DRAFT NIST Special Publication 800-179
Revision 1

Guide to Securing macOS 10.12 Systems for IT Professionals

A NIST Security Configuration Checklist

Lee Badger
Murugiah Souppaya
Mark Trapnell
Eric Trapnell
Dylan Yaga
Karen Scarfone

C O M P U T E R S E C U R I T Y

National Institute of Standards and Technology
U.S. Department of Commerce

DRAFT NIST Special Publication 800-179 Revision 1

Guide to Securing macOS 10.12 Systems for IT Professionals

A NIST Security Configuration Checklist

Lee Badger
Murugiah Souppaya
Mark Trapnell
Eric Trapnell
Dylan Yaga
Computer Security Division
Information Technology Laboratory

Karen Scarfone
Scarfone Cybersecurity
Clifton, VA

October 2018

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

Authority

This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 et seq., Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

National Institute of Standards and Technology Special Publication 800-179 Revision 1
Natl. Inst. Stand. Technol. Spec. Publ. 800-179 Rev. 1, 130 pages (October 2018)
CODEN: NSPUE2

Public comment period: *October 19, 2018* through *November 16, 2018*

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Email: 800-179comments@nist.gov

All comments are subject to release under the Freedom of Information Act (FOIA).

92 ## Reports on Computer Systems Technology

93 The Information Technology Laboratory (ITL) at the National Institute of Standards and
94 Technology (NIST) promotes the U.S. economy and public welfare by providing technical
95 leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test
96 methods, reference data, proof of concept implementations, and technical analyses to advance
97 the development and productive use of information technology. ITL's responsibilities include the
98 development of management, administrative, technical, and physical standards and guidelines for
99 the cost-effective security and privacy of other than national security-related information in
100 federal information systems. The Special Publication 800-series reports on ITL's research,
101 guidelines, and outreach efforts in information system security, and its collaborative activities
102 with industry, government, and academic organizations.

103

104 ## Abstract

105 This publication assists IT professionals in securing Apple macOS 10.12 desktop and laptop
106 systems within various environments. It provides detailed information about the security features
107 of macOS 10.12 and security configuration guidelines. The publication recommends and
108 explains tested, secure settings with the objective of simplifying the administrative burden of
109 improving the security of macOS 10.12 systems in three types of environments: Standalone,
110 Managed, and Specialized Security-Limited Functionality.

111

112 ## Keywords

113 Apple OS X; checklist; endpoint device security; hardening guide; host security; macOS; mobile
114 device security; operating system security; secure configuration.

Supplemental Content

For additional documents that support this publication, see:
https://github.com/usnistgov/applesec.

Trademark Information

Table of Contents

List of Figures

List of Tables

Executive Summary

When an IT security configuration checklist (e.g., hardening or lockdown guide) is applied to a system in combination with trained system administrators and a sound and effective security program (which includes a robust patch management program), a substantial reduction in vulnerability exposure can be achieved. Accordingly, the National Institute of Standards and Technology (NIST) has produced the *Guide to Securing Apple macOS 10.12 Systems for IT Professionals: A NIST Security Configuration Checklist* to assist personnel responsible for the administration and security of macOS 10.12[1] systems. This guide contains information that can be used by system administrators to secure local macOS 10.12 desktops and laptops more effectively in a variety of environments, including Standalone and Managed environments. The guidance should only be applied throughout an enterprise by trained and experienced system administrators.

The guidance presented in this document is applicable only to macOS 10.12 systems. The recommendations in this guide should not be applied to systems running anything other than macOS 10.12.

This guide provides detailed information about the security of macOS 10.12 and security configuration guidelines for the macOS 10.12 operating system. The guide documents the methods that system administrators can use to implement each security setting recommended. The principal goal of the document is to recommend and explain tested, secure settings for macOS 10.12 systems with the objective of simplifying the administrative burden of improving the security of macOS 10.12 systems in three types of environments: Standalone, Managed, and one custom environment labeled Specialized Security-Limited Functionality (SSLF).[2]

- **Standalone.** Standalone, sometimes called Small Office/Home Office (SOHO), describes small, informal computer installations that are used for home or business purposes. Standalone encompasses a variety of small-scale environments and devices, ranging from laptops, mobile devices, and home computers, to telework systems located on broadband networks, to small businesses and small branch offices of a company. Historically, Standalone environments are the least secured and most trusting. Generally, the individuals performing Standalone system administration are not knowledgeable about security. This can result in environments that are less secure than they need to be because the focus is generally on functionality and ease-of-use.

- **Managed.** Managed environments, sometimes referred to as Enterprise environments, have systems that share a common hardware and software configuration, are centrally deployed and managed, and are protected from threats on the Internet by using firewalls and other network security devices. Managed environments generally have staff dedicated to supporting users and providing security. The combination of this structure and a skilled staff allows better security practices to be implemented during initial system deployment and in ongoing support and maintenance, and for a consistent security

[1] Starting with version 10.12, Apple now refers to OS X as macOS.
[2] SSLF is defined in NIST SP 800-70 Revision 4, *National Checklist Program for IT Products – Guidelines for Checklist Users and Developers* [SP800-70r4].

posture to be maintained across the enterprise. Generally, Managed environments are more restrictive than Standalone environments.

- **Specialized Security-Limited Functionality (SSLF).** An SSLF environment is a likely target for attack or data exposure, and therefore security takes precedence over usability. This environment encompasses computers that are usually limited in their functionality to specific specialized purposes. They may contain highly confidential information (e.g., personnel records, medical records, financial information) or perform vital organizational functions (e.g., accounting, payroll processing). Typically, providing sufficiently strong protection for these systems involves a tradeoff between security and functionality based on the premise that any more functionality than is strictly necessary provides more opportunity for exploitation. This environment is characterized by a significant reduction in system functionality and a higher risk of applications breaking, resulting in an increased support cost. An SSLF environment could be a subset of another environment. While some Standalone users understandably might want to choose this environment due to concern for being as secure as possible, this environment is usually not advised for most Standalone users administering their own systems because of significant tradeoffs and administrative complexity. In most cases, the SSLF environment is not suitable for widespread enterprise usage.

By implementing the recommendations described throughout this publication, organizations should be able to meet the baseline requirements for macOS 10.12 systems. This is based upon the management, operational, and technical security controls described in NIST Special Publication (SP) 800-53 Revision 4, *Recommended Security Controls for Federal Information Systems and Organizations* [SP 800-53r4].

Although the guidance presented in this document has undergone considerable testing, every system and environment is unique, so system administrators should perform their own testing. The development of the NIST security baselines[3] was driven by the need to create more secure macOS 10.12 system configurations. These NIST security baselines provide guidance on how to define specific configurations with varying levels of security and make certain tradeoffs that depend on the target environment. Because some settings in the baselines may reduce the functionality or usability of the system, caution should be used when applying the security baselines. Specific settings in the baselines should be modified as needed (with due consideration of the security implications, including the possible need for compensating controls) so that the settings conform to local policies and support the required system functionality. NIST recommends that organizations fully test the baselines on representative systems before widespread deployment. Some settings may inadvertently interfere with applications, particularly legacy applications that may require a less restrictive security profile.

The security configuration guidance provided in this document was tested on clean macOS 10.12 installations. NIST recommends that system administrators build their systems from a clean formatted state to begin the process of securing macOS 10.12 systems. NIST recommends that the installation process be performed on a secure network segment or off the organization's

[3] Refer to Appendix D, Appendix I, and Appendix J for more information on the baselines and how to implement them.

network until the security configuration is completed, all patches are applied, and strong passwords are set for all accounts.

After the macOS 10.12 operating system has been installed and securely configured, it should be regularly monitored and patched when necessary to mitigate software vulnerabilities. Once Apple releases an update, it should be tested thoroughly and applied to all systems within an organization as soon as possible. Updates to third-party applications should receive similar treatment.

This guidance document includes recommendations for configuring selected applications built into macOS 10.12, such as web browsers and email clients. This list is not intended to be a complete list of applications for macOS 10.12, nor does it imply NIST's endorsement of particular products. Many of the configuration recommendations for the applications focus on preventing damage from malware, either to the applications themselves or to the macOS 10.12 system, while the applications are being used.

This document provides recommendations to assist organizations in making their macOS 10.12 systems more secure than out-of-the-box installations. The recommendations provide system administrators with the information necessary to modify the settings and to comply with local policy or special situations. The baseline recommendations and settings provide a high level of security for macOS 10.12 systems when used in conjunction with a sound and comprehensive local security policy and other relevant security controls. The guidelines are appropriate for organizational environments that are configuring and deploying laptops for mobile users and desktop computers for teleworkers.

Changes in SP 800-179 Revision 1

This document builds on the work and recommendations presented in SP 800-179. The guidance originally offered for OS X 10.10 has been updated to be compatible with macOS 10.12 systems. Settings no longer configurable or applicable have been removed from the guide. Likewise, additional guidance is offered for the new functionality present in version 10.12. Some settings have had their recommended values changed to better align with the usability and security requirements of the different usage profiles.

This guide no longer discusses settings that are considered secure by default. However, they are still listed in the companion spreadsheet.

Major Changes to This Configuration Guide Since Version 10.10

- System Integrity Protection (SIP) is the biggest new security feature introduced since 10.10. It prevents modification of Apple-specified system files. It is discussed further in Section 3.1.

- Siri, added in 10.12, is Apple's personal assistant technology. It allows for voice control of the system. More information on Siri and the security concerns it raises can be found in Section 6.8.5.4.

- Spotlight is now enhanced with Internet search functionality. Although a convenience feature, all search queries are now sent to Apple and select third parties by default. See Section 6.2.6 for further information on Spotlight.

- The system process `launchctl` is responsible for starting and stopping system services. It can be used to disable unused features such as file sharing, thus reducing the attack surface of the system. The majority of `launchctl` related guidance is located in Appendix J.16.

- An account lockout password policy item is now configured. It controls how many failed login attempts are permitted before a user account is locked for a predetermined length of time. It can be found with other password policies in Section 6.3.4.

- The secure erase feature has been removed from both the Graphical User Interface (GUI) and command line environments. Secure erase is not necessarily effective when used for newer systems with Solid State Drive (SSD) devices. As a compensating control, a crypto erase (affecting an entire device) can be performed if Filevault is enabled on the system.

1. Introduction

1.1 Purpose and Scope

This publication is designed to assist IT professionals in securing Apple macOS 10.12 desktop and laptop systems. Only trained and competent system administrators should apply these guidelines. Configuration of other versions of macOS, as well as macOS Server, is outside the scope of this publication. Other versions of macOS are only mentioned for informative purposes.

The guide provides detailed information about the security features of macOS 10.12 and security configuration guidelines for the macOS 10.12 operating system (OS). The guide documents the methods that IT professionals can use to implement each security setting recommended. The principal goal of the document is to recommend and explain tested, secure settings for macOS 10.12 desktops and laptops with the objective of simplifying the administrative burden of improving their security in three types of environments: Standalone, Managed, and Specialized Security-Limited Functionality (SSLF). The proposed controls are consistent with the minimum security controls for an IT system as represented in NIST Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems and Organizations* [SP 800-53r4].

1.2 Audience

This document has been created for IT professionals, particularly system administrators and information security personnel (security managers, engineers, administrators, etc.) who are responsible for securing or maintaining the security of macOS 10.12 systems. Auditors and others who need to assess the security of systems may also find this publication useful. The document assumes that the reader has experience installing and administering macOS-based systems [NISTIR 7298r2]. The document discusses various macOS 10.12 security settings in technical detail.

1.3 Document Structure

The remainder of this document is organized into the following sections and appendices:

- Section 2 provides insight into the threats and security controls that are relevant for various environments, such as a large enterprise or a home office, and describes the need to document, implement, and test controls, as well as monitor and maintain systems on an ongoing basis.
- Section 3 presents an overview of the security components offered by macOS 10.12.
- Section 4 provides guidelines for installing, backing up, and patching macOS 10.12 systems.
- Section 5 discusses security policy configuration and how security baselines can best be used.

- Section 6 provides an overview of the settings in the NIST security baselines and explains how the settings can provide better security for systems.
- Section 7 provides guidelines for IT professionals on how to use the guide effectively to secure macOS 10.12 systems.
- Appendix A discusses the components of the NIST security baselines.
- Appendix B maps the guide's security controls and baseline settings to the controls in NIST Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.
- Appendix C lists built-in tools used to create the security configuration for macOS 10.12 systems.
- Appendix D lists resources that may be useful macOS 10.12 security references.
- Appendix E lists acronyms and abbreviations used in this document.
- Appendix F gives a description of variables used in many Terminal commands in this document.
- Appendix G lists files that require manual editing.
- Appendix H lists processes that must be restarted to successfully apply settings.
- Appendix I lists file ownership and permissions recommendations.
- Appendix J describes all the Terminal commands needed for system configuration.
- Appendix K is a glossary of terms.
- Appendix L provides a list of NIST document references.

IT professionals should read the entire publication, including the appendices, before using the security baselines or implementing any of the other recommendations or suggestions in the guide. Readers with limited macOS 10.12 administration and security experience are cautioned not to apply the baselines or other recommendations to systems on their own. As described in Section 7, the effective use of this publication involves extensive planning and testing.

2. macOS Security Guide Development

In today's computing environment, the security of all computing resources, from network infrastructure devices to users' desktop and laptop computers, is essential. There are many threats to users' computers, ranging from remotely launched network service exploits to malware spread through emails, websites, and file downloads. Increasing the security of individual computers protects them from these threats and reduces the likelihood that a system will be compromised or that data will be disclosed to unauthorized parties. Effective and well-tested security configurations mean that less time and money are spent eradicating malware, restoring systems from backups, and reinstalling operating systems and applications. In addition, having stronger host security increases network security (e.g., home, business, government, the Internet); for example, most distributed denial of service attacks against networks use large numbers of compromised hosts.

The goal of this guide is to provide security configuration guidelines to the users and system administrators of macOS 10.12 systems. This advice can be adapted to any environment, from individual Standalone installations to large geographically diverse organizations. This guide draws on a large body of vendor knowledge, as well as government and security community experience gained over many years of securing computer systems.

This section of the guide is based largely on the steps proposed in NIST's FISMA (Federal Information Security Management/Modernization Act) Implementation Project for achieving more secure information systems.[4] Sections 2.1 and 2.2 address the need to categorize information and information systems. Each macOS 10.12 system can be classified as having one of three roles; each system can also be classified according to the potential impact caused by security breaches. Section 2.3 describes threats and provides examples of security controls that can mitigate these threats. Section 2.4 outlines the primary types of environments for information systems—Standalone, Managed, and Specialized Security-Limited Functionality—and ties each environment to typical threat categories and security controls. Section 2.5 briefly describes the security-related documentation that affects the configuration and usage of systems and applications. Section 2.6 provides a brief overview of the implementation of the security controls and the importance of performing functionality and security testing. Finally, Section 2.7 discusses the need to monitor the security controls and maintain the system.

2.1 macOS System Roles and Requirements

macOS security should consider the role that the system plays. In the past, macOS systems were divided into three roles: inward-facing, outward-facing, and mobile. An inward-facing macOS system is typically a user workstation on the interior of a network that is not directly accessible from the Internet. An outward-facing macOS system is one that is directly connected to the Internet. A system with a mobile role typically moves between a variety of environments and physical locations. Over time, the mobile role has become the predominant role for most macOS systems. Therefore, this publication assumes the mobile role.

[4] More information on the project is available at https://csrc.nist.gov/projects/risk-management.

Systems in the mobile role might use both traditional wired methods (e.g., Ethernet) and wireless methods (e.g., IEEE 802.11) for network connectivity. The mobility of the system makes it more difficult to manage centrally. It also exposes the system to a wider variety of threat environments; for example, in a single day the system might be in a home environment, an office environment, a wireless network hotspot, and a hotel room. An additional threat is the loss or theft of the system. This could lead to loss of productivity at a minimum, but could include the disclosure of confidential information or the possible opening of a backdoor into the organization if remote access is not properly secured.

Most macOS systems today are used for the same combination of tasks: accessing websites, reading email, performing instant messaging, using social networks, and conducting other tasks with both work-related and personal contexts. This range of activity, as well as the frequent lack of perimeter defenses, exposes macOS systems to a wider variety of threats than they were exposed to in the past.

2.2 Security Categorization of Information and Information Systems

The classic model for information security defines three objectives of security: maintaining confidentiality, integrity, and availability. *Confidentiality* refers to protecting information from being accessed by unauthorized parties. *Integrity* refers to ensuring the authenticity of information—that the information is not altered, and that the source of the information is genuine. *Availability* means that information is accessible by authorized users. Each objective addresses a different aspect of providing protection for information.

Determining how strongly a system needs to be protected is based largely on the type of information that the system processes and stores. For example, a system containing medical records probably needs much stronger protection than a computer only used for viewing publicly released documents. This is not to imply that the second system does not need protection; every system needs to be protected, but the level of protection may vary based on the value of the system and its data. To establish a standard for determining the security category of a system, NIST created Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems* [FIPS 199]. FIPS 199 establishes three security categories—low, moderate, and high—based on the potential impact of a security breach involving a particular system. The FIPS 199 definitions for each category are as follows:

> "The potential impact is **LOW** if the loss of confidentiality, integrity, or availability could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals. A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.

> The potential impact is **MODERATE** if the loss of confidentiality, integrity, or availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals. A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.
>
> The potential impact is **HIGH** if the loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals. A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries."

Each system should be protected based on the potential impact to the system of a loss of confidentiality, integrity, or availability. Protection measures (otherwise known as **security controls**) tend to fall into two categories. First, security weaknesses in the system need to be resolved. For example, if a system has a known vulnerability that attackers could exploit, the system should be patched so that the vulnerability is removed or mitigated. Second, the system should offer only the minimum required functionality to each authorized user. This principle is known as **least privilege**.[5] Limiting functionality and resolving security weaknesses have a common goal: give attackers as few opportunities as possible to breach a system.

Although each system should ideally be made as secure as possible, this is generally not feasible because the system needs to meet the functional requirements of the system's users. Another common problem with security controls is that they often make systems less convenient or more difficult to use. When usability is an issue, many users will attempt to circumvent security controls; for example, if passwords must be long and complex, users may write them down. Balancing security, functionality, and usability is often a challenge. This guide attempts to strike a proper balance and make recommendations that provide a reasonably secure solution while offering the functionality and usability that users require.

Another fundamental principle recommended by this guide is the use of multiple layers of security. For example, a host may be protected from external attack by several controls, including a network-based firewall, a host-based firewall, and OS patching. The motivation for having multiple layers is that if one layer fails or otherwise cannot counteract a certain threat,

---

[5] For more information on least privilege and other fundamental principles of computer security, see "The Protection of Information in Computer Systems" by Jerome Saltzer and Michael Schroeder, April 17, 1975 (http://web.mit.edu/Saltzer/www/publications/protection/).

other layers might prevent the threat from successfully breaching the system. A combination of network-based and host-based controls is generally most effective at providing consistent protection for systems. Note that in many situations, such as Standalone environments, there may not be any network-based controls present, thus creating a reliance on layers of host-based controls.

NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, proposes minimum baseline management, operational, and technical security controls for information systems. These controls are to be implemented based on the security categorizations proposed by FIPS 199, as described earlier in this section [SP 800-37r1][SP 800-39]. This guidance should assist agencies in meeting baseline requirements for macOS 10.12 systems deployed in their environments.

2.3 Threats to macOS Technologies

To secure a system, it is essential first to define the threats that need to be mitigated. This knowledge of threats is key to understanding the reasons that the various configuration options have been chosen in this guide. Most threats against data and resources are possible because of mistakes—either bugs in operating system and application software that create exploitable vulnerabilities, or errors made by users and administrators. Threats may involve intentional actors (e.g., an attacker who wants to access credit cards on a system) or unintentional actors (e.g., an administrator who forgets to disable the user accounts of a terminated employee). Threats can be local, such as a disgruntled employee, or remote, such as an attacker in another country. The following sections describe each major threat category, list possible controls, provide examples of threats, and summarize the potential impact of the threat. The list of threats is not exhaustive; it simply represents the major threat categories that were considered during the selection of the security controls as described in this guide. Organizations should conduct risk assessments to identify the specific threats against their systems and determine the effectiveness of existing security controls in counteracting those threats, then perform risk mitigation to decide what additional measures (if any) should be implemented [SP 800-30r1].

2.3.1 Local Threats

Local threats require either physical access to the system or logical access to the system (e.g., an authorized user account). Local threats are grouped into three categories: boot process, unauthorized local access, and privilege escalation.

2.3.1.1 Boot Process

Threat: An unauthorized individual boots a computer from third-party media (e.g., removable drives, Universal Serial Bus [USB] token storage devices). This could permit the attacker to circumvent operating system (OS) security measures and gain unauthorized access to information.

Examples:

- While traveling, an employee misplaces a laptop, and the party that acquires it tries to see what sensitive data it contains.

- A disgruntled employee boots a computer off third-party media to circumvent other security controls so the employee can access sensitive files (e.g., confidential data stored locally, local password file).

- Booting from the recovery partition in macOS.

Impact: Unauthorized parties could cause a loss of confidentiality, integrity, and availability.

Possible Controls:

- Implement physical security measures (e.g., locked doors, badge access) to restrict access to equipment.[6]

- Enable a strong and difficult-to-guess password for the Extensible Firmware Interface (EFI), and configure the EFI to boot the system from the local hard drive only, assuming that the case containing the OS and data is physically secure. This will help protect the data unless the hard drive is removed from the computer.

- Secure local files via encryption to prevent access to data if the physical media is placed in another computer.

2.3.1.2 Unauthorized Local Access

Threat: An individual who is not permitted to access a system gains local access.

Examples:

- A visitor to a company sits down at an unattended computer and logs in by guessing a weak password for a user account.

- A former employee gains physical access to facilities and uses old credentials to log in and gain access to company resources.

Impact: Because the unauthorized person is masquerading as an authorized user, this could cause a loss of confidentiality and integrity; if the user has administrative rights, this could also cause a loss of availability.

