load -w
/Library/Apple/System/Library/LaunchDaemons/com.apple.XProtect.daemon.scan.pl
ist

% /usr/bin/sudo /bin/launchctl load -w
/Library/Apple/System/Library/LaunchDaemons/com.apple.XprotectFramework.Plugi
nService.plist

% /usr/bin/sudo /usr/sbin/softwareupdate -l --background-critical

softwareupdate[97180]: Triggering a background check with forced scan
(critical and config-data updates only) ...
```

Note: Xprotect can only be enabled/disabled if SIP (System Integrity Protection) is disabled. If Xprotect is disabled, the system might be compromised and needs to be investigated.

References:

1. https://eclecticlight.co/2021/10/27/silently-updated-security-data-files-in-monterey/
2. https://eclecticlight.co/2020/12/14/silently-updated-security-data-files-in-big-sur/
3. https://eclecticlight.co/2019/10/17/security-data-files-how-theyve-changed-in-catalina/
4. https://eclecticlight.co/2022/05/12/apple-has-pushed-an-update-to-xprotect-21/
5. https://support.apple.com/guide/security/protecting-against-malware-sec469d47bd8/web
6. https://eclecticlight.co/2023/06/12/malware-detection-and-remediation-by-xprotect-remediator/

Additional Information:

To verify the XProtect Remediator logs run the following command:

```
% /usr/bin/sudo /usr/bin/log show --predicate 'subsystem ==
"com.apple.XProtectFramework.PluginAPI" AND category ==
"XPEvent.structured"' --info --last 1d' to check logs'
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●
v8	10.2 Configure Automatic Anti-Malware Signature Updates Configure automatic updates for anti-malware signature files on all enterprise assets.	●	●	●
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	8.2 Ensure Anti-Malware Software and Signatures are Updated Ensure that the organization's anti-malware software updates its scanning engine and signature database on a regular basis.	●	●	●
v7	8.4 Configure Anti-Malware Scanning of Removable Devices Configure devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected.	●	●	●

5.10 Ensure Secure Keyboard Entry Terminal.app Is Enabled (Automated)

Profile Applicability:

- Level 1

Description:

Secure Keyboard Entry prevents other applications on the system and/or network from detecting and recording what is typed into Terminal. Unauthorized applications and malicious code could intercept keystrokes entered in the Terminal.

Rationale:

Enabling Secure Keyboard Entry minimizes the risk of a key logger detecting what is entered in Terminal.

Impact:

Enabling this in Terminal would prevent an application that is otherwise validly intercepting keyboard input from intercepting that input in Terminal.app. This could impact productivity tools.

Audit:

For each user, run the following command to verify that keyboard entries in Terminal are secured:

```
% /usr/bin/sudo for i in $(/usr/bin/find /Users -type d -maxdepth 1);
do
  PREF=$i/Library/Preferences/com.apple.Terminal
  if [ -e $PREF.plist ]
  then
  echo -n "Checking User: '$i': "
  /usr/bin/defaults read $PREF.plist SecureKeyboardEntry
  fi
done
Checking User: '/Users/<username>': 1
Checking User: '/Users/<username>': 0
```

Any user that contains the output `0` is not in compliance

Remediation:

Run the following command to ensure keyboard entries are secure in Terminal for every user that is non-compliant:

```
% /usr/bin/sudo -u <username> /usr/bin/defaults write -app Terminal
SecureKeyboardEntry -bool true
```

References:

1. https://support.apple.com/en-ca/guide/terminal/trml109/mac
2. https://developer.apple.com/library/archive/technotes/tn2150/_index.html
3. https://krypted.com/mac-os-x/secure-keyboard-entry-on-macos/

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	4.1 Maintain Inventory of Administrative Accounts Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

5.11 Ensure Show All Filename Extensions Setting is Enabled (Automated)

Profile Applicability:

- Level 1

Description:

A filename extension is a suffix added to a base filename that indicates the base filename's file format.

Rationale:

Visible filename extensions allow the user to identify the file type and the application it is associated with which leads to quick identification of misrepresented malicious files.

Impact:

The user of the system can open files of unknown or unexpected filetypes if the extension is not visible.

Audit:

Run the following command to verify that displaying of file extensions is enabled:

```
% /usr/bin/sudo -u <username> /usr/bin/defaults read
/Users/<username>/Library/Preferences/.GlobalPreferences.plist
AppleShowAllExtensions

1
```

Remediation:

Run the following command to enable displaying of file extensions:

```
% /usr/bin/sudo -u <username> /usr/bin/defaults write
/Users/<username>/Library/Preferences/.GlobalPreferences.plist
AppleShowAllExtensions -bool true

% /usr/bin/sudo killall Finder
```

Default Value:

Filename extensions are turned off by default.

References:

1. https://blog.xpnsec.com/macos-filename-homoglyphs-revisited/
2. https://null-byte.wonderhowto.com/how-to/hacking-macos-create-fake-pdf-trojan-with-applescript-part-2-disguising-script-0184706/

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.3 Address Unauthorized Software Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.	●	●	●
v7	2.6 Address unapproved software Ensure that unauthorized software is either removed or the inventory is updated in a timely manner	●	●	●

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**Install Updates, Patches and Additional Security Software**		
1.1	Ensure All Apple-provided Software Is Current (Automated)	□	□
1.2	Ensure Auto Update Is Enabled (Automated)	□	□
1.3	Ensure Download New Updates When Available Is Enabled (Automated)	□	□
1.4	Ensure Install of macOS Updates Is Enabled (Automated)	□	□
1.5	Ensure Install Application Updates from the App Store Is Enabled (Automated)	□	□
1.6	Ensure Install Security Responses and System Files Is Enabled (Automated)	□	□
2	**System Settings**		
2.1	**Network**		
2.1.1	Ensure Firewall Is Enabled (Automated)	□	□
2.2	**General**		
2.2.1	**Date & Time**		
2.2.1.1	Ensure Set Time and Date Automatically Is Enabled (Automated)	□	□
2.2.1.2	Ensure the Time Service Is Enabled (Automated)	□	□
2.2.2	**Sharing**		
2.2.2.1	Ensure Remote Apple Events Is Disabled (Automated)	□	□
2.2.2.2	Ensure Content Caching Is Disabled (Automated)	□	□

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.3	**Privacy & Security**		
2.3.1	Ensure Sending Diagnostic and Usage Data to Apple Is Disabled (Automated)	□	□
2.3.2	Ensure Limit Ad Tracking Is Enabled (Automated)	□	□
2.3.3	Ensure Gatekeeper Is Enabled (Automated)	□	□
2.4	**Lock Screen**		
2.4.1	Ensure an Inactivity Interval of 20 Minutes Or Less for the Screen Saver Is Enabled (Automated)	□	□
2.4.2	Ensure Require Password After Screen Saver Begins or Display Is Turned Off Is Enabled for 5 Seconds or Immediately (Automated)	□	□
2.4.3	Ensure a Custom Message for the Login Screen Is Enabled (Automated)	□	□
2.4.4	Ensure Login Window Displays as Name and Password Is Enabled (Automated)	□	□
2.4.5	Ensure Show Password Hints Is Disabled (Automated)	□	□
2.5	**Login Password**		
2.5.1	Ensure Users' Accounts Do Not Have a Password Hint (Automated)	□	□
2.6	**Users & Groups**		
2.6.1	Ensure Guest Account Is Disabled (Automated)	□	□
2.6.2	Ensure Guest Access to Shared Folders Is Disabled (Automated)	□	□
2.6.3	Ensure Automatic Login Is Disabled (Automated)	□	□
3	**Logging and Auditing**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
3.1	Ensure Security Auditing Is Enabled (Automated)	□	□
3.2	Ensure Security Auditing Flags For User-Attributable Events Are Configured Per Local Organizational Requirements (Automated)	□	□
3.3	Ensure install.log Is Retained for 365 or More Days and No Maximum Size (Automated)	□	□
3.4	Ensure Security Auditing Retention Is Enabled (Automated)	□	□
3.5	Ensure Access to Audit Records Is Controlled (Automated)	□	□
3.6	Ensure Firewall Logging Is Enabled and Configured (Automated)	□	□
4	**Network Configurations**		
4.1	Ensure Bonjour Advertising Services Is Disabled (Automated)	□	□
4.2	Ensure HTTP Server Is Disabled (Automated)	□	□
4.3	Ensure NFS Server Is Disabled (Automated)	□	□
5	**System Access, Authentication, and Authorization**		
5.1	**File System Permissions and Access Controls**		
5.1.1	Ensure Home Folders Are Secure (Automated)	□	□
5.1.2	Ensure Apple Mobile File Integrity (AMFI) Is Enabled (Automated)	□	□
5.1.3	Ensure Signed System Volume (SSV) Is Enabled (Automated)	□	□
5.1.4	Ensure Appropriate Permissions Are Enabled for System Wide Applications (Automated)	□	□