Possible Controls:

- Require valid username and password authentication before allowing any access to system resources, and enable a password-protected screen saver. These actions help to prevent an attacker from walking up to a computer and immediately gaining access.

[6] Organizations should have a physical and environmental protection policy that includes requirements for providing adequate physical security for systems and networks. Most technical controls can be easily defeated without physical security.

- Enable a logon banner containing a warning of the possible legal consequences of misuse.

- Implement a password policy to enforce stronger passwords, so that it is more difficult for an attacker to guess passwords.

- Do not use or reuse a single password across multiple accounts; for example, the password for a personal email account should not be the same as that used to gain access to the macOS system.

- Establish and enforce a checkout policy for departing employees that includes the immediate disabling of their user accounts.

- Physically secure removable storage devices and media, such as CDs and flash drives, that contain valuable information. An individual who gains access to a workspace may find it easier to take removable media than attempt to get user-level access on a system.

2.3.1.3 Privilege Escalation

Threat: An authorized user with normal user-level rights escalates the account's privileges to gain administrator-level access.

Examples:

- A user takes advantage of a vulnerability in a service to gain administrator-level privileges and access another user's files.

- A user guesses the password for an administrator-level account, gains full access to the system, and disables several security controls.

Impact: Because the user is gaining full privileges on the system, this could cause a loss of confidentiality, integrity, and availability.

Possible Controls:

- Restrict access to all administrator-level accounts and administrative tools, configuration files, and settings. Use strong, difficult-to-guess passwords for all administrator-level accounts [SP 800-63-3]. These actions will make it more difficult for users to escalate their privileges.

- Disable unused local services. Vulnerabilities in these services may permit users to escalate their privileges.

- Install application and OS updates. These updates will resolve system vulnerabilities, reducing the number of attack vectors that can be used.

- Encrypt sensitive data. Even administrator-level access would not permit a user to access data in encrypted files.

2.3.2 Remote Threats

Unlike local threats, remote threats do not require physical or logical access to the system. The categories of remote threats described in this section are network services, data disclosure, and malicious payloads.

2.3.2.1 Network Services

Threat: Remote attackers exploit vulnerable network services on a system. This includes gaining unauthorized access to services and data, and causing a denial of service (DoS) condition.

Examples:

- An attacker gains access to a system through a service that did not require authentication.
- An attacker impersonates a user by taking advantage of a weak remote access protocol.
- A worm searches for systems with an unsecured service listening on a particular port, and **then uses the service to gain full control of the system.**

Impact: Depending on the type of network service that is being exploited, this could cause a loss of confidentiality, integrity, and availability.

Possible Controls:

- Disable unused services. This provides attackers with fewer chances to breach the system.
- Install application and OS updates. These updates will resolve system software vulnerabilities, reducing the number of attack vectors that can be used.
- Require strong authentication (preferably multifactor authentication) before allowing access to a service. Implement a password policy to enforce stronger passwords that are harder to guess. Establish and enforce a checkout policy for departing employees that includes the immediate disabling of their user accounts. These actions help to ensure that only authorized users can access each service.
- Do not use weak remote access protocols and applications; instead, use only accepted, industry standard strong protocols (e.g., Internet Protocol Security [IPsec], Secure Shell [SSH], Transport Layer Security [TLS]) for accessing and maintaining systems remotely.
- Use firewalls or packet filters to restrict access to each service to the authorized hosts only. This prevents unauthorized hosts from gaining access to the services and also prevents worms from propagating from one host to other hosts on the network.
- Enable logon banners containing a warning of the possible legal consequences of misuse.

2.3.2.2 Data Disclosure and Data Integrity

Threat: A third party intercepts sensitive data sent over a network.

Examples:

- On a nonswitched wired network or an unsecured wireless network, a third party is running a network monitoring utility. When a legitimate user transmits a file in an insecure manner, the third party captures the file and accesses its data.
- An attacker intercepts usernames and passwords sent in plaintext over a local network segment or a wireless network.
- A man in the middle attack could occur on untrusted networks.

Impact: The interception of data could lead to a loss of confidentiality and/or data integrity. For example, if authentication data (such as passwords) are intercepted, it could cause a loss of confidentiality and integrity, and possibly a loss of availability.

Possible Controls:

- Use switched networks for wired networks, which make it more difficult to sniff packets.[7]
- Use a secure user identification and authentication system, preferably with multifactor authentication.
- Encrypt network communications or application data with various protocols (e.g., TLS, IPsec, SSH, WPA2) particularly when accessing the Internet from public Wi-Fi. This protects the data from being accessed by a third party. Where possible, use signatures and MACs (message authentication codes) to provide integrity.
- Use trusted and known Domain Name System (DNS) servers.

2.3.2.3 Malicious Payloads

Threat: Malicious payloads such as viruses, worms, Trojan horses, and active content attack systems through many vectors. End users of the system may accidentally trigger malicious payloads.

Examples:

[7] Switched networks cannot completely prevent packet sniffing. For example, techniques such as address resolution protocol (ARP) spoofing can be used to convince a switch to direct traffic to an attacker's machine instead of the intended destination. The attacker's machine can then forward the packets to the legitimate recipient.

- A user visits a web site and downloads a free game that includes a Trojan horse. When the user installs the game on her computer, the Trojan horse is also installed, which compromises the system.

- A user with administrative-level privileges surfs the web and accidentally visits a malicious web site, which successfully infects the user's system.

- A user opens and executes a payload that was attached to a spam or spoofed message.

- A user connects an untrusted or unprotected USB storage device.

- A user interacts with content hosted on a social network site.

Impact: Malware often gains full administrative-level privileges to the system, or inadvertently crashes the system. Malware may cause a loss of confidentiality, integrity, and availability.

Possible Controls:

- Operate the system on a daily basis with a standard or managed user account. Only use administrator-level accounts when needed for specific maintenance tasks. Many instances of malware cannot successfully infect or remain persistent on a system unless the current user has administrative privileges.

- Educate users on avoiding malware infections, and make them aware of local policy regarding the use of potential transmission methods, such as instant messaging (IM) software, social network services, and unknown or untrusted applications not downloaded from Apple's App Store. Users who are familiar with the techniques for spreading malware should be less likely to infect their systems.

- Use antimalware software as an automated way of preventing most infections and detecting the infections that were not prevented.

- Use application whitelisting technology to allow authorized applications to run and communicate externally over the network.

- Use email clients that support spam filtering—automatically detecting and quarantining messages that are known to be spam or have the same characteristics as typical spam.

- Use multiple web browsers. Although, browsers provide sandboxing technology to isolate the sessions, dedicate one browser to casual Internet surfing and searching. Use a second browser to interact with personal or work-related sensitive sites and services.

- Use multifactor authentication mechanisms, particularly when accessing sensitive remote services and data.

- Do not install or use non-approved applications (e.g., P2P, IM) to connect to unknown servers. Educate users regarding the potential danger caused by P2P, IM, social network

services, and unknown, untrusted, and unsigned software applications not downloaded from the App Store.

- Configure server and client software, such as email servers and clients, web proxy servers and clients, and productivity applications to reduce exposure to malware. For example, email servers and clients could be configured to block email attachments with certain file types. This should help to reduce the likelihood of infections.

- Configure systems, particularly in Specialized Security-Limited Functionality environments, so that the default file associations prevent automatic execution of active content files (e.g., Java, JavaScript).

This section has described various types of local and remote threats that can negatively affect systems. The possible controls listed for the threats are primarily technical, as are the controls discussed throughout this document. However, it is important to further reduce the risks of operating a macOS system by also using management and operational controls. Examples of important operational controls are restricting physical access to a system; performing contingency planning [SP 800-34r1]; backing up the system, storing the backups in a safe and secure location, and testing the backups regularly; and monitoring Apple mailing lists for relevant security bulletins. Management controls could include developing policies regarding macOS system security and creating plans for maintaining macOS systems. By selecting and implementing management, operational, and technical controls for macOS, organizations can better mitigate the threats that macOS systems may face.

Another reason to use multiple types of controls is to provide better security in situations where one or more controls are circumvented or otherwise violated. This may be done not only by attackers, but also by authorized users with no malicious intent. For example, taping a list of passwords to a monitor for convenience may nullify controls designed to prevent unauthorized local access to that system. Establishing a policy against writing down passwords (management control), educating users on the dangers of password exposure (operational control), and performing periodic physical audits to identify posted passwords (operational control) may all be helpful in reducing the risks posed by writing down passwords. On macOS, the keychain application is available to manage passwords. See Section 6.3.6 for more information. Technical controls may be helpful as well, such as using Personal Identity Verification (PIV) smart cards [CSD16], derived PIV [SP 800-157] credentials, or another method other than (or in addition to) passwords for system authentication (preferably multifactor authentication).

2.4 macOS Environments

This section describes the types of environments in which a macOS host may be deployed—Standalone, Managed, and custom—as described in the NIST National Checklist Program (NCP) [SP 800-70r4]. The typical custom environment for macOS is Specialized Security-Limited Functionality, which is for systems at high risk of attack or data exposure, with security taking precedence over functionality. Each environment description summarizes the primary threats and controls that are typically part of the environment.

2.4.1 Standalone

Standalone, sometimes called Small Office/Home Office (SOHO), describes small, informal computer installations that are used for home or business purposes. Standalone encompasses a variety of small-scale environments and devices, ranging from laptops, mobile devices, and home computers, to telework systems located on broadband networks, to small businesses and small branch offices of a company. Historically, Standalone environments are the least secured and most trusting. Generally, the individuals performing Standalone system administration are less knowledgeable about security. This often results in environments that are less secure than they need to be because the focus is usually on functionality and ease-of-use. A Standalone system might not use any security software (e.g., antimalware software, host-based firewall). In some instances, there are no network-based controls such as firewalls, so Standalone systems may be directly exposed to external attacks. Therefore, Standalone environments are frequently targeted for exploitation.

Because the primary threats in Standalone environments are external, and Standalone computers generally have less restrictive security policies than Managed or Specialized Security-Limited Functionality computers, they tend to be most vulnerable to attacks from remote threat categories. (Although remote threats are the primary concern for Standalone environments, it is still important to protect against other threats.) Standalone systems are typically threatened by attacks against network services and by malicious payloads (e.g., viruses, worms). These attacks are most likely to affect availability (e.g., crashing the system, consuming all network bandwidth, breaking functionality) but may also affect integrity (e.g., infecting data files) and confidentiality (e.g., providing remote access to sensitive data, emailing data files to others).

Standalone security has improved with the proliferation of small, inexpensive, hardware-based firewall routers that protect, to some degree, the Standalone machines behind them. The adoption of host-based firewalls is helping to better secure Standalone environments. Another key to Standalone security is strengthening the hosts on the Standalone network by patching vulnerabilities and altering settings to restrict unneeded functionality. The simplicity of a Standalone environment allows updates and patches to be applied quickly after they are released, because the updates are being delivered directly from the vendor, with no delays for local review.

2.4.2 Managed

The Managed environment, also known as an Enterprise environment, is typically comprised of large organizational systems with defined, organized suites of hardware and software configurations, usually consisting of centrally-managed workstations and servers protected from threats on the Internet with firewalls and other network security devices. Managed environments generally have a group dedicated to supporting users and providing security. The combination of structure and skilled staff allows better security practices to be implemented during initial system deployment and in ongoing support and maintenance. Managed installations typically use a domain model to effectively manage a variety of settings and allow the sharing of resources (e.g., file servers, printers). The enterprise can enable only the services needed for normal business operations, with other possible avenues of exploit removed or disabled. Authentication, account,

and policy management can be administered centrally to maintain a consistent security posture across an organization.

The Managed environment is more restrictive and provides less functionality than the Standalone environment. Managed environments typically have better control on the flow of various types of traffic, such as filtering traffic based on protocols and ports at the enterprise's connections with external networks. Because of the supported and largely homogeneous nature of the Managed environment, it is typically easier to use more functionally-restrictive settings than it is in Standalone environments. Managed environments also tend to implement several layers of defense (e.g., firewalls, antimalware servers, intrusion detection systems, patch management systems, email filtering), which provide greater protection for systems. In many Managed environments, interoperability with legacy systems may not be a major requirement, further facilitating the use of more restrictive settings. In a Managed environment, this guide should be used by advanced users and system administrators. The Managed environment settings correspond to an enterprise security posture that will protect the information in a moderate risk environment.

In the Managed environment, systems are typically susceptible to local and remote threats. In fact, threats often encompass all the categories of threats defined in Section 2.3. Local attacks, such as unauthorized usage of another user's workstation, most often lead to a loss of confidentiality (i.e., unauthorized access to data) but may lead to a loss of integrity (i.e., data modification) or availability (i.e., theft of a system). Remote threats may be posed not only by attackers outside the organization but also by internal users who are attacking other internal systems across the organization's network. Most security breaches caused by remote threats involve malicious payloads sent by external parties, such as malware acquired via email or infected websites. Threats against network services tend to affect a smaller number of systems and may be caused by internal or external parties. Both malicious payloads and network service attacks are most likely to affect availability (e.g., crashing the system, consuming all network bandwidth, breaking functionality) but may affect integrity (i.e., infecting data files) and confidentiality (i.e., providing remote access to sensitive data). Data disclosure threats tend to come from internal parties who are monitoring traffic on local networks, and they primarily affect confidentiality.

2.4.3 Specialized Security-Limited Functionality (SSLF)

A Specialized Security-Limited Functionality (SSLF) environment is any environment that is at high risk of attack or data exposure. Systems that are often found in SSLF environments include outward-facing web, email, and DNS servers, and firewalls. Typically, providing sufficiently strong protection for these systems involves a significant reduction in system functionality. It assumes that systems have limited or specialized functionality in a highly-threatened environment such as an outward facing firewall or public Web server, or the system's data content or mission purpose is of such value that aggressive trade-offs in favor of security outweigh the potential negative consequences to other useful system attributes such as interoperability with other systems. The SSLF environment encompasses computers that contain high value assets data such as highly confidential information (e.g., personnel records, medical records, financial information) and perform vital organizational functions (e.g., accounting,

payroll processing, air traffic control). These computers might be targeted by third parties for exploitation, but also might be targeted by trusted parties inside the organization.

An SSLF environment could be a subset of a Standalone or Managed environment. For example, three desktops in a Managed environment that hold confidential employee data could be thought of as an SSLF environment within a Managed environment. In addition, a laptop used by a mobile worker might be an SSLF environment within a Standalone environment. An SSLF environment might also be a self-contained environment outside any other environment—for instance, a government security installation dealing in sensitive data.

Systems in SSLF environments face the same threats as systems in Managed environments. Threats from both insiders and external parties are a concern. Because of the risks and possible consequences of a compromise in an SSLF environment, it usually has the most functionally restrictive and secure configuration. The suggested configuration is complex and provides the greatest protection at the expense of ease-of-use, functionality, and remote system management. In an SSLF environment, this guide is targeted at experienced security specialists and seasoned system administrators who understand the impact of implementing these strict requirements.

2.5 Security Controls Documentation

An organization typically has many documents related to the security of macOS systems. Foremost among the documents is a macOS security configuration guide that specifies how macOS systems should be configured and secured.[8] As mentioned in Section 2.2, NIST SP 800-53 proposes management, operational, and technical security controls for systems, each of which should have associated documentation. In addition to documenting procedures for implementing and maintaining various controls, every environment should also have other security-related policies and documentation that affect the configuration, maintenance, and usage of systems and applications. Examples of such documents are as follows:

- Rules of behavior and acceptable use policy;
- Configuration management policy, plan, and procedures;
- Authorization to connect to the network;
- Incident response plan;
- IT contingency plans; and
- Security awareness and training for end users and administrators.

[8] Organizations should verify that their macOS security configuration guides are consistent with this publication. Organizations without macOS security configuration guides should modify this document to create a configuration guide tailored for their environments.

2.6 Implementation and Testing of Security Controls

Implementing security controls can be a daunting task. As described in Section 2.2, many security controls have a negative impact on system functionality and usability. In some cases, a security control can even have a negative impact on other security controls. For example, installing a patch could inadvertently break another patch, or enabling a firewall could inadvertently block antimalware software from automatically updating its supporting content or disrupt patch management software, remote management software, and other security and maintenance-related utilities. Therefore, it is important to perform testing for all security controls to determine what impact they have on system security, functionality, and usability, and to take appropriate steps to address any significant issues.

As described in Section 5, NIST has compiled a set of security baselines as well as additional recommendations for security-related configuration changes. The controls proposed in this guide and the NIST macOS security baselines are consistent with the FISMA controls, as discussed in Section 2.2. See Section 5 for more information on the composition and use of these baselines.

Although the guidelines presented in this document have undergone considerable testing, every system is unique, so it is possible for specific settings to cause unexpected problems. System administrators should perform their own testing, especially for the applications used by their organizations, to identify any functionality or usability problems before the guidance is deployed throughout organizations.[9] It is important to confirm that the desired security settings have been implemented properly and are working as expected.

2.7 Monitoring and Maintenance

Every system needs to be monitored (ideally, continuously) and maintained on a regular basis so that security issues can be identified and mitigated promptly, reducing the likelihood of a security breach. However, no matter how carefully systems are monitored and maintained, incidents may still occur, so organizations should be prepared to respond to them [SP 800-61r2].[10] Depending on the environment, some preventative actions may be partially or fully automated. Guidance on performing various monitoring and maintenance activities is provided in subsequent sections of this document or other NIST publications. Recommended actions include the following:

- Subscribing to and monitoring various vulnerability notification mailing lists.
- Acquiring and installing software updates (e.g., OS and application patches, antimalware supporting content).

[9] Any changes made to the baselines or settings should be documented as part of the overall documentation of macOS systems' security configuration.

[10] Organizations should have an incident response policy and a formal incident response capability. For guidance on incident handling preparation and execution, see NIST SP 800-61 Revision 2, *Computer Security Incident Handling Guide*, available at https://doi.org/10.6028/NIST.SP.800-61r2.

- Monitoring event logs to identify problems and suspicious activity such as installation of unsanctioned software applications.
- Providing remote system administration and assistance.
- Monitoring changes to OS and software settings, as configuration drifts may occur over time.
- Protecting and sanitizing media.
- Responding promptly to suspected incidents.
- Assessing the security posture of a system through vulnerability assessments [SP 800-115].
- Disabling unneeded user accounts and deleting accounts that have been disabled for some time.
- Maintaining system, peripheral, and accessory hardware (periodically and as needed), and logging all hardware maintenance activities.

2.8 Summary of Recommendations

- Protect each system based on the potential impact to the system of a loss of confidentiality, integrity, or availability.
- Reduce the opportunities that attackers have to breach a system by resolving security weaknesses and limiting functionality according to the principle of least privilege.
- Select security controls that provide a reasonably secure solution while supporting the functionality and usability that users require.
- Use multiple layers of security so that if one layer fails or otherwise cannot counteract a certain threat, other layers might prevent the threat from successfully breaching the system.
- Conduct risk assessments to identify threats against systems and determine the effectiveness of existing security controls in counteracting the threats. Perform risk mitigation to decide what additional measures (if any) should be implemented.
- Document procedures for implementing and maintaining security controls. Maintain other security-related policies and documentation that affect the configuration, maintenance, and usage of systems and applications, such as an acceptable use policy, a configuration management policy, and IT contingency plans.
- Test all security controls, including the settings in the NIST security baselines, to determine what impact they have on system security, functionality, and usability. Take

1027 appropriate steps to address any significant issues before applying the controls to
1028 production systems.

1029 • Monitor and maintain systems on a regular basis so that security issues can be identified
1030 and mitigated promptly. Actions include acquiring and installing software updates,
1031 monitoring event logs, providing remote system administration and assistance,
1032 monitoring changes to OS and software settings, protecting and sanitizing media,
1033 responding promptly to suspected incidents, performing vulnerability assessments,
1034 disabling and deleting unused user accounts, and maintaining hardware.

1035

3. macOS Security Components Overview

This section presents an overview of selected security features offered by the macOS operating system (OS). This section highlights the security features and security-supporting features in macOS 10.12, such as privacy protection, anti-malware, and firewall capabilities.

3.1 System Integrity Protection

A new feature called System Integrity Protection (SIP) was added in OS X 10.11.[11] SIP prevents modification of many system files and directories by all users including root. These files can only be modified by specific Apple-signed processes, such as Apple software updates and installers. As a result, such files can no longer be customized for a secure configuration and many file permission settings have been removed from this guide. Protected files and directories include: `/System`, `/usr`, `/bin`, `/sbin`, and built-in applications. All protected files and directories are listed in the file `/System/Library/Sandbox/rootless.conf`. This list is shown in Appendix I.1.

3.2 Gatekeeper

Gatekeeper was a new feature in OS X 10.8 that essentially enforces high-level application whitelisting for installing applications. Already-installed applications are unaffected by Gatekeeper settings. There are two configuration options for Gatekeeper: to allow only applications from the App Store and to allow only applications from the App Store and "identified developers."[12] These settings can be overridden by right-clicking a restricted application in Finder, selecting "Open" and then providing administrator-level credentials, if requested. These actions only need to be performed once for each application.

3.3 Software Updates

In macOS 10.12, software updates are obtained from the App Store. The system can be configured to automatically download and install updates. See Section 4.3 for more information on macOS updates.

3.4 Privacy Settings

macOS provides several privacy settings to allow users control over the actions performed with their information. Examples include the following:

- Activating or deactivating Location Services, and restricting which applications can use Location Services;
- Controlling which applications can access the user's Calendar and Contacts;
- Sharing anonymous diagnostic information with Apple; and

[11] For more information, see: https://support.apple.com/en-us/HT204899.
[12] Apple provides what it calls a "safe downloads list", which identifies the developers whose applications can be downloaded through this Gatekeeper option.

- Configuring Safari to use "Do Not Track" headers.