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
5.1.5	Ensure No World Writable Folders Exist in the System Folder (Automated)	□	□
5.1.6	Ensure No World Writable Folders Exist in the Library Folder (Automated)	□	□
5.2	**Password Management**		
5.2.1	Ensure Password Account Lockout Threshold Is Configured (Automated)	□	□
5.2.2	Ensure Password Minimum Length Is Configured (Automated)	□	□
5.2.3	Ensure Complex Password Must Contain Alphabetic Characters Is Configured (Automated)	□	□
5.2.4	Ensure Complex Password Must Contain Numeric Character Is Configured (Automated)	□	□
5.2.5	Ensure Complex Password Must Contain Special Character Is Configured (Automated)	□	□
5.2.6	Ensure Complex Password Must Contain Uppercase and Lowercase Characters Is Configured (Automated)	□	□
5.2.7	Ensure Password Age Is Configured (Automated)	□	□
5.2.8	Ensure Password History Is Configured (Automated)	□	□
5.3	Ensure the Sudo Timeout Period Is Set to Zero (Automated)	□	□
5.4	Ensure a Separate Timestamp Is Enabled for Each User/tty Combo (Automated)	□	□
5.5	Ensure the "root" Account Is Disabled (Automated)	□	□
5.6	Ensure an Administrator Account Cannot Login to Another User's Active and Locked Session (Automated)	□	□
5.7	Ensure a Login Window Banner Exists (Automated)	□	□

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
5.8	Ensure the Guest Home Folder Does Not Exist (Automated)	□	□
5.9	Ensure XProtect Is Running and Updated (Automated)	□	□
5.10	Ensure Secure Keyboard Entry Terminal.app Is Enabled (Automated)	□	□
5.11	Ensure Show All Filename Extensions Setting is Enabled (Automated)	□	□

Appendix: CIS Controls v7 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1	Ensure All Apple-provided Software Is Current	□	□
1.2	Ensure Auto Update Is Enabled	□	□
1.3	Ensure Download New Updates When Available Is Enabled	□	□
1.4	Ensure Install of macOS Updates Is Enabled	□	□
1.5	Ensure Install Application Updates from the App Store Is Enabled	□	□
1.6	Ensure Install Security Responses and System Files Is Enabled	□	□
2.1.1	Ensure Firewall Is Enabled	□	□
2.2.2.1	Ensure Remote Apple Events Is Disabled	□	□
2.3.1	Ensure Sending Diagnostic and Usage Data to Apple Is Disabled	□	□
2.3.3	Ensure Gatekeeper Is Enabled	□	□
2.4.1	Ensure an Inactivity Interval of 20 Minutes Or Less for the Screen Saver Is Enabled	□	□
2.4.2	Ensure Require Password After Screen Saver Begins or Display Is Turned Off Is Enabled for 5 Seconds or Immediately	□	□
2.4.3	Ensure a Custom Message for the Login Screen Is Enabled	□	□
2.4.4	Ensure Login Window Displays as Name and Password Is Enabled	□	□
2.4.5	Ensure Show Password Hints Is Disabled	□	□
2.6.2	Ensure Guest Access to Shared Folders Is Disabled	□	□
2.6.3	Ensure Automatic Login Is Disabled	□	□
3.1	Ensure Security Auditing Is Enabled	□	□
3.2	Ensure Security Auditing Flags For User-Attributable Events Are Configured Per Local Organizational Requirements	□	□

Recommendation		Set Correctly	
		Yes	No
3.5	Ensure Access to Audit Records Is Controlled	□	□
3.6	Ensure Firewall Logging Is Enabled and Configured	□	□
4.1	Ensure Bonjour Advertising Services Is Disabled	□	□
4.2	Ensure HTTP Server Is Disabled	□	□
4.3	Ensure NFS Server Is Disabled	□	□
5.1.1	Ensure Home Folders Are Secure	□	□
5.1.2	Ensure Apple Mobile File Integrity (AMFI) Is Enabled	□	□
5.1.3	Ensure Signed System Volume (SSV) Is Enabled	□	□
5.1.4	Ensure Appropriate Permissions Are Enabled for System Wide Applications	□	□
5.1.5	Ensure No World Writable Folders Exist in the System Folder	□	□
5.1.6	Ensure No World Writable Folders Exist in the Library Folder	□	□
5.2.7	Ensure Password Age Is Configured	□	□
5.3	Ensure the Sudo Timeout Period Is Set to Zero	□	□
5.4	Ensure a Separate Timestamp Is Enabled for Each User/tty Combo	□	□
5.5	Ensure the "root" Account Is Disabled	□	□
5.6	Ensure an Administrator Account Cannot Login to Another User's Active and Locked Session	□	□
5.7	Ensure a Login Window Banner Exists	□	□
5.8	Ensure the Guest Home Folder Does Not Exist	□	□
5.9	Ensure XProtect Is Running and Updated	□	□
5.10	Ensure Secure Keyboard Entry Terminal.app Is Enabled	□	□
5.11	Ensure Show All Filename Extensions Setting is Enabled	□	□

Appendix: CIS Controls v7 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1	Ensure All Apple-provided Software Is Current	□	□
1.2	Ensure Auto Update Is Enabled	□	□
1.3	Ensure Download New Updates When Available Is Enabled	□	□
1.4	Ensure Install of macOS Updates Is Enabled	□	□
1.5	Ensure Install Application Updates from the App Store Is Enabled	□	□
1.6	Ensure Install Security Responses and System Files Is Enabled	□	□
2.1.1	Ensure Firewall Is Enabled	□	□
2.2.1.1	Ensure Set Time and Date Automatically Is Enabled	□	□
2.2.1.2	Ensure the Time Service Is Enabled	□	□
2.2.2.1	Ensure Remote Apple Events Is Disabled	□	□
2.2.2.2	Ensure Content Caching Is Disabled	□	□
2.3.1	Ensure Sending Diagnostic and Usage Data to Apple Is Disabled	□	□
2.3.2	Ensure Limit Ad Tracking Is Enabled	□	□
2.3.3	Ensure Gatekeeper Is Enabled	□	□
2.4.1	Ensure an Inactivity Interval of 20 Minutes Or Less for the Screen Saver Is Enabled	□	□
2.4.2	Ensure Require Password After Screen Saver Begins or Display Is Turned Off Is Enabled for 5 Seconds or Immediately	□	□
2.4.3	Ensure a Custom Message for the Login Screen Is Enabled	□	□
2.4.4	Ensure Login Window Displays as Name and Password Is Enabled	□	□
2.4.5	Ensure Show Password Hints Is Disabled	□	□
2.5.1	Ensure Users' Accounts Do Not Have a Password Hint	□	□

Recommendation		Set Correctly	
		Yes	No
2.6.1	Ensure Guest Account Is Disabled	□	□
2.6.2	Ensure Guest Access to Shared Folders Is Disabled	□	□
2.6.3	Ensure Automatic Login Is Disabled	□	□
3.1	Ensure Security Auditing Is Enabled	□	□
3.2	Ensure Security Auditing Flags For User-Attributable Events Are Configured Per Local Organizational Requirements	□	□
3.3	Ensure install.log Is Retained for 365 or More Days and No Maximum Size	□	□
3.4	Ensure Security Auditing Retention Is Enabled	□	□
3.5	Ensure Access to Audit Records Is Controlled	□	□
3.6	Ensure Firewall Logging Is Enabled and Configured	□	□
4.1	Ensure Bonjour Advertising Services Is Disabled	□	□
4.2	Ensure HTTP Server Is Disabled	□	□
4.3	Ensure NFS Server Is Disabled	□	□
5.1.1	Ensure Home Folders Are Secure	□	□
5.1.2	Ensure Apple Mobile File Integrity (AMFI) Is Enabled	□	□
5.1.3	Ensure Signed System Volume (SSV) Is Enabled	□	□
5.1.4	Ensure Appropriate Permissions Are Enabled for System Wide Applications	□	□
5.1.5	Ensure No World Writable Folders Exist in the System Folder	□	□
5.1.6	Ensure No World Writable Folders Exist in the Library Folder	□	□
5.2.1	Ensure Password Account Lockout Threshold Is Configured	□	□
5.2.2	Ensure Password Minimum Length Is Configured	□	□
5.2.3	Ensure Complex Password Must Contain Alphabetic Characters Is Configured	□	□
5.2.4	Ensure Complex Password Must Contain Numeric Character Is Configured	□	□
5.2.5	Ensure Complex Password Must Contain Special Character Is Configured	□	□

Recommendation		Set Correctly	
		Yes	No
5.2.6	Ensure Complex Password Must Contain Uppercase and Lowercase Characters Is Configured	□	□
5.2.7	Ensure Password Age Is Configured	□	□
5.2.8	Ensure Password History Is Configured	□	□
5.3	Ensure the Sudo Timeout Period Is Set to Zero	□	□
5.4	Ensure a Separate Timestamp Is Enabled for Each User/tty Combo	□	□
5.5	Ensure the "root" Account Is Disabled	□	□
5.6	Ensure an Administrator Account Cannot Login to Another User's Active and Locked Session	□	□
5.7	Ensure a Login Window Banner Exists	□	□
5.8	Ensure the Guest Home Folder Does Not Exist	□	□
5.9	Ensure XProtect Is Running and Updated	□	□
5.10	Ensure Secure Keyboard Entry Terminal.app Is Enabled	□	□
5.11	Ensure Show All Filename Extensions Setting is Enabled	□	□