3.5 Credential Management

A *keychain* is a mechanism for securely storing user passwords for applications and other small pieces of sensitive information, such as cryptographic keys, digital certificates, and account numbers. Using a keychain can greatly reduce the number of passwords that have to be remembered. The keychain itself has a password that must be entered to gain access to the passwords stored in the keychain; this protects the keychain contents from being accessed by unauthorized users. Because only a single password has to be remembered, more complex, harder-to-guess passwords can be chosen for applications.

By default, keychains are stored locally. Keychains can also be saved to removable media, such as a USB flash drive.[13] This allows passwords to be securely transported between Mac computers. A user can have multiple keychains, such as a portable keychain with only those passwords that need to be used on multiple computers, and a regular keychain (stored on the local computer) with the other passwords.

3.6 Host-Based Firewalls

macOS offers two host-based firewalls—an application-based one that can be configured through the GUI, and a protocol-based one that can be configured through the command line. The application-based firewall filters incoming network traffic only, by application, based on the digital signature of each application. For example, it can be configured to prohibit the use of email services (e.g., SMTP, POP3, etc.) when they are employed by applications other than the designated email client application, and it can prohibit the use of all email services when the designated email client application is not running. If an organization wants to prohibit the use of chat services, it can configure the application-based firewall to block all incoming chat service attempts.

The protocol-based firewall, `pf`[14], is a stateful inspection firewall that can restrict both incoming and outgoing network traffic based on the TCP and UDP port numbers that the traffic uses. `pf` is intended to be used by administrators and advanced users who want stronger protection and more control over network traffic than the application-based firewall can provide. Rules for the application-based firewall and the `pf` firewall may conflict with each other, but if either firewall denies access, the traffic is blocked. If "Enable stealth mode" or "Block all incoming connections" is enabled through the application firewall, `pf` is activated with a set of predefined rules. Creating custom rules for the application firewall, however, does not make rules for or enable `pf`. Additional information about `pf` is located in Section 6.6.1.

[13] Consult your organization's removable media policies to determine if this is acceptable in your environment.
[14] Before OS X 10.8, the protocol-based firewall was called `ipfw`. The `pf` firewall provides similar functionality to `ipfw`.

3.7 Storage Encryption

macOS 10.12 is FIPS approved and supports three forms of storage encryption: FileVault[15], FileVault 2, and Disk Utility. These encryption methods possess varying functionality and strengths. However, NIST recommends the full disk encryption capability provided by FileVault 2 or equivalent third-party validated solution.

FileVault 2 provides full disk encryption [SP 800-111] via the XTS-AES 128-bit encryption algorithm. Full disk encryption offers more coverage than just encrypting the home folder portions of the disk. FileVault 2 requires that the Recovery Partition (which typically is hidden from user view) be installed on the startup volume.

FileVault 2 cannot be used to encrypt data stored on removable media, network drives, and other non-local locations. For those cases, macOS provides Disk Utility, which performs many functions, including the encryption of disk images. A disk image is a file that contains encoded files and folders. Disk Utility can encrypt disk images, which allows encrypted files to be sent to others via email, file transfers, etc., and to be stored securely on removable media, network shares, and other locations. Disk Utility supports the FIPS 140 approved algorithms 128-bit and 256-bit AES encryption. In addition to encrypting disk images, macOS offers a method for producing encrypted backups on external media using Time Machine, which is explained in Section 4.2.

3.8 Code Execution Protection

The following are examples of macOS 10.12's code execution protection features:

- Address space layout randomization (ASLR) is a security technique that is supported by many operating systems, including macOS 10.12. When ASLR is used, executables and their related components (e.g., libraries, etc.) are placed into memory at random locations, so that an attacker (or malware) cannot predict or readily guess where one component is located based on the location of another component. ASLR is built into macOS 10.12, and the OS provides no option for disabling or otherwise configuring it.

- Execute disable (XD) is a feature built into the CPUs of macOS 10.12 systems that separates data and executables in memory. This helps to deter an attacker from injecting malicious "data" and then executing that data. There is no option for disabling XD.

- Several macOS features rely on application signing to identify particular applications and verify their integrity—examples include the application-based firewall and the keychains. Apple signs applications included with macOS, and third-party applications may be signed by their developers as well. The operating system may sign applications for use with certain OS features.

[15] macOS 10.12 does not support new instantiations of legacy FileVault. For more information on legacy FileVault, consult the previous version of this guide, SP 800-179.

- macOS offers application sandboxing. This separates an application from the rest of the host in designated ways, dictating which resources it is allowed to utilize. One benefit of sandboxing is that it prevents one application from accessing another application's data. Other benefits include restricting an application's network and file access. However, sandbox support must be built into the application, and the user cannot force an application to run in a sandbox. Sandboxing is used for all new applications on the App Store.

- macOS has a quarantine feature for downloaded files. When a file is downloaded from an external source, such as a web server or an email attachment, the application that downloaded it (i.e., Safari, Mail, or Messages) tags it as quarantined. When a user attempts the execution of a quarantined file, the user is presented with the download metadata (timestamp and location) and asked whether he or she still wants to execute the file or not. If the user agrees to execute it, the quarantine tagging is removed. The purpose of quarantining is to reduce the likelihood that a user will run a malicious executable that he or she has downloaded.

3.9 Encrypted Virtual Memory

macOS secures its virtual memory by encrypting it, thwarting attempts to extract sensitive data from it. This feature has been enabled by default since version 10.6. Disabling virtual memory encryption is not possible after version 10.8.

3.10 Application Whitelisting

macOS provides application whitelisting capabilities through its Parental Controls feature. This feature, if enabled, restricts which installed applications may be executed by a particular user. See Section 6.5.2 for additional information.

4. Installation, Backup, and Patching

This section provides guidance on installing, backing up, and patching macOS systems, as well as migrating data between macOS systems and identifying security issues in macOS systems.

4.1 Performing an Installation

This section discusses the basic methods for performing a macOS 10.12 installation, both for new installations and for upgrades. This section breaks down the installation process into three phases: media sanitization, old patches, and OS installation, migration, and upgrades. NIST recommends performing clean installations, when possible.

4.1.1 Media Sanitization

Appropriate methods for media sanitization are determined by the operating environment. For Standalone systems where FileVault is enabled, it is sufficient to erase the encryption keys. For SSLF and Managed systems, please defer to the organization's policy on media sanitization. More information on NIST's media sanitation guidance is located in [SP 800-88r1].

4.1.2 Old Patches

NIST recommends performing a clean install. However, when a clean install is not possible, old patches should be installed prior to an OS upgrade.[16] If a system is being upgraded from a previous version of macOS, it is recommended that all existing patches be installed for the OS before doing the upgrade. Also, if a new installation is being performed, but data is being migrated from an old system, it is recommended that the old system's OS be fully patched first.

4.1.3 OS Installation and Upgrades

For macOS, new installations, upgrades, and reinstallations use the same software. A new installation can be performed as "clean" or as a reinstall over an existing macOS 10.12 installation. Apple recommends doing a clean install if macOS 10.12 is already installed. This section will only provide instructions for clean installations and upgrades, not reinstallations.

New installations and upgrades follow the same basic process, except that new installations will ask more questions than an upgrade. For example, when a new installation occurs, the Setup Assistant performs operations such as configuring networking and creating an initial administrator account that are not necessary for an upgrade. The Installer presents the user with the option to run the Migration Assistant, which can transfer a user's configuration settings, accounts, data, etc. from another macOS system. See Section 4.1.4 for more on the Migration Assistant.

As of September 2017, it is no longer possible to obtain a new copy of macOS 10.12 from Apple via the App Store. However, 10.12 can be downloaded using an Apple account that has

[16] Apple states that some updates rely on previous updates: https://support.apple.com/en-us/HT201541.

previously downloaded the OS. It can be obtained through the **Purchased** tab in the App Store. Organizations should retain a copy of the version of macOS that comes with new systems so that they can restore to that version later if necessary.[17]

There are several methods of performing an installation or upgrade. These tend to fall into two categories:

- A **dynamic installation process**, involving performing a full installation of macOS 10.12 from installation media, then completing the configuration of the installed system (e.g., configuring security settings).

- The **monolithic imaging process**, which refers to setting up and configuring one system completely, then cloning it (creating an image of it) and copying that image to other systems. After the image is put in place, minor configuration changes may be needed, such as setting a unique system name and adding accounts for local users.

Administrators should be aware that, by default, the macOS installer creates a recovery partition that is used in the event of a system failure. The recovery partition is also required to enable FileVault. This is a good recovery mechanism, but it may present another attack vector.

The subsections below provide more detail on the available installation methods.

4.1.3.1 System Image Utility

System Image Utility is an Apple-provided utility that is available on macOS 10.12. System Image Utility is used to create a network disk image, which refers to a disk image that is accessible over a network. As part of the disk image creation process, the images can be preloaded with configuration profiles provided by Profile Manager. When the disk images are accessed over a network, a Mac with macOS Server software is required to host them. Depending on the source media available, the utility supports up to three image creation options, described below in Figure 1.[18] All image creation options are available if the OS installer app file is located in the Applications directory and selected in System Image Utility.

[17] If macOS 10.12 was never downloaded, it will not be available for download, even if the computer is already running macOS 10.12.

[18] For more information on image creation see https://support.apple.com/en-us/HT202061.

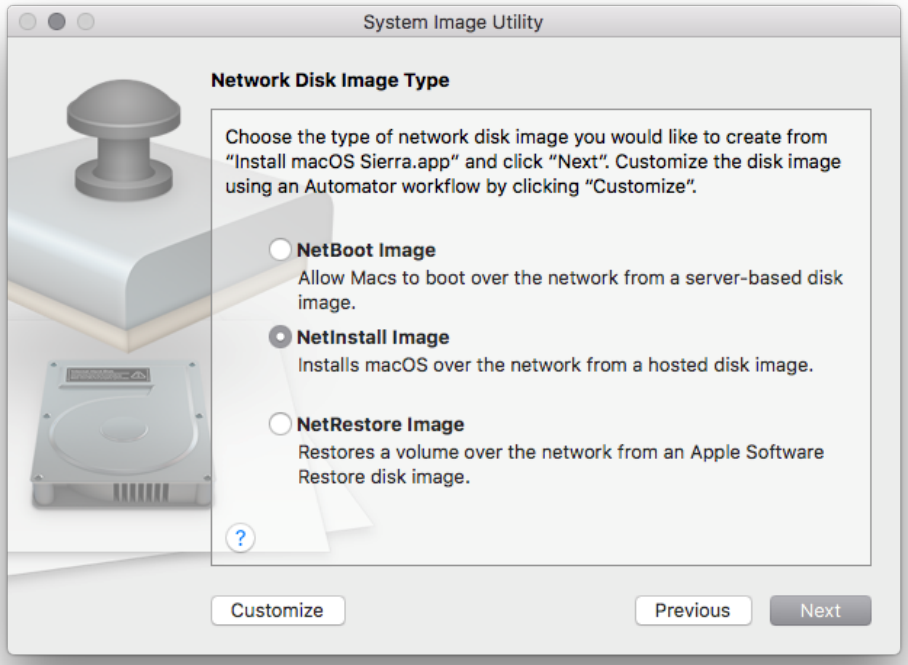


Figure 1: System Image Utility (after selecting the source "Install macOS Sierra.app")

- **NetBoot**: Boot a macOS 10.12 system from a remote network disk image (i.e., stored on a macOS Server). This image type is not appropriate for deploying images to systems, only for running systems remotely from an image.

- **NetInstall**: Install macOS 10.12 from a remote network disk image. This is similar to using the standard macOS 10.12 installer. It allows an administrator to select which macOS 10.12 packages are installed on a local system. The administrator will be responsible for configuring the system properly after the installation completes. In 10.12, it is now possible to create a NetInstall image with configuration profiles, scripts or other packages. This can be created separately from OS installation media.

- **NetRestore**: Restore a macOS 10.12 volume from a remote Apple Software Restore disk image. This type of system image is a clone of a configured macOS 10.12 system, and using this image will restore the cloned image onto a local system. There are no configuration options available for a NetRestore installation; the entire cloned image will be restored onto the system.

NetRestore images are used with Apple Software Restore (program name asr), which is a command-line utility included in macOS 10.12 systems that can restore a system based on a NetRestore image.

Note that there must be a DHCP server on the local network at boot time for the client to connect to the image storing machine. macOS Server can provide a DHCP server. To enable a DHCP server in the macOS Server application, expand the **Advanced** section on the left pane, select **DHCP**, and then toggle the **On/Off** switch.

4.1.3.2 Third-Party Utilities

There is a variety of third-party utilities that can perform custom installations of macOS 10.12. These utilities perform "imaging," but this is more complicated than simply copying an image to a host. Instead, these utilities perform modular installations of macOS 10.12 components that include extensive configuration of the system. The utilities can also execute scripts to perform customizations that are not directly supported by the utilities.

The advantage of using third-party utilities for installing macOS 10.12 is that they can handle both installation and configuration in an integrated and automated way, and administrators therefore do not have to do installation and configuration as separate steps. Configuration in particular can be a tedious manual process, although automated tools are increasingly available for implementing configurations. It is entirely feasible to do a standard macOS installation and then use a third-party utility to configure that installation.

4.1.4 Migration Assistant

Migration Assistant is a utility built into macOS 10.12 that can "transfer user accounts, applications, and computer settings" and data to a macOS 10.12 system from another Mac, a Windows PC, a disk from a Mac or PC, or a Time Machine backup. Although Migration Assistant can be very helpful at transferring user data (e.g., files) and profiles (i.e., accounts), it can inadvertently cause problems by migrating compromised, vulnerable, or outdated applications, as well as migrating security misconfigurations from one system to another.

It is recommended that Migration Assistant only be used to transfer user data and local profiles[19], preferably through Time Machine backups. Applications should not be migrated using Migration Assistant. Data and profiles should not be migrated until after macOS 10.12 and all applications have been installed and fully patched.

4.2 Backing Up

NIST recommends that data are backed up regularly and protected with a strong password. To increase the availability of data in the case of a system failure or data corruption caused by a power failure or other event, macOS has built-in capabilities to back up and restore data and systems. Time Machine is the built-in backup and restore utility. It does not provide all of the advanced backup and security features that third-party backup and restore utilities may offer, but it can encrypt its backups, and recover an entire disk in case of failure. It does backup updates once an hour, as long as the backup media is available, so it provides very granular backups.

[19] If a macOS system uses a domain account (non-local account), the account itself should not be migrated using Migration Assistant. Only local accounts should be migrated.

By default, Time Machine is disabled. To enable it, go to **System Preferences / Time Machine**, and set it to "ON". To configure it, click the "Select Disk…" button, select the disk that will hold the backups, enable the "Encrypt backups" option, and then click the "Use Disk" button. The system may prompt the user to allow the backup media to be erased and reformatted for compatibility. The system will also prompt the administrator to enter a backup password (to encrypt the backup) and a password hint. The administrator should enter a strong password to protect the backup and enter nothing useful for a password hint, to better protect the password. This password will be required every time the Time Machine backup media is connected to the macOS system, and to recover from a previously encrypted backup. However, the password can be saved in a keychain for automatic unlocking of the disk when it is connected. See Figure 2 for a sample Time Machine configuration.

Figure 2: Time Machine System Backup

When using an encrypted Time Machine disk, it is important to understand that a different (perhaps newer) version of macOS may not be able to restore from the encrypted Time Machine disk or may restore an invalid configuration. When using encrypted Time Machine backups, it is therefore important to have access to a macOS system running the same version (e.g., macOS 10.12) that was used to create the backups in order to guarantee the ability to recover backed-up data.

Another backup option built into macOS is iCloud. iCloud is available for limited backup capabilities, such as duplicating contacts in the cloud. Organizations should disable iCloud unless there is a specific reason to be using it for backup purposes or other reasons. Note that disabling iCloud also prevents use of the Find My Mac utility, which itself can pose security and

privacy risks. Location services must be running in order to use Find My Mac;[20] the use of location services is not recommended, however. To disable iCloud, go to **System Preferences / iCloud**, and deselect all of the services listed in the pane (Mail, Contacts, Calendars & Reminders, etc.) Note that users can re-enable iCloud without administrative privileges.

Besides the backup methods provided by Apple, there are also various third-party local and enterprise utilities for backing up and restoring files and systems. These can be used instead of or in addition to the Apple backup methods. Regardless of the backup method chosen, it is very important to verify periodically that backups and restores can be performed successfully; backing up a system regularly will not be beneficial if the backups are corrupted or the wrong files are being backed up, for example.

Organizations should have policies and procedures that address the entire backup and recovery process, as well as the protection and storage of backup and recovery media. Because backups may contain sensitive user data as well as system configuration and security information (e.g., passwords and KeyChain database), backup media should be properly protected to prevent unauthorized access. For additional guidance on backups and backup security, see [SP 800-34r1].

4.3 Installing Updates

It is essential to keep a system's operating system and applications up to current patch levels to eliminate known vulnerabilities and weaknesses. Apple provides two mechanisms for distributing security updates for Apple-provided software: the App Store and manual package updates. These are discussed below. There are also third-party applications that can be used to manage both Apple and non-Apple patches, and some non-Apple applications can update themselves automatically as well. Organizations should use one or more of these update mechanisms to ensure that the operating system and major applications are kept fully patched.

For more information on enterprise patch management and general recommendations for patching, see [SP 800-40r3].

4.3.1 App Store

Through the App Store preferences pane, a macOS system can be configured to check the App Store automatically every day for new updates, download them, and install them. Using the App Store is the preferred update mechanism for Standalone systems. If using this technique to keep a macOS system up-to-date, organizations should configure it to do the checks, downloads, and installations automatically. Figure 3 shows these options enabled. Note that because administrator-level credentials are needed for installation, update installation cannot be fully automated for typical users (who should not be running as administrator on a daily basis).

[20] https://support.apple.com/kb/PH25730?locale=en_US

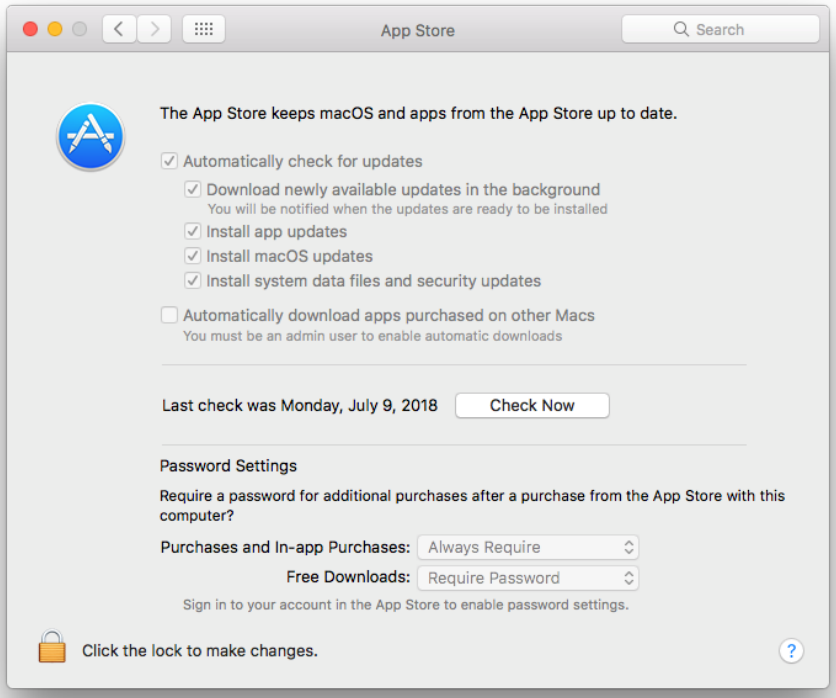


Figure 3: Software Update Options

Some organizations do not want the latest updates applied immediately to their macOS systems. For example, in a Managed environment, it may be undesirable for updates to be deployed to production systems until macOS administrators and security administrators have tested them. In addition, in large environments, many systems may need to download the same update simultaneously. This could cause a serious impact on network bandwidth. Organizations with such concerns often establish a local update server (using macOS Server) that contains approved updates and restrict the locations from which macOS systems can retrieve updates.[21] Managed and SSLF systems should follow their organizational update policies [SP 800-40r3]. See Appendix J.17 for a list of commands that can be used to configure system update settings through the command line.

4.3.2 Manual Package Updates

As discussed on Apple's server help page,[22] each update can be downloaded and installed through the command line. This allows scripting of the update process.

[21] For more information on setting up a local update server, see https://help.apple.com/serverapp/mac/5.6/#/apdE691575F-EDA4-4903-B09C-A49858EA1AEA.

[22] https://help.apple.com/serverapp/mac/5.6/#/apdE691575F-EDA4-4903-B09C-A49858EA1AE

Additionally, macOS system updates are available in packages known as combo updates. These updates can be downloaded to removable media and can be used to update new systems before they are connected to the Internet.

4.4 Summary of Recommendations

- Regardless of how an organization chooses to install macOS software and updates, the choices should be clearly described in a configuration management policies and procedures document, and both administrators and regular users should be instructed to follow the guidance contained therein.

- Media sanitization guidelines are determined by the operating environment. For Standalone systems with FileVault, encryption keys should be erased. For other systems, refer to the organizational policy.

- Apple recommends performing a clean installation instead of a reinstall. Migration Assistant should only be used to transfer user data and local profiles, but not applications.

- Until a new system has been fully installed and patched, either keep it disconnected from all networks, or connect it to an isolated, strongly protected network. System updates can be downloaded from Apple's website using a patched system, copied to external media and installed offline.[23]

- iCloud should be disabled unless there is specific reason to use it.

- Organizations should have policies addressing the entire backup and recovery process. Verify periodically that backups and restores can be performed successfully and that backups are protected.

- Keep systems up to current patch levels to eliminate known vulnerabilities and weaknesses.

[23] The macOS 10.12.6 combo update is available from Apple's website: https://support.apple.com/kb/DL1931?viewlocale=en_US&locale=en_US.

5. Overview of macOS Managed Security Configuration

This section discusses options for managing the security configuration of macOS desktops and laptops in a Managed environment.