Appendix: CIS Controls v7 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1	Ensure All Apple-provided Software Is Current	□	□
1.2	Ensure Auto Update Is Enabled	□	□
1.3	Ensure Download New Updates When Available Is Enabled	□	□
1.4	Ensure Install of macOS Updates Is Enabled	□	□
1.5	Ensure Install Application Updates from the App Store Is Enabled	□	□
1.6	Ensure Install Security Responses and System Files Is Enabled	□	□
2.1.1	Ensure Firewall Is Enabled	□	□
2.2.1.1	Ensure Set Time and Date Automatically Is Enabled	□	□
2.2.1.2	Ensure the Time Service Is Enabled	□	□
2.2.2.1	Ensure Remote Apple Events Is Disabled	□	□
2.2.2.2	Ensure Content Caching Is Disabled	□	□
2.3.1	Ensure Sending Diagnostic and Usage Data to Apple Is Disabled	□	□
2.3.2	Ensure Limit Ad Tracking Is Enabled	□	□
2.3.3	Ensure Gatekeeper Is Enabled	□	□
2.4.1	Ensure an Inactivity Interval of 20 Minutes Or Less for the Screen Saver Is Enabled	□	□
2.4.2	Ensure Require Password After Screen Saver Begins or Display Is Turned Off Is Enabled for 5 Seconds or Immediately	□	□
2.4.3	Ensure a Custom Message for the Login Screen Is Enabled	□	□
2.4.4	Ensure Login Window Displays as Name and Password Is Enabled	□	□
2.4.5	Ensure Show Password Hints Is Disabled	□	□
2.5.1	Ensure Users' Accounts Do Not Have a Password Hint	□	□

Recommendation		Set Correctly	
		Yes	No
2.6.1	Ensure Guest Account Is Disabled	□	□
2.6.2	Ensure Guest Access to Shared Folders Is Disabled	□	□
2.6.3	Ensure Automatic Login Is Disabled	□	□
3.1	Ensure Security Auditing Is Enabled	□	□
3.2	Ensure Security Auditing Flags For User-Attributable Events Are Configured Per Local Organizational Requirements	□	□
3.3	Ensure install.log Is Retained for 365 or More Days and No Maximum Size	□	□
3.4	Ensure Security Auditing Retention Is Enabled	□	□
3.5	Ensure Access to Audit Records Is Controlled	□	□
3.6	Ensure Firewall Logging Is Enabled and Configured	□	□
4.1	Ensure Bonjour Advertising Services Is Disabled	□	□
4.2	Ensure HTTP Server Is Disabled	□	□
4.3	Ensure NFS Server Is Disabled	□	□
5.1.1	Ensure Home Folders Are Secure	□	□
5.1.2	Ensure Apple Mobile File Integrity (AMFI) Is Enabled	□	□
5.1.3	Ensure Signed System Volume (SSV) Is Enabled	□	□
5.1.4	Ensure Appropriate Permissions Are Enabled for System Wide Applications	□	□
5.1.5	Ensure No World Writable Folders Exist in the System Folder	□	□
5.1.6	Ensure No World Writable Folders Exist in the Library Folder	□	□
5.2.1	Ensure Password Account Lockout Threshold Is Configured	□	□
5.2.2	Ensure Password Minimum Length Is Configured	□	□
5.2.3	Ensure Complex Password Must Contain Alphabetic Characters Is Configured	□	□
5.2.4	Ensure Complex Password Must Contain Numeric Character Is Configured	□	□
5.2.5	Ensure Complex Password Must Contain Special Character Is Configured	□	□

Recommendation		Set Correctly	
		Yes	No
5.2.6	Ensure Complex Password Must Contain Uppercase and Lowercase Characters Is Configured	□	□
5.2.7	Ensure Password Age Is Configured	□	□
5.2.8	Ensure Password History Is Configured	□	□
5.3	Ensure the Sudo Timeout Period Is Set to Zero	□	□
5.4	Ensure a Separate Timestamp Is Enabled for Each User/tty Combo	□	□
5.5	Ensure the "root" Account Is Disabled	□	□
5.6	Ensure an Administrator Account Cannot Login to Another User's Active and Locked Session	□	□
5.7	Ensure a Login Window Banner Exists	□	□
5.8	Ensure the Guest Home Folder Does Not Exist	□	□
5.9	Ensure XProtect Is Running and Updated	□	□
5.10	Ensure Secure Keyboard Entry Terminal.app Is Enabled	□	□
5.11	Ensure Show All Filename Extensions Setting is Enabled	□	□

Appendix: CIS Controls v7 Unmapped Recommendations

Recommendation		Set Correctly	
		Yes	No
	No unmapped recommendations to CIS Controls v7	□	□