5.1 Directory Services

A directory service is responsible for managing computing resources, such as computers, printers, and networks. It handles user authentication and ensures that connected resources follow organizational policies. This eases system administration because the systems are managed from a central location. Furthermore, user accounts are independent of the individual machines, which allows users to log in to any directory-bound computer. macOS systems are compatible with both the Open Directory and the Active Directory services.

5.2 Application Installation and Configuration

There are several methods available for installing applications, including the following:

- **Apple disk images** (`.dmg`). These are mainly used when an application just needs to be copied into the correct location in order to install it.

- **Installer application**. Installer is an application built into macOS that is used to install software from package (`.pkg`) and metapackage (`.mpkg`) files. It has a GUI version and a command line version (located at `/usr/sbin/installer`). The package and metapackage files can be used not only to install applications, but also to deploy application updates and application configuration settings.

- **App Store**. The App Store can be used to download and install a variety of applications from Apple and third parties.

- **Application-provided proprietary means**. A third-party application may provide its own proprietary installation method.

- **Third-party application management software**. An organization may use a utility that handles application management or software distribution, such as regulating which versions of software are permitted to be installed on the organization's systems and ensuring that this software is kept fully patched. These third-party utilities might also provide mechanisms for distributing application configuration settings.

While all of these methods may alter security configuration settings as part of their installation processes, note that two of these methods—the Installer application and third-party application management software—can be used outside of the installation process to distribute security configuration settings to macOS systems. This is useful for maintaining settings for already-installed applications.

In addition to the Installer application and third-party application management software, there are other means of altering settings for existing applications, as well as the operating system itself. For example, shell scripts can be run on a macOS system to alter OS configuration

settings. There is a variety of configuration management tools, some supporting the Security Content Automation Protocol (SCAP), which can also be used to alter OS and application settings.

5.3 Security Content Automation Protocol (SCAP)

System security is largely dependent upon staying up to date with security patches, maintaining well-considered configuration settings, and identifying and remediating other security weaknesses as they are identified. Unfortunately, macOS does not provide built-in utilities for assessing its system security, other than basic auditing capabilities. Third-party utilities are needed to verify patch installation, identify security configuration setting weaknesses, and find other security issues on macOS systems.

Configuration management tools are available that can be used to assess the security postures of macOS systems, either periodically or on a continuous basis (i.e., continuous monitoring). These tools have a variety of capabilities, such as comparing security settings with baseline settings and identifying missing patches. Some tools can also correct problems that they find by changing settings, installing patches, and performing other actions. Some tools can provide an independent verification that the security controls are implemented as intended and can document this verification for use in demonstrating compliance with laws, regulations, and other security requirements. NIST has been leading the development of SCAP [SP 800-117][SP 800-126r2], which is a set of specifications for expressing security information in standardized ways. Configuration management tools that support SCAP can use security baselines that are made publicly available by organizations such as NIST, and they can generate output in standardized forms that can be used by other tools.

6. NIST macOS Security Configuration

This section provides an overview of the security configuration options for macOS 10.12 systems and explains how they can provide better security than the default out-of-the-box parameters. These configuration options are grouped by the following categories:

- System Hardware and Firmware (Section 6.1),
- Filesystem Security (Section 6.2),
- User Accounts and Groups (Section 6.3),
- Auditing (Section 6.4),
- Software Restriction (Section 6.5),
- Network Services (Section 6.6),
- Applications (Section 6.7), and
- Other Security Management Options (Section 6.8).

Throughout this section, there are instructions for changing security configuration settings. The instructions may provide multiple values for each setting, depending on the profile (Standalone, Managed, SSLF). If only one value is specified, then it should be assumed that all profiles use that value. Some settings are applied to a single user, and a `~` in the directory path represents the path to the current user's home directory that will be modified. In order to modify another user's settings, use `~$USER` instead of `~`.[24] Unless explicitly stated otherwise, it is assumed in each case that the person making the changes has access to an administrator-level account on the macOS system and uses that account to make the changes. Using an administrator-level account to modify user-level configuration settings in this way may change a file's owner. See Appendix C for a list of tools that can be used to make configuration changes, along with short descriptions of their functionality.

Since most power-management settings are not security relevant, they are not included in the configuration; however, a few commands are included in Appendix J.15.

6.1 System Hardware and Firmware

A system is not secured unless the hardware and firmware have been secured. This section describes techniques for restricting access to firmware and disabling unneeded hardware components.

[24] See Appendix F for more information on system variables.

6.1.1 Restricting Access to Firmware

Macs have moved away from Open Firmware and have adopted the Extensible Firmware Interface (EFI). Other systems have made the same transition away from the comparable BIOS. The EFI launches the OS and determines whether the OS should boot normally or in single-user mode, which automatically logs in the root account, providing full administrator-level access to the system. Unauthorized booting in single-user mode is a major security weakness, but it can be prevented by setting an EFI password. An EFI password also prevents unauthorized personnel from booting the system from another media. Organizations should not rely on EFI passwords to provide security unless the physical security of the system is ensured. Be sure to consult the organization's policy on firmware security.

6.1.2 Disabling Hardware Components

macOS systems contain many hardware interfaces for purposes such as wireless networking, data transfer, and multimedia. Each interface creates a potential point of attack on the system. Accordingly, an organization may determine that one or more of these interfaces are unnecessary and should be disabled, particularly in SSLF environments. An example is an organization that prohibits the use of cameras on desktop and laptop systems. Another example is a policy that Bluetooth should be disabled if not paired with the system's keyboard, mouse, or trackpad. Organizations should determine which interfaces may be needed and disable all other interfaces. Organizations should be mindful of accessibility features made available through various hardware interfaces that might otherwise be unused. For example, accessibility features such as Dictation and VoiceOver make extensive use of the microphone (or line in) and speakers.

In previous versions of macOS it was possible to disable some hardware interfaces by moving the associated kernel extensions (files that end with a `.kext` extension) out of the `/System/Library/Extensions` directory, effectively disabling operating system support for the chosen interface. However, this action can no longer be performed due to System Integrity Protection (SIP).[25] In macOS 10.12, configuration settings must be changed to disable the interfaces. Note that with this method, in most cases users are able to override the configuration settings without any administrative privileges, so organizations should not rely on these configuration settings to provide security, since users can alter them at will. For any macOS host where disabling hardware interfaces is a security prerogative, the host's interfaces should be continuously monitored to detect any restoration of disabled interface functionality.

Note that disabling some hardware interfaces may impact the ability to use accessibility features. These settings are designed to improve ease-of-use and may be required for some users. These settings include text-to-speech, auditory alerts and the ability to control the system through voice commands. Accessibility settings may negatively affect security by causing information leakage, but this effect can be partially mitigated with modifications to the operating environment. The majority of these settings rely on the audio hardware interface. Accessibility features are disabled by default and NIST recommends that they remain off unless needed.

[25] See Section 3.1 for more information on SIP.

The methods for disabling hardware components can be implemented by running the commands found in Appendix J.1.

6.2 Filesystem Security

This section covers filesystem security for both internal and removable media. Its information is presented in the following categories: hard drive formatting and mounting, Finder, storage encryption, secure erase, file and folder permissions, and Spotlight.

6.2.1 Formatting and Mounting

The system's main hard drive partition should be formatted as HFS+. This filesystem supports all the filesystem security features provided by macOS 10.12.

Disk arbitration should not be disabled. Disk arbitration determines if new drives should be mounted automatically. Although disabling this prevents the inadvertent mounting of drives that may contain malicious content, this also prevents internal disks from being mounted upon system restart. macOS is unable to boot if disk arbitration is disabled.

Network filesystems can be automatically mounted with the automount tool. While convenient, access to remote files can pose a risk, especially if they are accessible by others. Remote files with setid bits enabled could run with elevated privileges. For this reason, automount should remain configured with the nosuid mount option. This is the default configuration, and NIST recommends that it should not be changed. See Appendix J.11 for the necessary commands.

6.2.2 Finder

Finder should be configured to show file extensions, to show a warning before changing a file extension and to search this system when performing a search. By default, Finder does not show hidden files and folders, which is beneficial to normal users unaware of the system's structure. However, administrators with intimate knowledge of the macOS system could notice unusual hidden files and would benefit from their visibility. Consequently, hidden files should be displayed in an SSLF environment. These options can improve defenses against malware. To configure these options, go to **Finder / Preferences / Advanced**; then enable the corresponding options as shown in Figure 4. To configure Finder settings through the command line, see Appendix J.2.

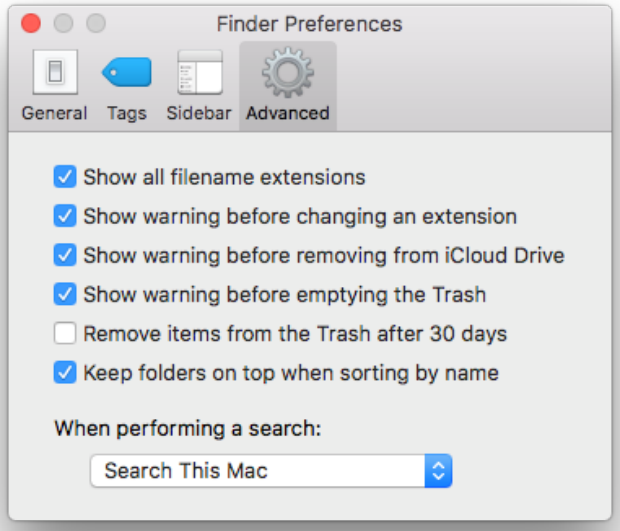


Figure 4: Advanced Finder Preferences

6.2.3 Storage Encryption

As discussed in Section 3.7, macOS 10.12 provides two mechanisms for storage encryption: FileVault 2 and encrypted disk images. NIST recommends the use of full disk encryption (FileVault 2).

6.2.3.1 FileVault 2

It is recommended when enabling FileVault 2[26] to log out of the system and log in with an administrator account. After doing so, go to **System Preferences / Security & Privacy / FileVault**. Select the button marked "Turn On FileVault…" to begin enabling FileVault. Designate which users should be allowed to unlock the FileVault encryption (i.e., log onto the system after it has been encrypted) and have each user authenticate him or herself.[27] macOS will then generate a recovery key[28] and present it on the screen so that it can be transferred to a secure location (not on the system) for use in case all the passwords on the system are forgotten or otherwise lost. macOS will provide an option to store the recovery key with Apple through the iCloud service; this key is only protected through recovery questions, so this option is not

[26] The macOS 10.12 user interface refers to FileVault 2 as FileVault. This section continues that convention.

[27] If a user is not available to authenticate him or herself at this time, the authentication step can be skipped. However, the user will need to authenticate within an administrator's session (**System Preferences** / **Security & Privacy** / **FileVault** tab, "Enable Users..." button).

[28] In version 10.6 and earlier, there was no recovery key; instead, there was a "master password". The recovery key has replaced the master password in terms of functionality.

recommended because of the possibility of the recovery key being retrieved by unauthorized personnel.

After rebooting the macOS system, the encryption process will begin for FileVault. This may take several hours, depending on the hardware characteristics of the system and the amount of data that needs to be encrypted. However, this encryption process can take place in the background while other work occurs. When finished, the FileVault settings page should look similar to that of Figure 5.

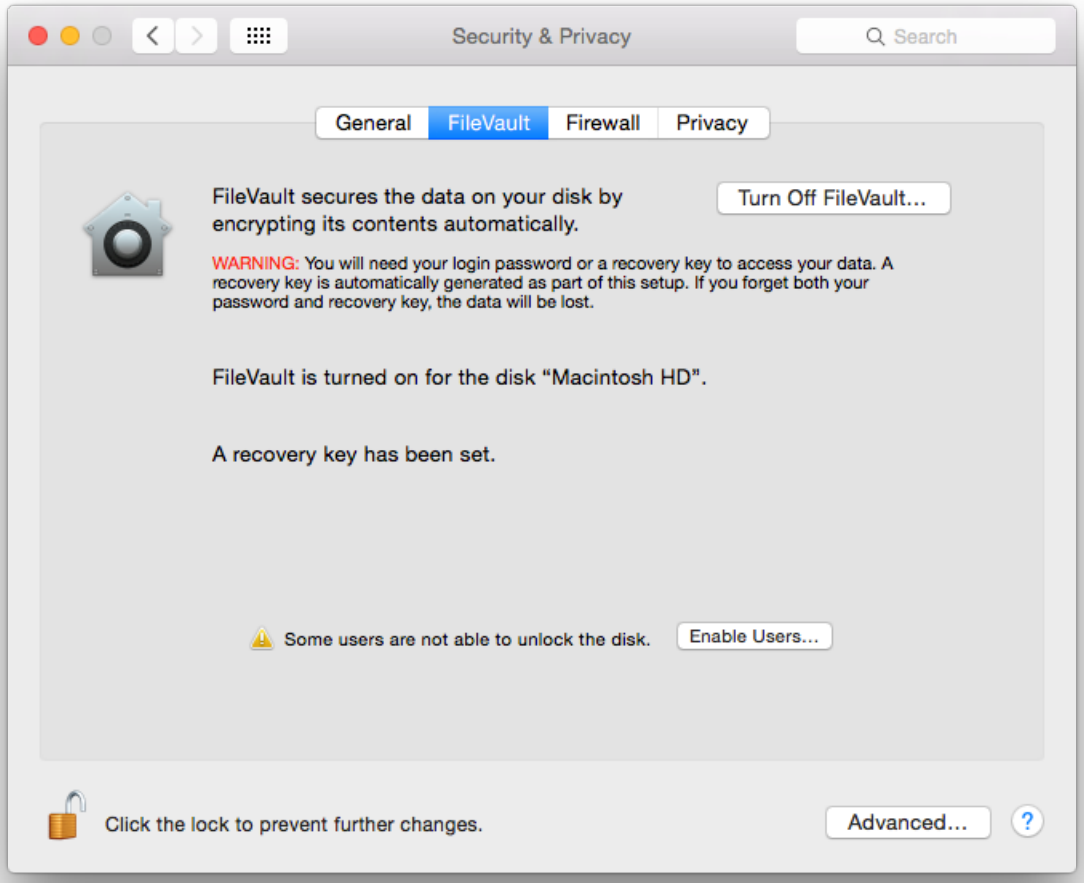


Figure 5: FileVault Settings

For more information on FileVault, see the Apple technical white paper titled "Best Practices for Deploying FileVault 2".[29] Of particular interest is that this paper describes additional enterprise tools for FileVault key management and recovery.

6.2.3.2 Encrypted Disk Image

As explained in Section 3.7, an encrypted disk image can be used to safeguard a single file or a group of files, in addition to (or instead of) using FileVault. The encrypted disk image can reside on the macOS system or on removable media. NIST recommends using encrypted disk images on drives where FileVault is not available. Users and administrators can follow these steps to create an encrypted disk image:

1. Run the **Disk Utility** and select **File / New / Blank Disk Image**.

2. Enter a name and location for the encrypted image to be stored. Set the size to the maximum that you may need (the size can't be changed after the image is created). Set the encryption to either 128-bit AES or 256-bit AES. After adjusting all the necessary settings, click the **Create** button.

3. Enter a password that will be used for decrypting the disk image. The dialog box provides an option to store the password in the user's keychain. When done with the dialog box, click the **OK** button. The encrypted disk image will be created using the designated name and location.

This technique can be very effective at securing individual files containing sensitive information, such as sensitive personally identifiable information (PII). A discussion of securing files in the form of email attachments is outside of the scope of this publication, but more information (e.g., on S/MIME) is available from [SP 800-45v2].

6.2.3.3 FIPS-Enabled System

By default, macOS 10.12 runs in FIPS mode (i.e., uses FIPS-validated[30] cryptographic modules).

6.2.4 Secure Erase

The Secure Erase feature existed in prior versions of macOS, but has since been removed from Finder[31] and Disk Utility.[32] Recommendations for secure file deletion can be found in [SP 800-88r1].

---

29 https://web.archive.org/web/20170822164742/https://training.apple.com/pdf/WP_FileVault2.pdf

30 https://km.support.apple.com/library/APPLE/APPLECARE_ALLGEOS/HT207497/APPLEFIPS_GUIDE_CO_macOS10.12.pdf

31 Note the section on Finder: https://support.apple.com/en-us/HT205267.

32 https://support.apple.com/kb/PH22241?locale=en_US

6.2.5 File and Folder Permissions

macOS's file and folder permissions have their roots in BSD Unix; although macOS has significant changes from BSD Unix, file and folder permissions should look familiar to Unix-savvy administrators. Examples include requiring certain critical system files (such as `/usr/bin/sudo`) to be owned by `root` and group-owned by `wheel`, setting modes (e.g., `644`, `755`) on particular files and folders, and removing the setuid bit from selected system executables.[33]

In previous versions of macOS, administrators were responsible for configuring file system access control mechanisms (e.g. setuid, rwx bits) to protect system files. However, most of the system files are now protected by SIP, and thus can no longer be modified. The NIST baselines include permission settings only for the user home directories. These settings exist to prevent users from accessing other users' files on the same system. See Appendix I.2 for more information on user home directory permissions.

6.2.6 Spotlight

Spotlight is a system-wide search capability. It indexes files to facilitate fast searches. However, this indexing can inadvertently capture sensitive information, potentially exposing it to unauthorized access. Organizations should evaluate these risks and determine if particular files or groups of files should be omitted from Spotlight indexing and searching, such as files containing sensitive PII. To specify folders to be excluded, go to **System Preferences / Spotlight / Privacy**. In this pane, add the folders or disks that should not be searched by Spotlight. Note that users can alter these settings without administrative privileges.

Spotlight searches are not limited to the local system. Queries, including any potentially sensitive information they contain, are sent to third-party Internet search providers. In order to protect user privacy, this functionality should be disabled. To disable these features, open **System Preferences / Spotlight / Search Results** and uncheck "Spotlight Suggestions" in the scroll area and "Allow Spotlight Suggestions in Look up" at the bottom of the window as shown in Figure 6. "Allow Spotlight Suggestions in Look up" can be disabled with the terminal command available in Appendix J.13.

[33] An explanation of file and folder permissions can be found at http://www.nersc.gov/users/storage-and-file-systems/unix-file-permissions/.

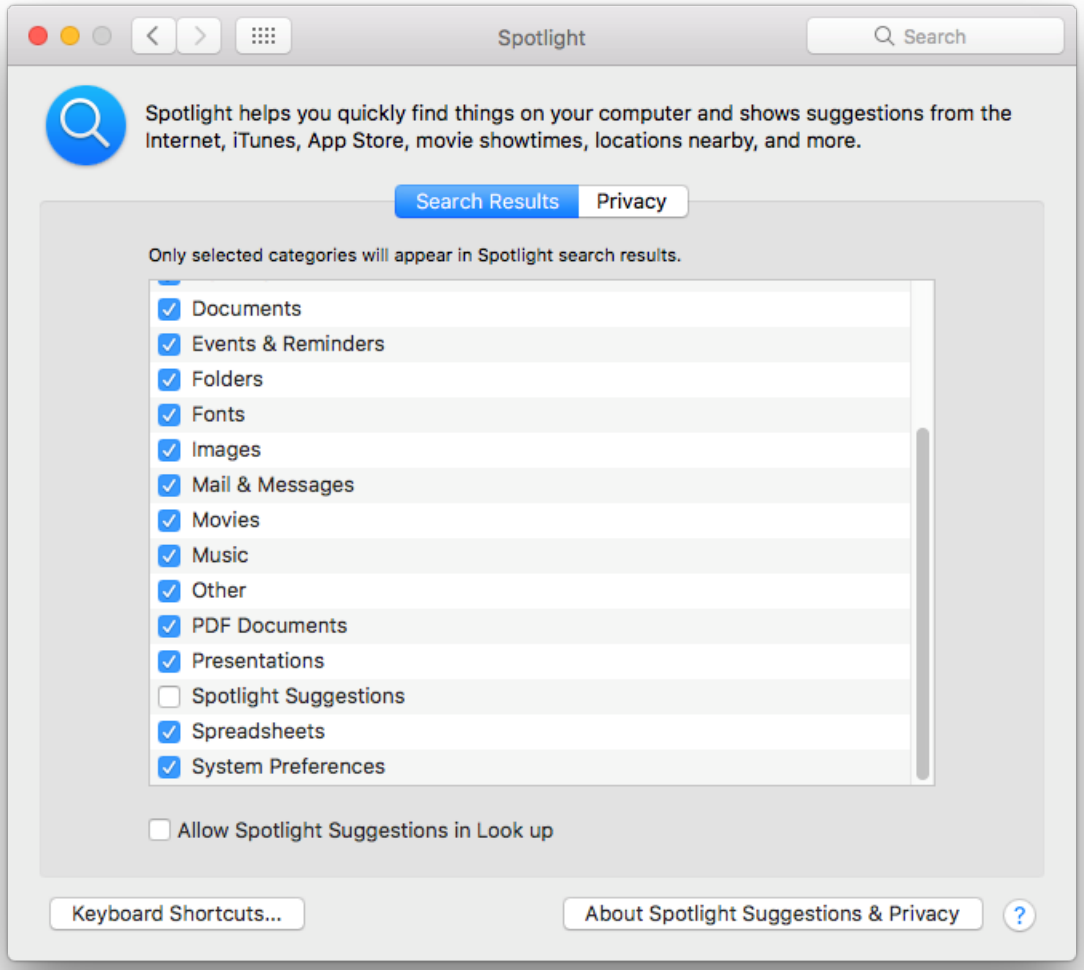


Figure 6: Spotlight Search Results

6.3 User Accounts and Groups

This section discusses the configuration settings related to user accounts and groups. The discussion is divided into the following categories: user account types, login options, parental controls, password policies, session locking, credential storage, alternate credentials, and sudo.

6.3.1 User Account Types

There are three general types of accounts for users: administrator, standard, and managed. Administrator accounts can do everything. Administrator accounts should only be used for system administration tasks. At least one non-administrator (standard) account should be created for daily operation of the system. A standard account can do things, including installing software, that affect the account owner but not other users. A managed account is just like a

standard account, except that there are some additional restrictions available (**System Preferences / Parental Controls**), including application limitations.