Appendix: CIS Controls v8 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1	Ensure All Apple-provided Software Is Current	□	□
1.2	Ensure Auto Update Is Enabled	□	□
1.3	Ensure Download New Updates When Available Is Enabled	□	□
1.4	Ensure Install of macOS Updates Is Enabled	□	□
1.5	Ensure Install Application Updates from the App Store Is Enabled	□	□
1.6	Ensure Install Security Responses and System Files Is Enabled	□	□
2.1.1	Ensure Firewall Is Enabled	□	□
2.2.2.1	Ensure Remote Apple Events Is Disabled	□	□
2.3.1	Ensure Sending Diagnostic and Usage Data to Apple Is Disabled	□	□
2.3.3	Ensure Gatekeeper Is Enabled	□	□
2.4.1	Ensure an Inactivity Interval of 20 Minutes Or Less for the Screen Saver Is Enabled	□	□
2.4.2	Ensure Require Password After Screen Saver Begins or Display Is Turned Off Is Enabled for 5 Seconds or Immediately	□	□
2.4.3	Ensure a Custom Message for the Login Screen Is Enabled	□	□
2.4.4	Ensure Login Window Displays as Name and Password Is Enabled	□	□
2.4.5	Ensure Show Password Hints Is Disabled	□	□
2.5.1	Ensure Users' Accounts Do Not Have a Password Hint	□	□
2.6.1	Ensure Guest Account Is Disabled	□	□
2.6.2	Ensure Guest Access to Shared Folders Is Disabled	□	□
2.6.3	Ensure Automatic Login Is Disabled	□	□
3.1	Ensure Security Auditing Is Enabled	□	□

Recommendation		Set Correctly	
		Yes	No
3.2	Ensure Security Auditing Flags For User-Attributable Events Are Configured Per Local Organizational Requirements	□	□
3.3	Ensure install.log Is Retained for 365 or More Days and No Maximum Size	□	□
3.4	Ensure Security Auditing Retention Is Enabled	□	□
3.5	Ensure Access to Audit Records Is Controlled	□	□
3.6	Ensure Firewall Logging Is Enabled and Configured	□	□
4.1	Ensure Bonjour Advertising Services Is Disabled	□	□
4.2	Ensure HTTP Server Is Disabled	□	□
4.3	Ensure NFS Server Is Disabled	□	□
5.1.1	Ensure Home Folders Are Secure	□	□
5.1.2	Ensure Apple Mobile File Integrity (AMFI) Is Enabled	□	□
5.1.3	Ensure Signed System Volume (SSV) Is Enabled	□	□
5.1.4	Ensure Appropriate Permissions Are Enabled for System Wide Applications	□	□
5.1.5	Ensure No World Writable Folders Exist in the System Folder	□	□
5.1.6	Ensure No World Writable Folders Exist in the Library Folder	□	□
5.2.1	Ensure Password Account Lockout Threshold Is Configured	□	□
5.2.2	Ensure Password Minimum Length Is Configured	□	□
5.2.3	Ensure Complex Password Must Contain Alphabetic Characters Is Configured	□	□
5.2.4	Ensure Complex Password Must Contain Numeric Character Is Configured	□	□
5.2.5	Ensure Complex Password Must Contain Special Character Is Configured	□	□
5.2.6	Ensure Complex Password Must Contain Uppercase and Lowercase Characters Is Configured	□	□
5.2.7	Ensure Password Age Is Configured	□	□
5.2.8	Ensure Password History Is Configured	□	□
5.3	Ensure the Sudo Timeout Period Is Set to Zero	□	□

Recommendation		Set Correctly	
		Yes	No
5.4	Ensure a Separate Timestamp Is Enabled for Each User/tty Combo	□	□
5.5	Ensure the "root" Account Is Disabled	□	□
5.6	Ensure an Administrator Account Cannot Login to Another User's Active and Locked Session	□	□
5.7	Ensure a Login Window Banner Exists	□	□
5.8	Ensure the Guest Home Folder Does Not Exist	□	□
5.9	Ensure XProtect Is Running and Updated	□	□
5.11	Ensure Show All Filename Extensions Setting is Enabled	□	□

Appendix: CIS Controls v8 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1	Ensure All Apple-provided Software Is Current	□	□
1.2	Ensure Auto Update Is Enabled	□	□
1.3	Ensure Download New Updates When Available Is Enabled	□	□
1.4	Ensure Install of macOS Updates Is Enabled	□	□
1.5	Ensure Install Application Updates from the App Store Is Enabled	□	□
1.6	Ensure Install Security Responses and System Files Is Enabled	□	□
2.1.1	Ensure Firewall Is Enabled	□	□
2.2.1.1	Ensure Set Time and Date Automatically Is Enabled	□	□
2.2.1.2	Ensure the Time Service Is Enabled	□	□
2.2.2.1	Ensure Remote Apple Events Is Disabled	□	□
2.2.2.2	Ensure Content Caching Is Disabled	□	□
2.3.1	Ensure Sending Diagnostic and Usage Data to Apple Is Disabled	□	□
2.3.2	Ensure Limit Ad Tracking Is Enabled	□	□
2.3.3	Ensure Gatekeeper Is Enabled	□	□
2.4.1	Ensure an Inactivity Interval of 20 Minutes Or Less for the Screen Saver Is Enabled	□	□
2.4.2	Ensure Require Password After Screen Saver Begins or Display Is Turned Off Is Enabled for 5 Seconds or Immediately	□	□
2.4.3	Ensure a Custom Message for the Login Screen Is Enabled	□	□
2.4.4	Ensure Login Window Displays as Name and Password Is Enabled	□	□
2.4.5	Ensure Show Password Hints Is Disabled	□	□
2.5.1	Ensure Users' Accounts Do Not Have a Password Hint	□	□