Each user should be utilizing a unique standard or managed account for his or her daily use of a macOS system. User account settings are accessible under **System Preferences / Users & Groups**.

NIST recommends that administrators periodically review user accounts and disable those that have been inactive for 90 days, as well as disabling temporary accounts after 30 days. Organizations should follow procedures to disable accounts as soon as they are no longer needed (e.g., the user leaves the organization or the user's responsibilities change). Disabled accounts should be deleted after a specific period to release resources and prevent unneeded accounts from accidentally being re-enabled.

There are some special built-in accounts on macOS systems:

- **Guest**. The Guest account, a special managed account, is considered a security vulnerability in most situations because it has no password associated with it. Once an attacker has gained guest-level access, the attacker can try to elevate privileges to further exploit a system. NIST recommends that the Guest account be disabled on all macOS systems unless there is a clearly demonstrated need to use a Guest account. The Guest account is not allowed to log in to a computer by default. However, guest users can access shared folders remotely by default. This setting is called "Allow guest users to connect to shared folders" and should be disabled. Both of these settings are available under **System Preferences / Users & Groups / Guest User** and are disabled by default. Note that when a guest logs out of a macOS system, the guest's environment is destroyed and reinitialized.

- **Root**. The root account is not to be confused with the administrator accounts; root is a separate account that is disabled by default. Root and administrator accounts have similar privileges, but the root account has considerably less overhead associated with it (for example, the person does not have to authenticate repeatedly to issue administrator-level commands when using the root account). The root account is intended for command line access. NIST recommends that the root account be disabled on all macOS systems and that a separate administrator account be established for each person who will be performing regular administrative tasks. The administrator accounts should then use the `sudo` command to perform actions with root-level privileges even if the root account is disabled. An administrator uses the `sudo` command to perform system-wide modifications. The root account should be the only account with User ID 0.

Other types of users include local, network, and mobile, but these classifications only refer to the account's physical location and not the associated privilege levels. It is recommended to have accounts of all types hidden from the login screen so that account names are not visible, but it is also useful to understand the available account types. Local user accounts are the default account type and exist solely on the system on which they are created. Network accounts allow a user to login from any system on the network, and the user's files on one system are independent of all the others. Alternatively, network accounts can be configured to use a centralized home folder,

which allows access from any networked system. Mobile accounts are similar to network accounts, but the user's home folder contents are synchronized between the different systems.

However, even with all account types hidden, FileVault-enabled systems display usernames at the initial login screen. Additionally, the username is visible on the lock screen if a user has an active session. With FileVault enabled, usernames are only hidden after a user has authenticated with the system and then logged out.

6.3.2 Login Options

The Login Options pane within the **System Preferences / Users & Groups** screen contains several options related to user login, as shown in Figure 7. Sections 6.3.2.1 through 6.3.2.5 provide additional information on several of these security- and privacy-related options.

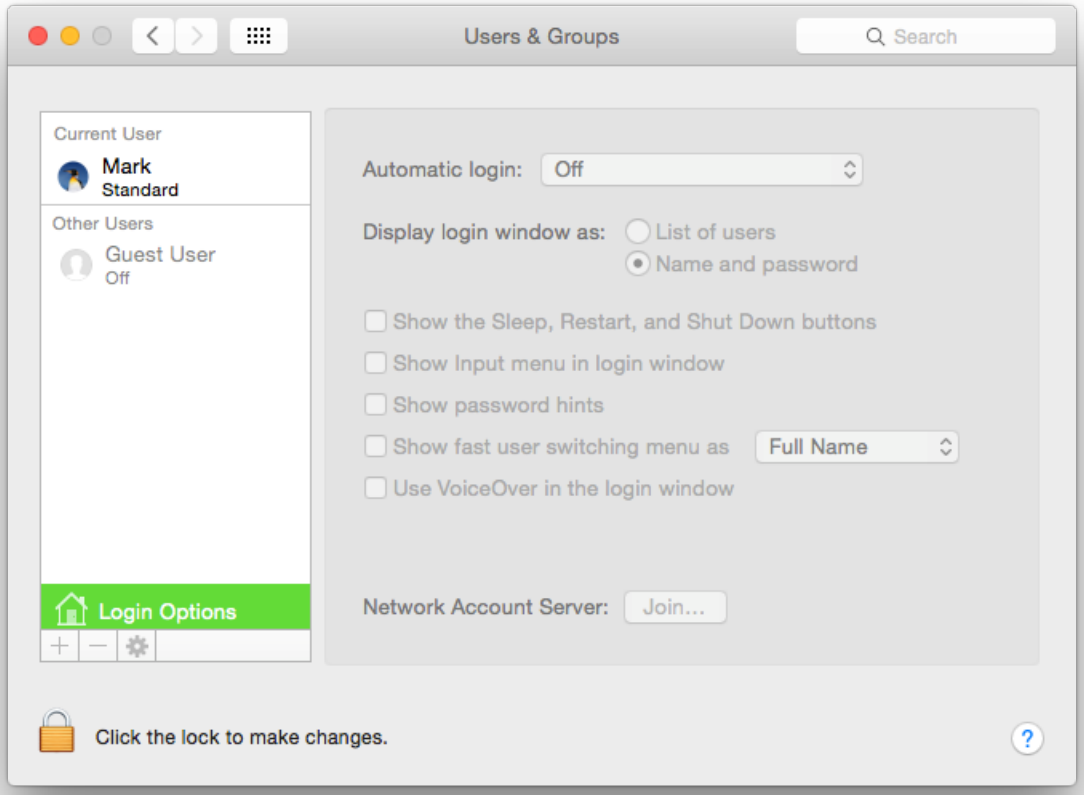


Figure 7: Login Options Pane

The user login options shown in the GUI can also be configured via the command line. The commands for these login-related options can be found in Appendix J.4. Some login window options are not available to be changed through the GUI. These command-line-only settings can be configured using the commands in Appendix J.4.

6.3.2.1 Automatic Login

By default, macOS requires credentials to log into an administrator account and does not log in automatically. The corresponding configuration setting for this is shown at the top of Figure 7.

6.3.2.2 Display Login Window

The NIST baselines set the display login window option to "Name and password", as shown in Figure 7. The "List of users" option displays a list of usernames on the login window. This option would only require an attacker to obtain the password in order to be authenticated. If name and password boxes are shown instead, an attacker would have to know not only a password, but also the username that corresponds with it. This makes an attack slightly harder, but it also makes login more inconvenient for users. Organizations should weigh the security benefits against the usability impact and decide which setting is best for the circumstances.

6.3.2.3 Password Hints

One of the options shown in Figure 7 is "Show password hints". If enabled, this will display password hints that users have created for their accounts to help them remember their passwords. Although this can improve usability, it can also significantly affect security in a negative way by helping attackers to recover user passwords. As with the Display Login Window option described in Section 6.3.2.2, organizations should consider both security and usability when determining how this option should be set. The NIST baselines disable this option. See Appendix J.4 for the password-hint configuration setting.

6.3.2.4 Fast User Switching

NIST recommends disabling fast user switching for systems in Managed and SSLF environments that have policies against its use. The fast user switching feature permits two or more users to be logged into the same macOS system simultaneously. Only one user session is in the foreground at any given time. The employment of fast user switching is beneficial on low-security systems where someone may need brief access to a system that is in use, because it preserves security and privacy for both people while minimizing the impact on usability. This is a good alternative to having users share their accounts.

However, on other systems, the risks associated with having multiple users logged in simultaneously may be considered too great. In such cases, the fast user switching capability should be disabled, requiring one user to log out before another user logs in. To disable fast user switching, disable the Figure 7 option involving fast user switching ("Show fast user switching menu").

6.3.2.5 Network Account Server

NIST recommends following organizational policy on joining an Active Directory domain. The last configuration setting in Figure 7 is for the use of an Active Directory domain or an Open Directory server. By clicking on the "Join…" button, a computer can be associated with an organization's directory server.

6.3.2.6 Console Login

If the login window is displayed as "Name and password," a user may attempt a console login. This is performed by typing exactly ">console" (without the quotes) into the username field on the login screen. Informal testing at NIST revealed that, in its default configuration, use of this feature may cause the system to become unresponsive. Console logins can be disabled by running the Terminal command listed in Appendix J.4.

6.3.3 Parental Controls

If Parental Controls are enabled for a user account, a wide variety of restrictions can be placed on what the user can do on the system. This includes restricting which applications may be executed, as described in Section 6.5.2. Other types of restrictions of potential interest for security include the following:

- Which websites the user can visit,
- What hours of the day the system can be used, and
- Whether CDs and DVDs can be burned on the system.

6.3.4 Password Policies

In addition to educating users regarding the selection and use of passwords, it is also important to set password parameters so that passwords are sufficiently strong. This reduces the likelihood of an attacker guessing or cracking passwords to gain unauthorized access to the system. The following parameters are specified in the NIST baselines:

- **Maximum password age**. This forces users to change their passwords after a password has reached the maximum age. The lower this value is set, the more likely users will be to choose poor passwords that are easier for them to remember (e.g., Mypasswd1, Mypasswd2, Mypasswd3). The higher this value is set, the more likely the password will be compromised and used by unauthorized parties.
- **Minimum password length**. This specifies the minimum length of a password in characters. The rationale behind this setting is that longer passwords are more difficult to guess and crack than shorter passwords. The downside is that longer passwords are often more difficult for users to remember and to enter accurately. Organizations that want to set a relatively large minimum password length should encourage their users to use passphrases, which may be easier to remember than conventional passwords.
- **Password complexity requirements**. macOS has several settings that can be used to require a mixture of character types, including uppercase and lowercase letters, digits, and special characters such as punctuation marks. Additionally, there is a setting to ensure that a password does not have a guessable pattern. These settings can make it more difficult to guess or crack passwords.

- **Enforce password history**. This setting determines how many old passwords the system will remember for each account. Users will be prevented from reusing any of the old passwords. For example, if this is set to 15, then the system will not allow users to reuse any of their last 15 passwords. Old passwords may have been compromised, or an attacker may have invested resources to crack encrypted passwords. Reusing an old password could inadvertently give attackers access to the system.

- **Account lockout**. This policy item is designed to prevent brute force guessing of user passwords. It is a combination of two attributes and determines when a user account should be locked after failed login attempts. Two components influence this setting: failed attempts before lockout and lockout duration. For example, three failed password attempts could result in the account being locked for 15 minutes.

- **Guessable pattern**. This policy dictates that a password cannot contain more than two sequential (ascending or descending, e.g., "321") or consecutive (run of the same, e.g., "aaa") characters. This prevents users from creating easily guessable passwords.

One of the main challenges in setting account policies is balancing security, functionality, and usability. For example, locking out user accounts after only a few failed logon attempts in a long time period may make it more difficult to gain unauthorized access to accounts by guessing passwords, but may also sharply increase the number of calls to the help desk to unlock accounts accidentally locked by failed attempts from legitimate users. This could cause more users to write down their passwords or choose easier-to-remember passwords. Organizations should carefully think out such issues before setting macOS account policies.

Note that the macOS 10.12 GUI does not provide any mechanisms for setting password or account lockout policies. Instead, these settings can be accessed via a command prompt using the `pwpolicy` command.

The `pwpolicy` configuration utility does not appear to apply all of the available password rules typically available in Managed environments. To deter password guessing attacks, macOS can be configured to lock out (i.e., disable) an account when too many failed login attempts occur. Note that if the accompanying failed login reset time policy is not set, a locked account remains inaccessible until an administrator intervenes.

There are two ways to set password policy settings: apply them to specific users or set a global policy. User-specific policies override global policies, so the user policies must either be left unset or be set along with the global policies. Alternatively, on macOS 10.12, existing policies can be cleared on a per-user basis with the command `pwpolicy –u $USER -clearaccountpolicies` before applying global policies to ensure that they affect all users. Use the Terminal commands given in Appendix J.5 to change password policy settings.

6.3.5 Session Locking

It is important to provide protection against unauthorized local access to macOS systems. One such control is to lock the current user's session through automatic or manual means. A screen saver can lock a session automatically after the system has been idle for a certain number of

minutes, requiring the user to authenticate before unlocking the system. NIST recommends using an authentication-enabled screen saver on all macOS systems that need protection from unauthorized physical access. Settings for enabling a screen saver (which is accomplished by setting a "start after" time other than "Never") are located in **System Preferences / Desktop & Screen Saver / Screen Saver**. NIST recommends that the screen saver be set to start after 20 minutes of idle time. If values other than 1, 2, 5, 10, 20, 30, or 60 are used, the idle time value will be reset to 20 the next time the Screen Saver preferences pane is opened. Depending on the accessibility of the system and its environment, a different value may be more suitable.

Other screen saver options for locking are located under **System Preferences / Security & Privacy / General**. To require locking, enable the option to "Require password after sleep or screen saver begins" and set it to "Immediately" or "5 seconds". From a security perspective, these are roughly equivalent; from a system usability perspective, setting it to "5 seconds" may be much more convenient for users than setting it to "Immediately," while not significantly impacting security. There is also an option for the login window screen saver that can be configured through the command line. Note that users can alter any of the screen saver options and that these options are set per user, not per system.

Users can manually lock their sessions. A user can put the cursor over a designated "hot corner" of the screen to automatically lock the system, if this has been configured (located under **System Preferences / Desktop & Screen Saver**). Selecting either of the "Put Display to Sleep" or "Start Screen Saver" hot corners will allow the user to lock the session. In order to improve ease of access, the use of a modifier key in conjunction with the start-screen-saver hot corner is not recommended. Users are cautioned not to designate any of the hot corners as "Disable Screen Saver" because this could inadvertently reduce security.

There is another option that only administrators can set related to session locking. Under **System Preferences / Security & Privacy**, click the "Advanced…" button and uncheck the option to "Log out after x minutes of inactivity". If checked, this option could cause users' work in progress to be lost. It is more user friendly to have a password-protected screen saver instead of the inactivity log out option.

Session-locking settings can also be configured through the command prompt. See Appendix J.6 for NIST recommendations on the Standalone, Managed, and SSLF profiles for session locking settings.

6.3.6 Credential Storage

Section 3.5 has already described the macOS feature known as keychains. Although password management as provided by keychains is a valuable security feature, by default it is not configured as securely as it should be.

By default, the user account and primary keychain have the same password set. Additionally, the primary keychain is unlocked when the user logs in (since the passwords are the same). To set a different password for the primary keychain, run the **Keychain Access** utility, and choose the primary keychain from the list of keychains. Click on **Edit / Change Password for Keychain**, and change the keychain's password. Note that this may impact some core services that use the

keychain, such as the caching of the encryption passphrases for wireless networks. NIST recommends separating daily-use passwords from those used for sensitive information access. Creating a separate keychain can be accomplished by clicking the "+" icon at the bottom of the **Keychain Access** window.

NIST recommends that the keychain locks when the screen saver starts. By default, keychains do not automatically lock when a system sleeps. This increases the risk of unauthorized disclosure or modification of keychain data. To correct this, run the **Keychain Access** utility and choose the primary keychain from the list of keychains. From the menu, select **Edit / Change Settings for Keychain**, and select the "Lock when sleeping" option. A related setting found on the same menu, "Lock after x minutes of inactivity", causes the keychain to lock after it has not been used for x minutes.

6.3.7 Alternate Credentials

macOS supports the use of alternate credentials for logical user authentication; examples include token-based authentication, biometric-based authentication, and Personal Identity Verification (PIV) cards. As shown at the bottom of Figure 7, there is a "Network Account Server" option in the **Users & Groups** window. Clicking on the "Join…" button opens a window for specifying the Open Directory or Active Directory server that should be used for alternate credentials. If the server name is not known, or additional options are needed, click on the "Open Directory Utility…" button to run the **Directory Utility** application.

If alternate credentials are not being supported, and there is no other reason to enable directory services, then directory services should not be enabled to prevent their possible abuse and exploitation. A common example is Standalone systems, which often do not bind to any directories.

6.3.8 Sudo

The `sudo` program allows an account with administrator privileges to perform an action as the super user (root). This is very powerful functionality, and its use needs to be controlled. Options related to `sudo` are located in `/private/etc/sudoers` and can be modified using the `visudo` command.

`sudo` restrictions should be applied to SSLF systems. NIST recommends requiring user authentication for each invocation of the `sudo` command. This setting can be found in Appendix J.3.

6.4 Auditing

This section discusses macOS 10.12's configuration settings related to auditing and system logging. Systemwide security auditing is enabled by default.

6.4.1 Audit Policies and Tools

macOS 10.12's auditing capabilities are based on `auditd`. macOS logs contain error messages, audit information, and other records of activity on the system that can be filtered with

`auditreduce` and viewed via the `praudit` command line utilities. These audit logs are independent of messages recorded by the `syslogd` system logging utility. Only administrators can read audit log files, and they do not show up in the Console utility.

The audit control file, `/etc/security/audit_control`, contains the policies for system auditing. Audit logs must be maintained for a sufficient amount of time—30 days—and must record all security-relevant events. The NIST configuration allows for a minimum of 5 GB of log storage. Logs older than 30 days will only be deleted if more than 5 GB of space is used by the auditing subsystem. Additionally, the maximum recommended size per audit file is 80 MB. Table 1 describes the NIST recommended audit event flags and Appendix J.14 explains how to configure audit settings.

Table 1: audit_control Flags

`audit_control` Flag	Flag Description
`lo`	Login and logout events
`ad`	Administrative events
`-all`	All failed events
`fd`	File deletion events
`fm`	File attribute modify events
`^-fa`	Do not log failed file attribute access events
`^-fc`	Do not log failed file creation events
`^-cl`	Do not log failed file closure events

Logging should be enabled and log retention time should be specified for various system logs for all environments. The logs on each system should be reviewed on a regular basis; the logs can be used not only to identify suspicious and malicious behavior and investigate security incidents, but also to assist in troubleshooting system and application problems. If the log retention time is very low, the system will not store as much information on system activity. Some organizations may have a logging policy and central log servers, so the baseline settings may need to be adjusted so they comply with the policy.

Other files involved with system auditing are `/etc/security/audit_warn` and `/etc/security/audit_user`. The shell script `audit_warn` is responsible for handling warning messages generated by `auditd`. `audit_warn` can be customized to perform actions depending on the type of warning messages received. The `audit_user` file contains the auditing events to record on a per-user basis. This file can specify that additional events not included by the `/etc/security/audit_control` file also be recorded.

It is recommended that auditing remain enabled; however, if auditing must be disabled, use the following commands, in the specified order. First, use `audit -t` to disable auditing for the

current session. Then, in order to prevent the `auditd` process from restarting at the next boot, use `launchctl disable system/com.apple.auditd`. The `auditd` process can be reenabled with `launchctl enable system/com.apple.auditd` and then restarting the system.

6.4.2 Date and Time Setting

It is important to configure macOS systems to synchronize their clocks on a regular basis with accurate time sources. If audit logs contain evidence of an attack, and the system's clock is inaccurate, the analysis of the attack is more difficult and the evidentiary value of the logs may be weakened. Time synchronization is convenient because users do not need to manually adjust the clock to compensate for inaccuracies in the system's timekeeping. macOS uses the Network Time Protocol (NTP) for time synchronization.

To configure a macOS host to use NTP, choose **System Preferences / Date & Time**. Enable the "Set date & time automatically" option and enter the name of the organization's designated NTP server (or select one of the Apple-provided default time servers). If there is more than one designated NTP server, their names can be entered as a list, separating each entry from the others with a space. Figure 8 below shows the **Date & Time** settings panel.

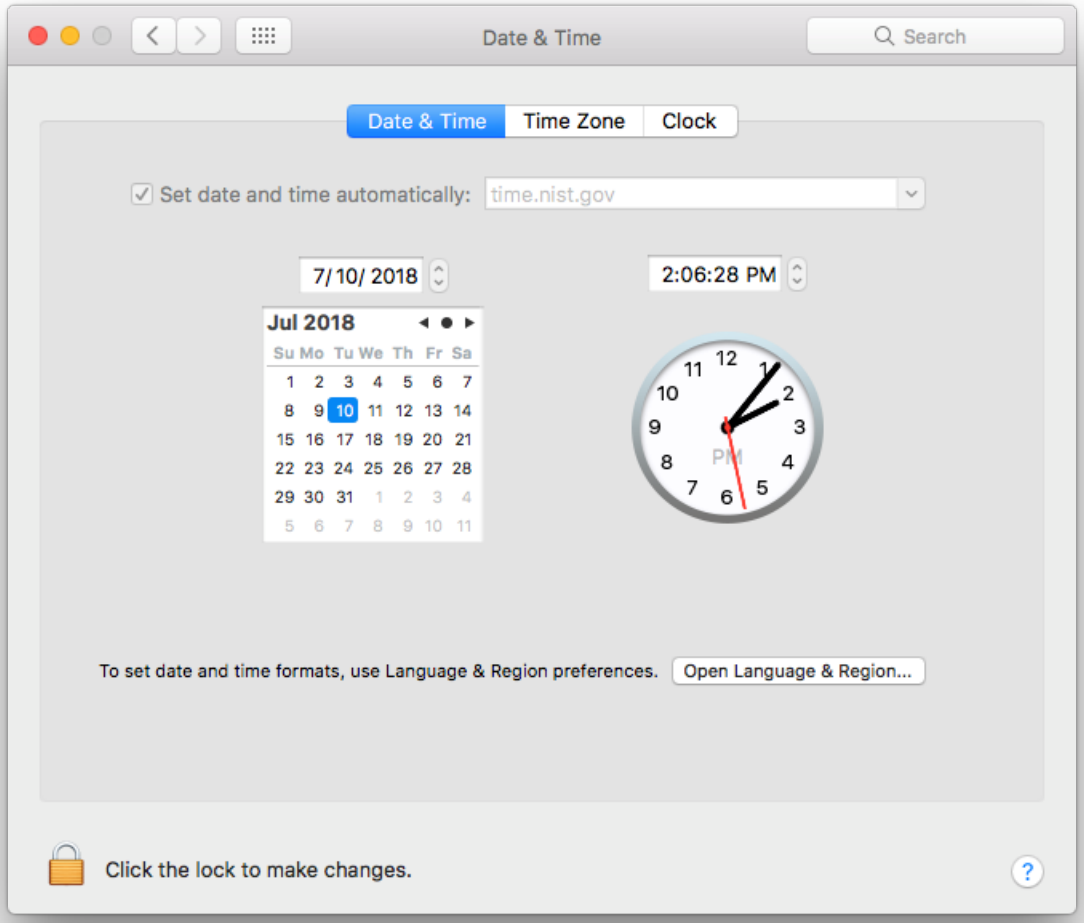


Figure 8: Setting the NTP Servers

To set a time server and to enable automatic updating of time, use the commands in Appendix J.11.

6.4.3 System Crash and Kernel Panic Reporting

Crash and kernel panic reports should be monitored to prevent potentially sensitive data from being written to unencrypted files. These reports are meant to provide diagnostic information regarding system crashes and panics. The reports are located in `/Library/Logs/DiagnosticReports`. If an organization does not plan to use the files for diagnostic purposes, the files should be manually deleted periodically to conserve disk space and limit the possibility of exposing sensitive information. Testing did not reveal a way to disable report generation.

6.5 Software Restriction

macOS offers multiple ways of restricting the execution of software; see Section 3.1 for additional information. This section briefly looks at two methods of limiting software execution: Gatekeeper and Parental Controls. Gatekeeper restricts the applications that may be installed onto a system, while Parental Controls restricts the applications already installed on a system that may be run by a user.

6.5.1 Gatekeeper

It is recommended to configure Gatekeeper to "App Store" for all systems. Gatekeeper's configuration options are not marked as pertaining to Gatekeeper, but rather are all bundled into the **System Preferences / Security & Privacy / General**. This pane has two options related to "Allow applications downloaded from", as described in Section 3.1. By default, the option to limit downloads to "App Store and identified developers" is enabled. To use the strictest Gatekeeper controls, select the "App Store" option. These options are shown in Figure 9 below. Some Gatekeeper settings can be configured using the commands found in Appendix J.17.

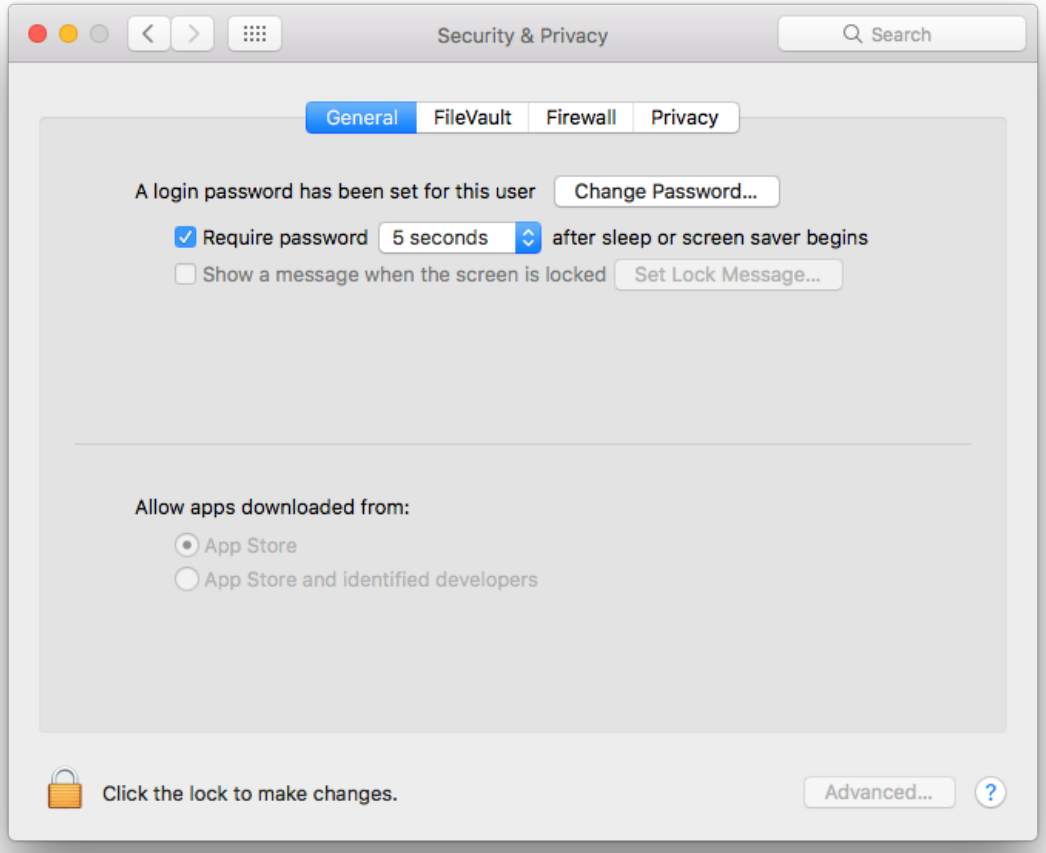


Figure 9: Gatekeeper Options

6.5.2 Parental Controls

Parental Controls can be used to specify which installed applications may be executed through the "Limit Applications" option in the **System Preferences / Parental Controls** window. If the Limit Applications option is enabled, a user will be unable to run an application unless an administrator has added it to the list of permitted applications for that user. The administrator can also configure each user account so that it can or cannot use apps from the App Store, either altogether or based on age ratings.

6.6 Network Services

This section discusses security issues related to network services. The information is organized into the following categories: firewalls, sharing, IPv6, the SSH daemon, wireless networking, Bonjour, and network daemons. For network service configuration commands, see Appendix J.11.

6.6.1 Firewalls

Both built-in firewalls, the application firewall and the stateful inspection firewall, are disabled by default. To enable the application firewall, go to **System Preferences / Security & Privacy / Firewall**. Click the "Turn On Firewall" button. There are five additional options under the "Firewall Options..." button:

- **Block all incoming connections**. NIST recommends that this option is enabled for SSLF systems. This blocks all incoming traffic except for a few protocols, such as DHCP, that may be needed for basic system services to function. This setting provides a high level of network security while possibly negatively impacting functionality. Before using this setting in a production environment, perform testing to determine how this setting affects all major applications on the system.

- **Enable selected applications**. Once the user has authenticated as an administrator (by clicking the lock and providing the username and password), specific applications can be authorized to accept incoming connections (subject to being allowed by the pf firewall described below).

- **Automatically allow built-in software to receive incoming connections.** NIST recommends that this option is enabled for Standalone and Managed systems. These options are only available if "Block all incoming connections" is disabled.

- **Automatically allow downloaded signed software to receive incoming connections**. NIST recommends that this option be disabled. Note that, even with this option disabled, downloaded and signed software can still receive incoming connections via a user prompt which authorizes them on an app-specific basis. Therefore, disabling this option provides notice to users and some protection but at the cost of some user effort.

- **Enable stealth mode**. This option is only available if "Block all incoming connections" is disabled. This option prevents the system from responding to pings, traceroutes, and other similar diagnostic tools.

1965 Enabling the stateful inspection firewall (`pf`; see the `pfctl man` page) is ineffective unless its
1966 ruleset has been configured, because by default, the `pf` ruleset does not block any network traffic.
1967 A detailed explanation of how to configure a `pf` ruleset is outside the scope of this publication.
1968 Table 2 presents a recommended `pf` ruleset. This ruleset should be altered depending on an
1969 organization's networking service needs.

1970 **Table 2: `pf` Firewall Services and Ports**

Service Name	TCP Port(s)	UDP Port(s)	Direction
FTP	20, 21	20, 21	Incoming
SSH	22	22	Incoming
telnet	23	23	Incoming
TFTP	69	69	Both
finger	79		Both
HTTP	80	80	Incoming
NFS	2049		Both
Remote Apple Events	3031		Incoming
SMB	139, 445	137, 138	Both
Apple File Server	548		Incoming
UUCP	540		Both
Screen Sharing	5900		Incoming
ICMP	N/A	N/A	Incoming
SMTP	25		Incoming
POP3	110		Incoming
POP3S	995		Incoming
IMAP	143		Incoming
IMAPS	993		Incoming
Printer Sharing	631		Incoming
Bonjour		1900	Both
mDNSResponder		5353	Both
iTunes Sharing	3689		Both
Optical Drive Sharing	49152		Both

1971

1972 The various application firewall settings can be changed via the command line with the
1973 commands given in Appendix J.7.

1974 ### 6.6.2 Sharing

1975 Sharing settings can be accessed via **System Preferences / Sharing**. By default, all sharing is
1976 disabled. There are several different types of sharing, as shown in Figure 10, including screen,
1977 file[34], printer, Internet, and Bluetooth. Other systems may have slightly different lists of sharing,
1978 based on their hardware characteristics (for example, systems with optical drives will have a
1979 "DVD or CD Sharing" option). For all the sharing services, there may be names or directories
1980 listed; however, this does not imply that the service is enabled. Note that this list includes three
1981 options for remote access to an macOS system:

1982 • **Remote Login**. The Remote Login feature allows Secure Shell (SSH) and Secure FTP
1983 (SFTP) connections to be made to the macOS system from other systems. By default,
1984 SSH and SFTP are disabled, and organizations should not enable them unless they are
1985 needed for system maintenance, access, etc. because they are additional attack vectors
1986 into a system.

1987 • **Remote Management and Screen Sharing**. Remote Management and Screen Sharing
1988 both allow remote operation of a computer. These services would be required for a
1989 technical support person to remotely see a macOS system's screen from another system.
1990 Since both settings allow external control of a system, they should be disabled unless
1991 needed.

1992 • **Remote Apple Events** (logging of events from other macOS systems on this system).
1993 This feature is intended to be used when a system is acting as a server, not a desktop or
1994 laptop. In most cases, it should be disabled.

[34] File sharing includes options for sharing files and folders using the Apple Filing Protocol (AFP), File Transfer Protocol (FTP), or Server Message Block (SMB) protocol.

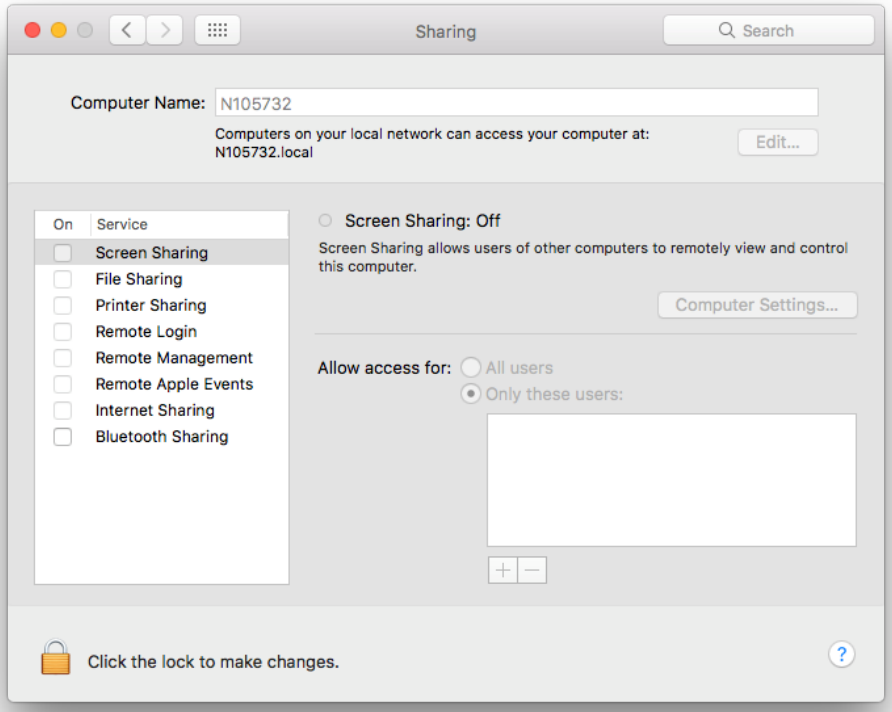


Figure 10: Sharing Options

To reduce the number of attack vectors against a system, all sharing and remote access services should be disabled unless explicitly needed. To enable a needed service, go to **System Preferences / Sharing**, and turn on the appropriate service. Computer names are used for networking purposes and are helpful for users to differentiate between machines. Computer names should not have content that identifies any of its users. To configure computer name settings, see Appendix J.11.

Sharing will only work if the firewall or firewalls are configured to permit it. For example, the built-in application firewall has an option called “Block all incoming connections”. If enabled, this will disable all sharing. To alter the setting for this option, go to **System Preferences / Security & Privacy / Firewall**. Click the “Firewall Options…” button and change the setting as appropriate for the “Block all incoming connections” option.

macOS has individual configuration settings for sharing each local printer. If a system has local printers, these printers should not be shared remotely unless they need to provide printing services to other systems. To disable sharing for a printer, choose **System Preferences / Printers & Scanners**, and for each local printer, deselect the “Share this printer on the network” option. Note that when the “Share this printer on the network” option is enabled; this also enables the Printer Sharing option in **System Preferences / Sharing**.

There is another form of macOS sharing that is not included in the Figure 10 menu: AirDrop. AirDrop is a peer-to-peer file sharing service. AirDrop is only available on certain Apple hardware that supports it, and it requires the use of Wi-Fi. Some Apple devices additionally use Bluetooth to initiate the AirDrop transfer.[35] AirDrop is only enabled when the user specifically has it open (**Finder / Go / Airdrop**). When open, AirDrop automatically scans for other AirDrop-enabled systems within Wi-Fi range. However, files are not transferred unless a user specifically authorizes the transfer.

NIST recommends that if any sharing services are enabled, they should be protected by another layer (such as a host-based firewall) that restricts access to the service. Allowing global access to any form of sharing is not recommended.

To disable sharing services via the command line, use the commands provided in Appendix J.8.

6.6.3 IPv6

If IPv6 is not needed, it should be disabled. To disable IPv6, perform the following steps:

1. In a Terminal window, enter `networksetup -setv6off Wi-Fi` (or other network name, if desired).
2. Provide admin credentials, if prompted.
3. Go to **System Preferences** / **Network**.
4. Select Wi-Fi (or the other network name chosen in step 1).
5. Press the "Advanced" button.
6. Select the "TCP/IP" tab.
7. Ensure the "Configure IPv6" drop-down menu is set to "Off".

6.6.4 SSH Daemon

NIST recommends that the Secure Shell (SSH) daemon (`sshd`) be disabled in all environments unless specifically needed. The NIST baselines contain several settings to make `sshd` more secure; these settings should be applied whether or not `sshd` is enabled just in case it becomes enabled inadvertently or is needed in the future.

The table in Appendix J.9 lists some of the possible settings that can be configured for the SSH daemon in order to mitigate significant vulnerabilities that can emerge; this is not, however, a comprehensive list of all changes that could be made to SSH. The settings exist in the

[35] See the section on AirDrop security in https://www.apple.com/business/site/docs/iOS_Security_Guide.pdf.

`/etc/ssh/sshd_config` file as key-value pairs in the format of "key value." For additional information on SSH security, see [NISTIR 7966].

6.6.5 Wireless Networking

Any wireless networking services (e.g., Wi-Fi, Bluetooth) that are not needed should be disabled. See Section 6.1.2 for more information on disabling hardware interfaces. For wireless networking services that are enabled, NIST recommends reviewing their configuration options and locking them down to the greatest extent possible. These services should also have their menu bar icons displayed so that users are aware of the operating states. Additional recommendations for these services can be found in Appendix J.10.

The **System Preferences** menu presents the following Bluetooth settings:

- "Turn Bluetooth On/Off,"
- "Allow Bluetooth devices to wake this computer,"
- "Open Bluetooth Setup Assistant at startup if no mouse or trackpad is detected,"
- "Open Bluetooth Setup Assistant at startup if no keyboard is detected,"
- "Show Bluetooth in menu bar," and
- "Bluetooth Sharing" (i.e., Bluetooth file sharing).

For example, the Bluetooth option "Allow Bluetooth devices to wake this computer" is beneficial if the system is using Bluetooth input devices (keyboard, mouse), but otherwise poses risk without providing benefit. The Bluetooth discoverability setting is not manually configured through the **System Preferences** or the command line. The setting automatically toggles to "on" and the computer becomes visible to other Bluetooth devices when the **System Preferences / Bluetooth** pane is opened.

Wireless settings can also be configured, and these settings include: preferred networks, toggled state on menu bar, and AirDrop. One setting that can be configured through the **System Preferences** is "Require administrator authorization to: Create computer-to-computer networks". Such an option should be enabled unless users specifically require this privilege and do not have administrator-level access. This setting is located under **System Preferences / Network**.

For additional information on wireless networking security, see *Guidelines for Securing Wireless Local Area Networks (WLANs)* [SP 800-153] and *Guide to Bluetooth Security* [SP 800-121r2].

6.6.6 Bonjour

Bonjour multicast advertisements should be disabled in all environments except Standalone. Bonjour advertises the system's capabilities, which opens it to attack. It allows other systems running Bonjour to detect a system and any services that it provides. By disabling Bonjour

multicast advertisements, only the service announcements are being disabled and not the services themselves. For information on disabling Bonjour advertisements, go to Appendix J.11.

6.6.7 DNS Servers

NIST recommends that systems be configured to use at least two DNS servers. This provides redundancy in the event of a failure. A failure in name resolution could lead to the failure of security functions requiring name resolution, which may include time synchronization, centralized authentication, and remote system logging. Command line configuration for DNS servers is available in Appendix J.11.

6.6.8 Network Daemons

Disabling network services reduces potential attack vectors into a system. If a service is unused it should be disabled. It is possible to disable Bluetooth, Wi-Fi, NFS, and Apple File Server at the daemon level. See Appendix J.16 for daemon disabling commands.

6.7 Applications

This section provides basic information on securing commonly used built-in macOS applications, namely Mail, Safari, and Terminal.

6.7.1 Mail

Email has become a popular means for malware propagation. The careful configuration of email clients is important not only to protect a given system, but also to prevent the propagation of malware from the system to other systems.

Examples of security-related settings for the built-in Mail client are listed below. Note that the validity of these settings will vary from organization to organization, depending on the email server infrastructure and the security needs versus the functionality needs.

- Under **Mail / Preferences / Accounts / Server Settings**, uncheck the checkbox for "Automatically manage connection settings for both incoming and outgoing servers. Then make sure the "Use TLS/SSL" option is enabled in both places.

- Under **Mail / Preferences / Junk Mail**, enable the "Enable junk mail filtering" option. There are other options available that support junk mail filtering, such as defining what actions should be performed when junk mail is received and determining which categories of messages should not be flagged as being junk mail (e.g., from certain senders).

- Under **Mail / Preferences / Viewing**, there are security-related options including "Use Smart Addresses", which if disabled will show email addresses instead of names. Additionally, there is the "Load remote content in messages" option, which if disabled will prevent possibly objectionable or malicious images from being displayed.

6.7.2 Safari

Web browsing is a common way for malware to infect systems and otherwise take advantage of systems. It is important to configure web browsers with security in mind, particularly in higher-security environments (e.g., SSLF), otherwise the web browser may provide an easy way for malware to infiltrate a system.

Examples of security-related settings for the built-in Safari web browser are listed below. Note that the validity of these settings will vary from organization to organization depending on security needs versus functionality needs.

- Under **Safari / Preferences / General**, there is an option titled "Open "safe" files after downloading", which is enabled by default. The intention of this option is to allow automatic opening of file types that are unlikely to include malicious content; however, the list of file formats includes PDFs, which have been known to contain malicious content. This option should be disabled unless all downloads are being inspected by antimalware software.

- Under **Safari / Preferences / AutoFill**, some of the options are for autofilling "User names and passwords" and "Credit cards". AutoFill should be disabled for all options.

- Under **Safari / Preferences / Security**, there are several security-related options under this pane, including the following:

  - "Warn when visiting a fraudulent website" will do as the name implies, so it should typically be enabled.

  - The option to "Block pop-up windows" should generally be enabled because of the frequency with which pop-up windows have been used to transmit malicious content. In some cases, however, a mission-critical web application will use popup windows; in this case, pop-up windows should be temporarily allowed only while the critical web application is being used.

  - There are options to "Allow Plug-ins" and "Enable JavaScript". Under the **Plug-in Settings** menu, there is a checkbox to enable Java. Organizations should consider disabling some or all of these options for high-security needs (e.g., systems in SSLF environments). NIST recommends disabling the Java plugin for all environments.

- Under **Safari / Preferences / Privacy**, there are several privacy-related options, as shown in Figure 11. Cookies are stored on a system from visiting websites and can be used to track user browsing behavior. Websites may require cookies in order to function properly, so organizations should weigh the benefits of added functionality against the risks to privacy that cookies embody. In order to mitigate these privacy risks, organizations can periodically delete cookies, but this may temporarily reduce functionality.

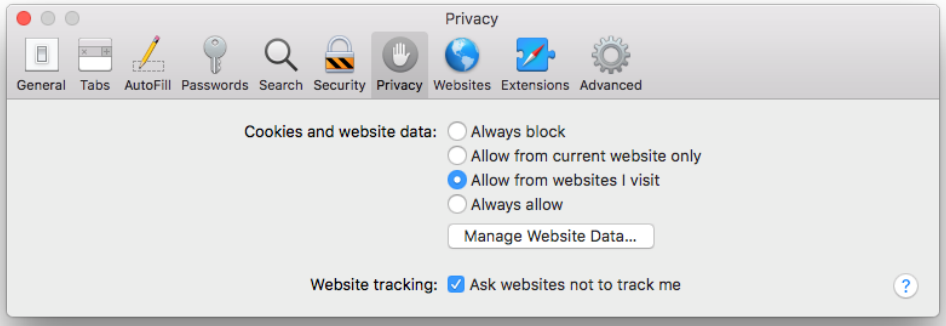


Figure 11: Privacy Options

- Under **Safari / Preferences / Websites**, there is a list of capabilities accessible by websites. Access to these features, such as camera, microphone or location data, can be controlled on a per-website basis.