Recommendation		Set Correctly	
		Yes	No
2.6.1	Ensure Guest Account Is Disabled	□	□
2.6.2	Ensure Guest Access to Shared Folders Is Disabled	□	□
2.6.3	Ensure Automatic Login Is Disabled	□	□
3.1	Ensure Security Auditing Is Enabled	□	□
3.2	Ensure Security Auditing Flags For User-Attributable Events Are Configured Per Local Organizational Requirements	□	□
3.3	Ensure install.log Is Retained for 365 or More Days and No Maximum Size	□	□
3.4	Ensure Security Auditing Retention Is Enabled	□	□
3.5	Ensure Access to Audit Records Is Controlled	□	□
3.6	Ensure Firewall Logging Is Enabled and Configured	□	□
4.1	Ensure Bonjour Advertising Services Is Disabled	□	□
4.2	Ensure HTTP Server Is Disabled	□	□
4.3	Ensure NFS Server Is Disabled	□	□
5.1.1	Ensure Home Folders Are Secure	□	□
5.1.2	Ensure Apple Mobile File Integrity (AMFI) Is Enabled	□	□
5.1.3	Ensure Signed System Volume (SSV) Is Enabled	□	□
5.1.4	Ensure Appropriate Permissions Are Enabled for System Wide Applications	□	□
5.1.5	Ensure No World Writable Folders Exist in the System Folder	□	□
5.1.6	Ensure No World Writable Folders Exist in the Library Folder	□	□
5.2.1	Ensure Password Account Lockout Threshold Is Configured	□	□
5.2.2	Ensure Password Minimum Length Is Configured	□	□
5.2.3	Ensure Complex Password Must Contain Alphabetic Characters Is Configured	□	□
5.2.4	Ensure Complex Password Must Contain Numeric Character Is Configured	□	□
5.2.5	Ensure Complex Password Must Contain Special Character Is Configured	□	□

Recommendation		Set Correctly	
		Yes	No
5.2.6	Ensure Complex Password Must Contain Uppercase and Lowercase Characters Is Configured	□	□
5.2.7	Ensure Password Age Is Configured	□	□
5.2.8	Ensure Password History Is Configured	□	□
5.3	Ensure the Sudo Timeout Period Is Set to Zero	□	□
5.4	Ensure a Separate Timestamp Is Enabled for Each User/tty Combo	□	□
5.5	Ensure the "root" Account Is Disabled	□	□
5.6	Ensure an Administrator Account Cannot Login to Another User's Active and Locked Session	□	□
5.7	Ensure a Login Window Banner Exists	□	□
5.8	Ensure the Guest Home Folder Does Not Exist	□	□
5.9	Ensure XProtect Is Running and Updated	□	□
5.10	Ensure Secure Keyboard Entry Terminal.app Is Enabled	□	□
5.11	Ensure Show All Filename Extensions Setting is Enabled	□	□

Appendix: CIS Controls v8 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1	Ensure All Apple-provided Software Is Current	□	□
1.2	Ensure Auto Update Is Enabled	□	□
1.3	Ensure Download New Updates When Available Is Enabled	□	□
1.4	Ensure Install of macOS Updates Is Enabled	□	□
1.5	Ensure Install Application Updates from the App Store Is Enabled	□	□
1.6	Ensure Install Security Responses and System Files Is Enabled	□	□
2.1.1	Ensure Firewall Is Enabled	□	□
2.2.1.1	Ensure Set Time and Date Automatically Is Enabled	□	□
2.2.1.2	Ensure the Time Service Is Enabled	□	□
2.2.2.1	Ensure Remote Apple Events Is Disabled	□	□
2.2.2.2	Ensure Content Caching Is Disabled	□	□
2.3.1	Ensure Sending Diagnostic and Usage Data to Apple Is Disabled	□	□
2.3.2	Ensure Limit Ad Tracking Is Enabled	□	□
2.3.3	Ensure Gatekeeper Is Enabled	□	□
2.4.1	Ensure an Inactivity Interval of 20 Minutes Or Less for the Screen Saver Is Enabled	□	□
2.4.2	Ensure Require Password After Screen Saver Begins or Display Is Turned Off Is Enabled for 5 Seconds or Immediately	□	□
2.4.3	Ensure a Custom Message for the Login Screen Is Enabled	□	□
2.4.4	Ensure Login Window Displays as Name and Password Is Enabled	□	□
2.4.5	Ensure Show Password Hints Is Disabled	□	□
2.5.1	Ensure Users' Accounts Do Not Have a Password Hint	□	□