Safari can be configured to show its status bar, and the command-line option is located in Appendix J.17. This is useful for confirming the underlying web address for a hyperlink.

6.7.3 Configuring Software Updates

Many software update settings can be configured using a command prompt. Available system updates can be displayed and applied using the `softwareupdate` tool in a similar manner to the App Store GUI. An example of using the `softwareupdate` tool is provided in Appendix J.17.

6.7.4 Terminal

The Terminal application has a configuration item labeled “Secure Keyboard Entry” available in the Terminal top menu bar. This prevents other applications from intercepting and modifying keyboard input. It is recommended to enable this setting. The configuration command is available in Appendix J.17.

6.8 Other Security Management Options

This section discusses security management options not covered in the other parts of Section 6, such as configuring CD and DVD preferences, login banners, privacy settings, and virtualization.

6.8.1 CD and DVD Preferences

There can be security risks in automatically performing actions when a CD or DVD is placed into an macOS system. CDs or DVDs could contain malicious content that could be automatically opened and exploit a vulnerability in the default application on the system. Automatic actions can be disabled through **System Preferences / CDs & DVDs** by choosing the “Ignore” option for each type of media. Note that the settings are not visible if there is no optical

drive, but will appear if a supported external drive is attached. These settings can also be configured through the command line using the commands described in Appendix J.12.

6.8.2 Login Banners

Login banners are often used to warn people of the permitted actions and possible legal consequences of misuse of a system. There are two ways to set up login banners for macOS:

- Set the text for the login window access warning. This option is best suited for short login banners (three lines or less).[36]
- Create a policy banner file that contains the text of the banner. The file must be located at `/Library/Security`, and it must be named `PolicyBanner` with a file extension of `.txt`, `.rtf`, or `.rtfd`.[37]

Depending on organizational rules, there may be a need to set up a warning banner for command line access (both remote and local).[38]

6.8.3 Privacy

General privacy settings are available through **System Preferences / Security & Privacy / Privacy**. These settings are divided into three categories:

- **Location Services**. The "Enable Location Services" option will enable or disable the use of location services. To preserve privacy, disabling location services is recommended unless there is a specific reason to have them enabled. If location services are enabled, only the necessary applications should have access to location information. This can be configured through the same menu.
- **Contacts**. This setting is comprised of a list of applications that have requested access to the Contacts information. Contacts access can be revoked by unchecking the permission box for a specific application. Only the necessary applications should have access to contact information in order to protect it from unintended disclosure.
- **Diagnostics & Usage**. This category holds two configuration settings: "Send diagnostic & usage data to Apple" and "Share crash data with app developers". According to the descriptions presented to the user, all data is anonymized before being sent to Apple and the app developers. The NIST baselines disable these settings. These settings require administrator-level credentials to enable.

---

[36] See http://help.apple.com/securityguide/mac/10.7/#apdC3C3745F-3036-4531-9697-D24F6FB5EC3C for instructions on implementing this option.

[37] http://help.apple.com/securityguide/mac/10.7/#apd07CB9812-3682-4522-9F9D-147774DF4733

[38] For instructions on setting up such a banner, see http://help.apple.com/securityguide/mac/10.7/#apdA5B369D5-9A06-421D-8DB2-B086BA657BDA.

Privacy settings can be configured through the command line as described in Appendix J.13.

6.8.4 Virtualization

A macOS system can be run as a virtual machine instance (a guest operating system) on an Apple host system.[39] This can provide additional isolation for activities occurring within the virtual macOS system. For more information on the use of full virtualization, see [SP 800-125].

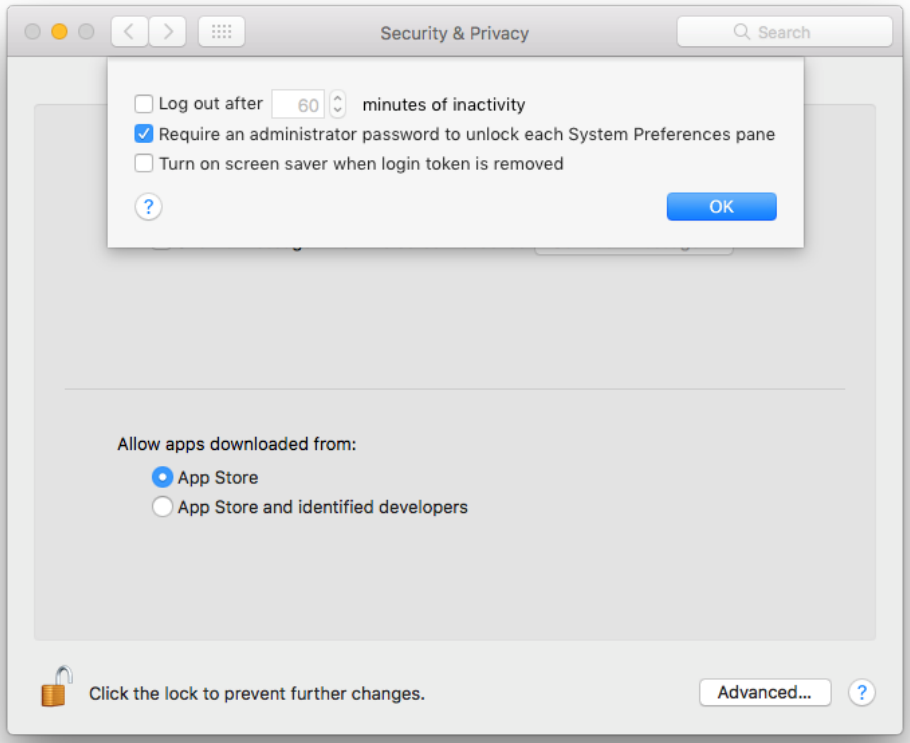
6.8.5 Other System Preferences

This section discusses additional settings, including administrator access for preferences, dock auto-hide, Dashboard and Siri.

6.8.5.1 Administrator Access for Preferences

Not all system preferences require an administrator password to be changed. In particular, all systemwide settings should require administrator authentication. This setting is found in the **System Preferences / Security & Privacy** pane, after clicking the "Advanced…" button at the bottom of the window. This is shown in Figure 12 below. The configuration commands are available in Appendix J.17.

[39] For limitations, see macOS 10.12 EULA Section 2B(iii) http://images.apple.com/legal/sla/docs/macOS1012.pdf.



2214

2215 **Figure 12: Administrator Access for System-wide Preferences**

2216 #### 6.8.5.2 Dock

2217 To change Dock preferences, go to **System Preferences / Dock**. NIST recommends that the
2218 Dock auto-hide setting be enabled for SSLF systems. The terminal command to configure Dock
2219 auto-hide is available in Appendix J.17.

2220 #### 6.8.5.3 Dashboard

2221 The Dashboard is disabled by default on macOS 10.12. Updates to Dashboard widgets may pose
2222 a security risk, so NIST recommends that the Dashboard remains disabled for SSLF systems.
2223 However, enabling it does not require administrator permission. The terminal commands for the
2224 Dashboard are available in Appendix J.17.

2225 #### 6.8.5.4 Siri

2226 Siri is a new feature in macOS 10.12. It allows for spoken commands to perform actions on the
2227 system, such as opening programs and performing searches. However, Siri collects voice, contact
2228 and location information and sends it to Apple. Therefore, NIST recommends that Siri be
2229 disabled using the command in Appendix J.13.

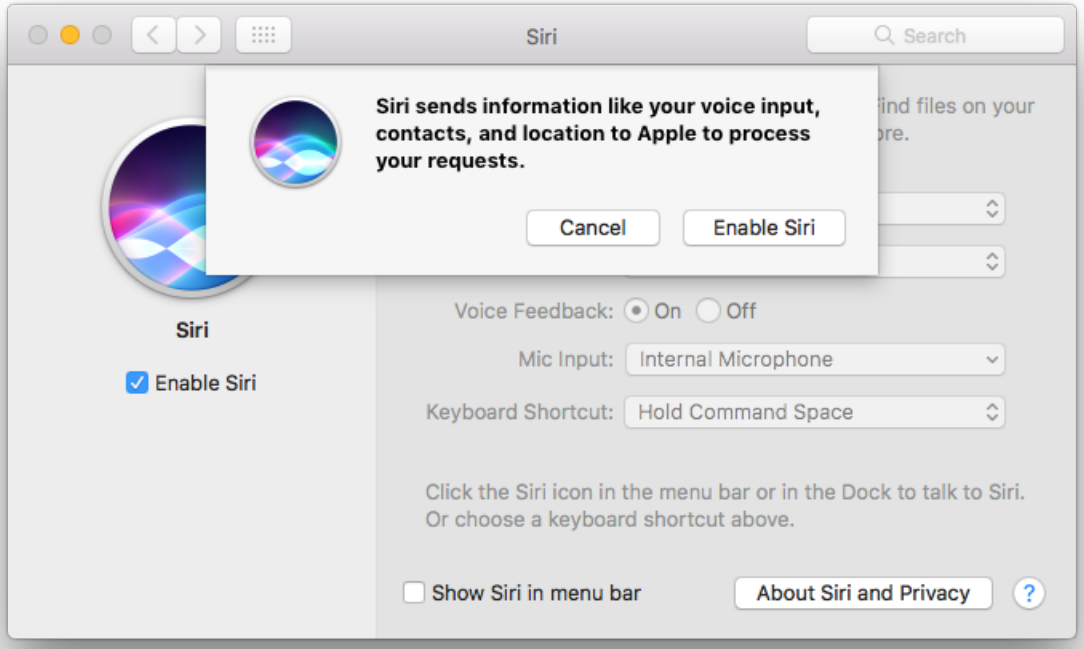


Figure 13: Siri Privacy Message

6.9 Summary of Recommendations

- Each hardware interface creates a potential point of attack, so an organization may determine that one or more of these interfaces are unnecessary and therefore should be disabled. However, the available method of disabling hardware interfaces is not foolproof, so on such hosts the disabled interfaces should be continuously monitored to detect any restoration. SIP complicates this issue by preventing removal of `kext` files.
- SIP should remain enabled to protect system files from modification.
- Use EFI passwords, but understand that they can only be relied on to provide security if the physical security of the system is assured.
- Use FileVault full disk encryption on system drives, and use Disk Utility to encrypt disk images on removable media.
- Make sure to properly sanitize storage media before disposal.
- Only use administrator accounts for system administration tasks. Each user should utilize a unique standard or managed account for daily use of macOS systems.

- Administrators should periodically review user accounts and disable those that have been inactive for 90 days, as well as disabling temporary accounts after 30 days. Organizations should follow procedures to disable accounts as soon as they are no longer needed. Disabled accounts should be deleted after a specific period of time to release resources and prevent unneeded accounts from accidentally being re-enabled.
- Disable the guest user account.
- The root account should be disabled on all macOS systems, and a separate administrator account should be established for each person who will be performing regular administrative tasks.
- Configure the login screen to hide account names.
- NIST recommends keeping the "Automatic login" option disabled.
- Implement and enforce a strong password policy in accordance with the organizational policy.[40] Password hints should be disabled.
- Use an authentication-enabled screen saver on all macOS systems. A screensaver should activate after no more than 20 minutes. A hot corner should be configured to activate the screen saver without any modifier keys.
- Carefully consider usability issues before setting macOS account policies.
- Make sure Gatekeeper is enabled to prevent installation of software from unknown sources.
- Configure and monitor logs for undesired system activity.
- Configure macOS systems to synchronize their clocks on a regular basis with accurate time sources.
- Configure firewalls to block undesired traffic.
- If IPv6 is not needed, disable it to reduce the possible attack vectors into the system.
- Disable Spotlight Suggestions to prevent local search queries from being sent to third parties.
- Disable any unneeded sharing and network services. Protect active sharing services with restrictive access measures, such as a host-based firewall.

[40] See Appendix B Table 9 control IA-5: Authenticator management for guidance on implementing and enforcing a strong password policy.

- SSH should be disabled unless required.
- Disable network interfaces such as Wi-Fi and Bluetooth if they are not used.
- Bonjour multicast advertisements should be disabled in Managed and SSLF environments.
- Configure CD & DVD preferences to disable auto-launching programs when a disk is inserted.
- Create a login banner in accordance with the organizational policy.
- System-wide settings should require administrator authentication.
- Disable Siri.

7. Putting It All Together

This publication covers many topics related to the security of macOS 10.12 systems. The purpose of this section is to put it all together by describing the basic process that IT professionals should follow to use this publication and the accompanying baselines. The primary steps are as follows:

1. Read the entire publication, including the appendices. As needed, review the additional reference material listed throughout the publication and in Appendix D.

2. As discussed in Section 4, install and patch the OS and applications on test systems. Ensure that there is a plan for system backups and restores, and be sure to test that they work as intended.

3. Refer to Section 2 to review the system threats, then select the appropriate operating environment. Review the security baseline and the settings spreadsheet columns corresponding to that environment. Refer to Section 6 as needed for more information on the different regions and values within the baseline.

4. Modify the baseline to reflect local policy and apply it to test systems using the appropriate deployment tool, as described in Section 5. Create multiple versions of the baseline if necessary to address multiple system roles or environments. Refer to Appendix C and Appendix D for other tools that may be useful for deployment.

5. Augment the baseline with additional controls presented in Section 6, as well as any others that are required, based on the local environment. Apply application-specific security configuration changes.

6. Verify that the controls have been deployed properly by testing system functions and security controls, as described in Sections 2.6 and 5.3. Modify and document any changes made to the baseline security controls (e.g., altering a setting so a particular application can function properly). Modify the baselines as necessary to incorporate changes that apply to all systems.

7. Perform another round of testing in a test environment before deploying the baselines and other changes to production systems.

8. Deploy the baselines and additional controls to production systems. Verify that the controls have been deployed properly by testing system functions and security controls.

9. Maintain the systems, as described in Section 2.7 This includes keeping systems updated (Section 4.3), monitoring the system's primary security controls (Section 5.3), performing periodic or continuous vulnerability assessments (Section 5.3), and monitoring the various logs described throughout the publication.

Appendix A. NIST Security Configurations

Appendix A briefly discusses the NIST security baselines and settings spreadsheet.

NIST produced a list of settings that are important for ensuring the security of a macOS system. These settings correspond to three different environments—Standalone, Managed, and SSLF. All of these settings are documented in a spreadsheet with the following columns:

- **Category**. The category of the setting as seen in Figure 14. The script and the spreadsheet use this to group like settings together.
- **Setting Name**. Combines with the CCE ID to produce the function name in the script.
- **Description**. A user-friendly explanation of the setting.
- **CCE IDv5**. The unique Common Configuration Enumeration (CCE) ID value assigned to each setting.
- **Security Baseline**. The human-readable setting value for each environment profile.
- **Technical Mechanism**. The in-depth explanation of how to apply the setting.
- **Read Setting State**. A command-line statement used to read the current state of the setting.
- **Write Setting State**. A command-line statement used to write the new value for the setting.
- **Standalone, Managed, and SSLF (Environment-Specific Value)**. Specifies the setting baseline value for Standalone, Managed, and SSLF.
- **STIG ID**. The unique ID of the related setting in the 10.12 DISA STIG (Defense Information Systems Agency Security Technical Implementation Guide).[41]
- **Rationale**. Security considerations that this setting addresses.
- **Reference**. Any references providing more information for the setting.

The spreadsheet and other associated materials can be found on the GitHub page listed in Appendix D. The NIST security baselines include many recommendations that are considered secure by default. These settings are omitted from this document, but are included in a separate tab of the settings spreadsheet.

[41] https://iase.disa.mil/stigs/os/mac/Pages/index.aspx

Figure 14 gives an illustrative overview of the setting categories covered by this guide. The number of settings for a category does not imply increased importance of one category over another.

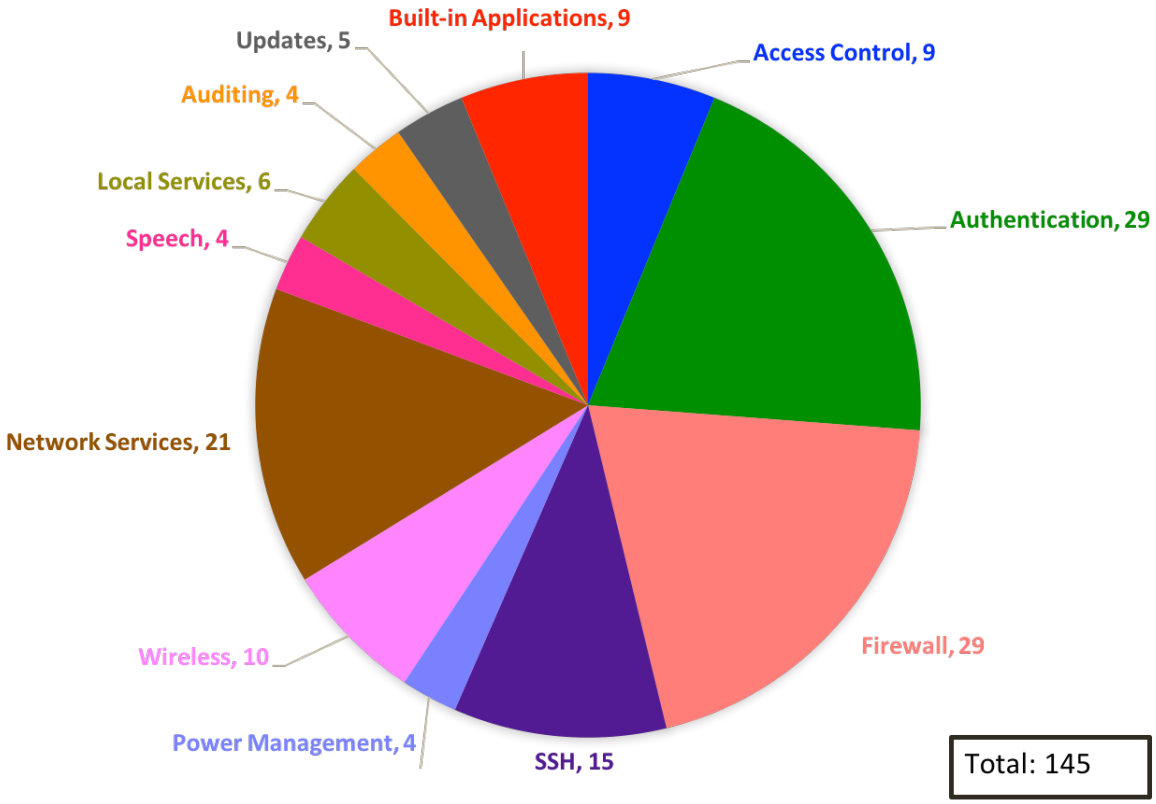


Figure 14: Distribution of Security Controls

Appendix B. Mapping macOS Controls to NIST SP 800-53 Rev 4

Appendix B maps many of the security controls and baseline settings referenced throughout this document to their corresponding controls in NIST Special Publication (SP) 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. The list of controls and mappings is not intended to be fully comprehensive or authoritative, and it omits SP 800-53 controls that are not directly related to individual macOS 10.12 systems. Note that a mapping does not imply full satisfaction of a given security control's requirements. If an organization were to follow the guidance in Sections 6.3.1 and 6.3.2.4, additional steps might still be required to fully satisfy control AC-2 requirements. The mappings are listed according to the control family categories established in SP 800-53. Each category has a separate table, with three columns containing the following information for each mapping:

- Number and name of the control from SP 800-53.
- The sections of this publication that map to the SP 800-53 control, and a brief description of the content within those sections that corresponds to the SP 800-53 control.
- The settings within this publication and their corresponding spreadsheet entries that map to the SP 800-53 control, if any.

The tables include the requirements and control enhancements that apply to low, moderate, and high impact systems. (Section 2.2 contains definitions for the impact categories.) After determining the impact level of a system, administrators can select the SP 800-53 controls that correspond to that impact level, and then identify the sections of this document and baseline settings that match those SP 800-53 controls. This would provide a starting point for identifying all of the security controls needed to secure the system.