Recommendation		Set Correctly	
		Yes	No
2.6.1	Ensure Guest Account Is Disabled	□	□
2.6.2	Ensure Guest Access to Shared Folders Is Disabled	□	□
2.6.3	Ensure Automatic Login Is Disabled	□	□
3.1	Ensure Security Auditing Is Enabled	□	□
3.2	Ensure Security Auditing Flags For User-Attributable Events Are Configured Per Local Organizational Requirements	□	□
3.3	Ensure install.log Is Retained for 365 or More Days and No Maximum Size	□	□
3.4	Ensure Security Auditing Retention Is Enabled	□	□
3.5	Ensure Access to Audit Records Is Controlled	□	□
3.6	Ensure Firewall Logging Is Enabled and Configured	□	□
4.1	Ensure Bonjour Advertising Services Is Disabled	□	□
4.2	Ensure HTTP Server Is Disabled	□	□
4.3	Ensure NFS Server Is Disabled	□	□
5.1.1	Ensure Home Folders Are Secure	□	□
5.1.2	Ensure Apple Mobile File Integrity (AMFI) Is Enabled	□	□
5.1.3	Ensure Signed System Volume (SSV) Is Enabled	□	□
5.1.4	Ensure Appropriate Permissions Are Enabled for System Wide Applications	□	□
5.1.5	Ensure No World Writable Folders Exist in the System Folder	□	□
5.1.6	Ensure No World Writable Folders Exist in the Library Folder	□	□
5.2.1	Ensure Password Account Lockout Threshold Is Configured	□	□
5.2.2	Ensure Password Minimum Length Is Configured	□	□
5.2.3	Ensure Complex Password Must Contain Alphabetic Characters Is Configured	□	□
5.2.4	Ensure Complex Password Must Contain Numeric Character Is Configured	□	□
5.2.5	Ensure Complex Password Must Contain Special Character Is Configured	□	□

Recommendation		Set Correctly	
		Yes	No
5.2.6	Ensure Complex Password Must Contain Uppercase and Lowercase Characters Is Configured	□	□
5.2.7	Ensure Password Age Is Configured	□	□
5.2.8	Ensure Password History Is Configured	□	□
5.3	Ensure the Sudo Timeout Period Is Set to Zero	□	□
5.4	Ensure a Separate Timestamp Is Enabled for Each User/tty Combo	□	□
5.5	Ensure the "root" Account Is Disabled	□	□
5.6	Ensure an Administrator Account Cannot Login to Another User's Active and Locked Session	□	□
5.7	Ensure a Login Window Banner Exists	□	□
5.8	Ensure the Guest Home Folder Does Not Exist	□	□
5.9	Ensure XProtect Is Running and Updated	□	□
5.10	Ensure Secure Keyboard Entry Terminal.app Is Enabled	□	□
5.11	Ensure Show All Filename Extensions Setting is Enabled	□	□

Appendix: CIS Controls v8 Unmapped Recommendations

Recommendation		Set Correctly	
		Yes	No
	No unmapped recommendations to CIS Controls v8	□	□

Appendix: Change History

Date	Version	Changes for this version
May 3, 2024	1.0.0	Initial Draft Release
May 29, 2024	1.0.0	Initial Release
October 14, 2024	1.1.0	Initial Draft Release
October 30, 2024	1.1.0	Add a recommendation that verifies that the time service is running (Ticket 22789)
October 30, 2024	1.1.0	Move 5.1.3 to 5.1.2, 5.1.4 to 5.1.3, 5.1.5 to 5.1.4, 5.1.6 to 5.1.4 with the removal of the SIPs recommendation (5.1.2) (Ticket 22794)
October 30, 2024	1.1.0	Update the remediation to verify where audit logs are being stored (Ticket 22945)
October 30, 2024	1.1.0	Password lockout timer has been removed due it being deprecated and removed. Lockout value is not affected. (Ticket 22795)
October 30, 2024	1.1.0	Remove SIPs recommendation in cloud macOS (Ticket 22793)
October 30, 2024	1.1.0	Update description to include information about auditd being deprecated (Ticket 22792)
October 30, 2024	1.1.0	Screen Sharing needs to be removed from the cloud version of macOS and shift 2.2.2.2 to 2.2.2.1 and 2.2.2.3 to 2.2.2.2 (Ticket 22790)

Date	Version	Changes for this version
October 30, 2024	1.1.0	Time within appropriate limits has been removed across all macOS benchmarks. (Ticket 22788)
October 30, 2024	1.1.0	Initial Version Release