Table 3: Access Control (AC) Family Controls

SP 800-53 Control Number and Name	Corresponding Sections in This Publication	Corresponding NIST Baseline Settings
AC-2: Account management	• Section 6.3.1 (Disabling unneeded accounts) • Section 6.3.2.4 (Disabling Fast User Switching)	CCE_79418_0_fast_user_switching

SP 800-53 Control Number and Name	Corresponding Sections in This Publication	Corresponding NIST Baseline Settings
AC-3: Access enforcement	• Section 3.1 (System Integrity Protection)	CCE_79405_7_check_system_integrity_protection_status
	• Section 6.2.5 (Setting file and folder permissions)	CCE_79404_0_all_files_in_a_users_home_dir_are_owned_by_that_user CCE_79407_3_files_in_home_dir_group_owned_by_owners_group CCE_79409_9_user_home_directories_permissions
	• Section 6.2.6 (Setting Spotlight permissions)	CCE_79435_4_disable_lookup_suggestions
	• Section 6.3.1 (Having separate accounts for use and administration)	N/A
	• Section 6.3.6 (Storing credentials securely)	N/A
	• Section 6.6.2 (Restricting use of shares and remote access tools)	CCE_79500_5_ssh_restrict_users CCE_79488_3_restrict_screen_sharing_to_specified_users CCE_79546_8_bluetooth_disable_file_sharing CCE_79529_4_disable_remote_management
	• Appendix I.2 (Permissions and Ownership)	CCE_79408_1_set_umask
AC-4: Information flow enforcement	• Section 2.3.2.1 (Using a firewall to limit network access to a host) • Section 3.6 (Using a host-based firewall to restrict network traffic) • Section 4.2 (Disabling iCloud) • Section 6.1.2 (Disabling unneeded hardware components, including network interfaces) • Section 6.2.6 (Spotlight settings)	CCE_79522_9_enable_firewall_logging CCE_79445_3_enable_firewall_logging_detail_level CCE_79443_8_allow_signed_downloaded_sw_receive_connections CCE_79444_6_allow_signed_sw_receive_connections CCE_79470_1_turn_on_firewall See Table 20 for pf rules CCE_79528_6_disable_remote_login CCE_79404_0_disable_bonjour_advertising

SP 800-53 Control Number and Name	Corresponding Sections in This Publication	Corresponding NIST Baseline Settings
	• Section 6.6.1 (Using a host-based firewall to restrict network traffic) • Section 6.6.2 (Disabling sharing) • Section 6.6.3 (Disabling IPv6) • Section 6.6.4 (Disabling sshd) • Section 6.6.5 (Disabling wireless networking) • Section 6.6.6 (Disabling Bonjour multicast advertisements) • Section 6.8.5.4 (Disabling Siri)	CCE_79476_8_disable_location_services CCE_79538_5_ssh_disable_x11_forwarding CCE_79507_0_disable_airdrop CCE_79508_8_disable_infrared_receiver CCE_79435_4_disable_lookup_suggestions CCE_79437_0_disable_siri
AC-6: Least privilege	• Section 2.2 (Assigning user rights based on least privilege) • Section 6.3.1 (Assigning user rights based on least privilege)	CCE_79443_8_allow_signed_downloaded_sw_receive_connections CCE_79444_6_allow_signed_sw_receive_connections
AC-7: Unsuccessful logon attempts	• Section 6.3.4 (Locking out accounts after too many failed login attempts)	CCE_79423_0_password_failed_login_lockout_policy
AC-8: System use notification	• Section 2.3.1.2 (Presenting a warning banner when a user attempts to log on) • Section 2.3.2.1 (Presenting a warning banner when a user attempts to log on) • Section 6.8.2 (Presenting a warning banner when a user attempts to log on)	CCE_79414_9_add_cli_login_banner CCE_79415_6_add_login_banner
AC-11: Session lock	• Section 2.3.1.2 (Using a password-protected screen saver) • Section 6.3.5 (Using a password-protected screen saver, manually locking user sessions)	CCE_79430_5_screensaver_grace_period CCE_79519_5_require_password_after_screensaver CCE_79431_3_start_screen_saver_hot_corner CCE_79517_9_no_modifier_keys_for_screen_saver_start CCE_79518_7_no_prevent_screensaver_corner CCE_79417_2_desktop_idle_time

SP 800-53 Control Number and Name	Corresponding Sections in This Publication	Corresponding NIST Baseline Settings
AC-17: Remote access	• Section 2.3.2.1 (Using industry-standard strong protocols for remote access)	CCE_79498_2_ssh_remove_non_fips_140_2_ciphers CCE_79499_0_ssh_remove_non_fips_140_2_macs CCE_79541_9_ssh_use_protocol_version_2 CCE_79433_9_use_network_time_protocol
	• Section 6.6.2 (Disabling built-in remote access services that are not needed)	CCE_79526_0_disable_remote_apple_events CCE_79528_6_disable_remote_login CCE_79529_4_disable_remote_management
AC-18: Wireless access	• Section 6.1.2 (Disabling hardware components) • Section 6.6.2 (Disabling Bluetooth file sharing) • Section 6.6.5 (Not connecting to any wireless network automatically, using wireless security features)	CCE_79547_6_remove_all_preferred_wireless_networks CCE_79503_9_bluetooth_disable_wake_computer CCE_79506_2_bluetooth_turn_off_bluetooth CCE_79546_8_bluetooth_disable_file_sharing CCE_79509_6_show_bluetooth_status_in_menu_bar CCE_79507_0_disable_airdrop CCE_79508_8_disable_infrared_receiver
AC-20: Use of external information systems	• Section 4.2 (iCloud settings) • Section 6.2.6 (Spotlight settings) • Section 6.8.5.4 (Disabling Siri)	CCE_79435_4_disable_lookup_suggestions CCE_79437_0_disable_siri

2370

2371 **Table 4: Awareness and Training (AT) Family Controls**

SP 800-53 Control Number and Name	Corresponding Sections in This Publication	Corresponding NIST Baseline Settings
AT-2: Security awareness training	• Section 2.3.2.3 (Educating users on avoiding malware infections) • Section 2.5 (Having security awareness and training for end users and administrators)	N/A
AT-3: Role-based security training	• Section 2.5 (Having security awareness and training for end users and administrators)	N/A

2372

2373 **Table 5: Audit and Accountability (AU) Family Controls**

SP 800-53 Control Number and Name	Corresponding Sections in This Publication	Corresponding NIST Baseline Settings
AU-2: Audit events	• Section 6.4 (Configuring system auditing)	CCE_79413_1_set_audit_control_flags
AU-4: Audit storage capacity	• Section 6.4.1 (Enabling logging and specifying log retention time)	CCE_79522_9_enable_firewall_logging CCE_79445_3_enable_firewall_logging_detail_level CCE_79411_5_audit_log_retention CCE_79410_7_audit_log_max_file_size
AU-6: Audit review, analysis, and reporting	• Section 2.7 (Monitoring logs) • Section 6.4.1 (Reviewing logs)	CCE_79412_3_do_not_send_diagnostic_info_to_apple
AU-8: Time stamps	• Section 6.4.2 (Performing clock synchronization)	CCE_79433_9_use_network_time_protocol

2374

2375 **Table 6: Security Assessment and Authorization (CA) Family Controls**

SP 800-53 Control Number and Name	Corresponding Sections in This Publication	Corresponding NIST Baseline Settings
CA-7: Continuous monitoring	• Section 2.7 (Monitoring security controls and configuration changes)	N/A

2376

2377 **Table 7: Configuration Management (CM) Family Controls**

SP 800-53 Control Number and Name	Corresponding Sections in This Publication	Corresponding NIST Baseline Settings
CM-1: Configuration management policy and procedures	• Section 2.5 (Having a configuration management policy, plan, and procedures) • Section 4 (Having a configuration management policy and user guidance for operating system and application installation and changes) • Section 5 (Managing security configurations)	N/A

SP 800-53 Control Number and Name	Corresponding Sections in This Publication	Corresponding NIST Baseline Settings
CM-2, Baseline configuration	• Section 2 (Having effective and well-tested security configurations)	All settings
CM-3: Configuration change control	• Section 2.6 (Documenting changes to default security baselines and settings) • Section 2.7 (Logging all hardware maintenance activities)	N/A
CM-4: Security impact analysis	• Section 2.6 (Testing changes to security controls) • Section 5 (Determine the effect of applying security baselines for a particular user or computer) • Section 6 (Considering the security effect of each decision made regarding a system)	N/A
CM-6: Configuration settings	• Section 2.5 (Having a security configuration guide) • Section 5 (Using security baselines to set security-relevant system settings and to compare actual settings to required settings)	N/A
CM-7: Least functionality	• Section 2.3.1.3 (Disabling unused local services)	CCE_79476_8_disable_location_services CCE_79471_9_disable_auto_actions_on_blank_CD_insertion CCE_79472_7_disable_auto_actions_on_blank_DVD_insertion CCE_79473_5_disable_auto_music_CD_play CCE_79474_3_disable_auto_picture_CD_display CCE_79475_0_disable_auto_video_DVD_play CCE_79506_2_bluetooth_turn_off_bluetooth CCE_79546_8_bluetooth_disable_file_sharing CCE_79507_0_disable_airdrop CCE_79533_6_disable_dictation CCE_79534_4_disable_voiceover CCE_79525_2_disable_printer_sharing CCE_79526_0_disable_remote_apple_events CCE_79528_6_disable_remote_login CCE_79529_4_disable_remote_management

SP 800-53 Control Number and Name	Corresponding Sections in This Publication	Corresponding NIST Baseline Settings
	• Section 2.3.2.1 (Disabling unused network services)	CCE_79483_4_disable_bonjour_advertising CCE_79526_0_disable_remote_apple_events CCE_79525_2_disable_printer_sharing CCE_79528_6_disable_remote_login CCE_79488_3_restrict_screen_sharing_to_specified_users CCE_79529_4_disable_remote_management CCE_79546_8_bluetooth_disable_file_sharing CCE_79507_0_disable_airdrop CCE_79481_8_disable_apple_file_server CCE_79482_6_disable_bluetooth_daemon CCE_79484_2_disable_nfs CCE_79485_9_disable_wifi_services
	• Section 3.10 (Application whitelisting)	N/A
	• Section 6.1.2 (Disabling unneeded hardware components)	N/A
	• Section 6.5 (Restricting the installation and execution of applications)	N/A
	• Section 6.6.1 (Using firewalls to restrict network traffic)	CCE_79522_9_enable_firewall_logging CCE_79445_3_enable_firewall_logging_detail_level CCE_79443_8_allow_signed_downloaded_sw_receive_connections CCE_79444_6_allow_signed_sw_receive_connections CCE_79470_1_turn_on_firewall See Table 20 for pf rules
	• Section 6.6.2 (Disabling sharing and remote access utilities)	CCE_79546_8_bluetooth_disable_file_sharing CCE_79511_2_no_guest_access_to_shared_folders CCE_79525_2_disable_printer_sharing CCE_79488_3_restrict_screen_sharing_to_specified_users CCE_79526_0_disable_remote_apple_events CCE_79528_6_disable_remote_login CCE_79529_4_disable_remote_management CCE_79483_4_disable_bonjour_advertising CCE_79507_0_disable_airdrop

SP 800-53 Control Number and Name	Corresponding Sections in This Publication	Corresponding NIST Baseline Settings
		CCE_79481_8_disable_apple_file_server
	• Section 6.6.3 (Disabling IPv6 support) • Section 6.6.4 (Disabling sshd support) • Section 6.6.5 (Disabling wireless networking) • Section 6.6.6 (Disabling Bonjour multicast advertisements)	N/A
		CCE_79500_5_ssh_restrict_users CCE_79528_6_disable_remote_login CCE_79494_1_ssh_disable_root_login CCE_79466_9_pf_rule_ssh
		CCE_79506_2_bluetooth_turn_off_bluetooth CCE_79546_8_bluetooth_disable_file_sharing CCE_79547_6_remove_all_preferred_wireless_networks CCE_79482_6_disable_bluetooth_daemon
		CCE_79483_4_disable_bonjour_advertising
CM-11: User-installed software	• Section 2.3.2.3 (Not installing or using non-approved applications) • Section 3.1 (Using Gatekeeper to limit which applications can be installed on a system) • Section 6.5 (Using Gatekeeper and Parental Controls to limit which applications can be executed on a system)	CCE_79406_5_enable_gatekeeper

Table 8: Contingency Planning (CP) Family Controls

SP 800-53 Control Number and Name	Corresponding Sections in This Publication	Corresponding NIST Baseline Settings
CP-2: Contingency plan	• Section 2.3 (Performing contingency planning) • Section 2.5 (Having IT contingency plans)	N/A

SP 800-53 Control Number and Name	Corresponding Sections in This Publication	Corresponding NIST Baseline Settings
CP-9: Information system backup	• Section 2.3 (Performing backups, storing them in a safe and secure location, and testing them regularly) • Section 4.2 (Performing backups and restores; testing backups)	N/A

2380

2381 **Table 9: Identification and Authentication (IA) Family Controls**

SP 800-53 Control Number and Name	Corresponding Sections in This Publication	Corresponding NIST Baseline Settings
IA-1: Identification and authentication policy and procedures	• Section 2.3.1.2 (Having a password policy) • Section 2.3.2.1 (Having a password policy)	CCE_79428_9_require_admin_password_for_system_prefs CCE_79422_2_password_enforce_password_history_restriction CCE_79424_8_password_guessable_pattern CCE_79419_8_password_complex_passwords_alphabetic_char CCE_79420_6_password_complex_passwords_numeric_char CCE_79421_4_password_complex_passwords_symbolic_char CCE_79427_1_password_uppercase_and_lowercase CCE_79426_3_password_minimum_length CCE_79425_5_password_maximum_age
IA-2: Identification and authentication (organizational users)	• Section 2.3.1.2 (Requiring valid username and password authentication) • Section 2.3.1.3 (Requiring strong passwords for administrator accounts) • Section 2.3.2.1 (Requiring strong authentication for using network services) • Section 2.3.2.3 (Using a daily-use account for normal system operations; using an administrator-level account only when needed for specific tasks) • Section 6.3.1 (Having an individual user account for each person)	CCE_79434_7_users_list_on_login CCE_79429_7_retries_until_hint CCE_79418_0_fast_user_switching CCE_79416_4_console_login CCE_79430_5_screensaver_grace_period CCE_79519_5_require_password_after_screensaver CCE_79431_3_start_screen_saver_hot_corner CCE_79517_9_no_modifier_keys_for_screen_saver_start CCE_79518_7_no_prevent_screensaver_corner CCE_79417_2_desktop_idle_time CCE_79514_6_disable_guest_user CCE_79428_9_require_admin_password_for_system_prefs CCE_79496_6_ssh_login_grace_period CCE_79492_5_ssh_challenge_response_authentication_disallowed CCE_79539_3_ssh_enable_password_authentication

SP 800-53 Control Number and Name	Corresponding Sections in This Publication	Corresponding NIST Baseline Settings
		CCE_79493_3_ssh_disable_pub_key_authentication CCE_79500_5_ssh_restrict_users CCE_79501_3_ssh_set_client_timeout CCE_79497_4_ssh_max_auth_tries_4_or_less CCE_79494_1_ssh_disable_root_login CCE_79537_7_ssh_disallow_empty_passwords CCE_79540_1_ssh_turn_off_user_environment CCE_79541_9_ssh_use_protocol_version_2 CCE_79538_5_ssh_disable_x11_forwarding CCE_79495_8_ssh_keep_alive_messages CCE_79433_9_use_network_time_protocol CCE_79520_3_sudo_restrict_to_single_terminal CCE_79432_1_sudo_timeout_period_set_to_0 CCE_79428_9_require_admin_password_for_system_prefs CCE_79422_2_password_enforce_password_history_restriction CCE_79424_8_password_guessable_pattern CCE_79419_8_password_complex_passwords_alphabetic_char CCE_79420_6_password_complex_passwords_numeric_char CCE_79421_4_password_complex_passwords_symbolic_char CCE_79427_1_password_uppercase_and_lowercase CCE_79426_3_password_minimum_length CCE_79425_5_password_maximum_age
	• Section 6.3.2.1 (Not permitting system login to be bypassed)	CCE_79513_8_disable_automatic_system_login
	• Section 6.3.2.4 (Disabling Fast User Switching)	CCE_79418_0_fast_user_switching
	• Section 6.3.2.5 (Using Active Directory services for authentication)	N/A
IA-4: Identifier management	• Section 6.3.1 (Creating a separate daily-use account for each user) • Section 6.3.4 (Having strong passwords for each user account)	CCE_79419_8_password_complex_passwords_alphabetic_char CCE_79420_6_password_complex_passwords_numeric_char CCE_79421_4_password_complex_passwords_symbolic_char CCE_79427_1_password_uppercase_and_lowercase CCE_79426_3_password_minimum_length

SP 800-53 Control Number and Name	Corresponding Sections in This Publication	Corresponding NIST Baseline Settings
IA-5: Authenticator management	• Section 2.3.2.2 (Using a secure user identification and authentication system)	N/A
	• Section 6.3.4 (Setting maximum password age; ensuring password strength; preventing password reuse through password history)	CCE_79422_2_password_enforce_password_history_restriction CCE_79424_8_password_guessable_pattern CCE_79425_5_password_maximum_age CCE_79419_8_password_complex_passwords_alphabetic_char CCE_79420_6_password_complex_passwords_numeric_char CCE_79421_4_password_complex_passwords_symbolic_char CCE_79427_1_password_uppercase_and_lowercase CCE_79426_3_password_minimum_length

Table 10: Incident Response (IR) Family Controls

SP 800-53 Control Number and Name	Corresponding Sections in This Publication	Corresponding NIST Baseline Settings
IR-1: Incident response policy and procedures	• Section 2.7 (Having an organization incident response policy)	N/A
IR-4: Incident handling	• Section 2.7 (Having a formal incident response capability)	N/A

Table 11: Maintenance (MA) Family Controls

SP 800-53 Control Number and Name	Corresponding Sections in This Publication	Corresponding NIST Baseline Settings
MA-1: System maintenance policy and procedures	• Section 2.3.2.3 (Creating a plan for maintaining macOS 10.12 systems)	N/A
MA-2: Controlled maintenance	• Section 2.7 (Performs regular security maintenance)	N/A
MA-4: Nonlocal maintenance	• Section 2.7 (Providing remote system administration and assistance)	N/A

2387 **Table 12: Media Protection (MP) Family Controls**

SP 800-53 Control Number and Name	Corresponding Sections in This Publication	Corresponding NIST Baseline Settings
MP-4: Media storage	• Section 2.3.1.2 (Physically securing removable media) • Section 2.7 (Protecting media) • Section 4.2 (Storing and protecting backup media)	N/A
MP-6: Media sanitization	• Section 2.7 (Sanitizing media) • Section 4.1.1 (Sanitizing media)	N/A

2388

2389 **Table 13: Physical and Environmental Protection (PE) Family Controls**

SP 800-53 Control Number and Name	Corresponding Sections in This Publication	Corresponding NIST Baseline Settings
PE-1: Physical and environmental protection policy and procedures	• Section 2.3.1.1 (Having a physical and environmental protection policy)	N/A
PE-3: Physical access control	• Section 2.3.1.1 (Implementing physical securing measures to restrict access to systems) • Section 2.3.2.3 (Restricting physical access to systems)	N/A

2390

2391 **Table 14: Planning (PL) Family Controls**

SP 800-53 Control Number and Name	Corresponding Sections in This Publication	Corresponding NIST Baseline Settings
PL-2: System security plan	• Section 2.5 (Having a security configuration guide and other security-related documentation)	N/A
PL-4: Rules of behavior	• Section 2.5 (Having a rules-of-behavior document)	N/A

2392

2393 **Table 15: Personnel Security (PS) Family Controls**

SP 800-53 Control Number and Name	Corresponding Sections in This Publication	Corresponding NIST Baseline Settings
PS-4: Personnel termination	• Section 2.3.1.2 (Disabling accounts as soon as employees leave the organization) • Section 2.3.2.1 (Disabling accounts as soon as employees leave the organization) • Section 6.3.1 (Disabling accounts as soon as they are no longer needed, such as an employee leaving the organization)	N/A
PS-5: Personnel transfer	• Section 6.3.1 (Disabling accounts as soon as they are no longer needed, such as an employee whose responsibilities change)	N/A

2394

2395 **Table 16: Risk Assessment (RA) Family Controls**

SP 800-53 Control Number and Name	Corresponding Sections in This Publication	Corresponding NIST Baseline Settings
RA-2: Security categorization	• Section 2.2 (Describes the FIPS 199 security categories and their relationship to SP 800-53 controls)	N/A
RA-3: Risk assessment	• Section 2.3 (Defining threats, conducting risk assessments, performing risk mitigation)	N/A
RA-5: Vulnerability scanning	• Section 2.7 (Performing vulnerability assessments to assess the security posture of the system) • Section 5.3 (Using vulnerability scanners to identify security issues)	N/A

2396

2397 **Table 17: System and Services Acquisition (SA) Family Controls**

SP 800-53 Control Number and Name	Corresponding Sections in This Publication	Corresponding NIST Baseline Settings
SA-5: Information system documentation	• Section 2.5 (Having a security configuration guide and other security-related documentation)	N/A

2398

2399 **Table 18: System and Communications Protection (SC) Family Controls**

SP 800-53 Control Number and Name	Corresponding Sections in This Publication	Corresponding NIST Baseline Settings
SC-4: Information in shared resources	• Section 3.9 (Encrypting virtual memory)	N/A
SC-8: Transmission confidentiality and integrity	• Section 2.3.2.2 (Encrypting network communications) • Section 6.6.4 (SSH Daemon)	CCE_79498_2_ssh_remove_non_fips_140_2_ciphers CCE_79499_0_ssh_remove_non_fips_140_2_macs
SC-13: Cryptographic protection	• Section 6.2.3.3 (Using FIPS-approved encryption algorithms)	CCE_79498_2_ssh_remove_non_fips_140_2_ciphers CCE_79499_0_ssh_remove_non_fips_140_2_macs
SC-18: Mobile code	• Section 2.3.2.3 (Configuring systems so that default file associations prevent automatic execution of active content files)	N/A
SC-28, Protection of information at rest	• Section 2.3.1.1 (Encrypting local files to prevent access) • Section 2.3.1.3 (Encrypting sensitive data) • Section 3.7 (Encrypting files to prevent access) • Section 3.9 (Encrypting virtual memory) • Section 4.2 (Encrypting Time Machine backups) • Section 6.2.3 (Encrypting files to prevent access)	N/A

2400

2401 **Table 19: System and Information Integrity (SI) Family Controls**

SP 800-53 Control Number and Name	Corresponding Sections in This Publication	Corresponding NIST Baseline Settings
SI-2: Flaw remediation	• Section 2.3.1.3 (Installing application and OS updates) • Section 2.3.2.1 (Testing and installing application and OS updates) • Section 2.7 (Acquiring and installing software updates) • Section 4.3 (Acquiring and installing security updates; configuring software update features) • Section 5.2 (Installing applications and application updates) • Section 5.3 (Checking the patch status of computers)	CCE_79544_3_install_system_data_updates CCE_79543_5_install_security_updates CCE_79502_1_update_apple_software CCE_79545_0_updates_download_in_background
SI-3: Malicious code protection	• Section 2.3.2.3 (Protecting systems from malicious payloads; using antivirus and antispyware software; configuring server and client software to reduce exposure to malware) • Section 3.8 (Using code execution protection features) • Section 6.2.2 (Displaying full filenames to identify suspicious extensions used by malware) • Section 6.5 (Restricting the execution of software) • Section 6.6.1 (Using host-based firewalls to block unknown software communications) • Section 6.7.4 (Using Terminal secure keyboard)	CCE_79438_8_display_file_extensions CCE_79543_5_install_security_updates CCE_79442_0_terminal_secure_keyboard
SI-4: Information system monitoring	• Section 2.7 (Monitoring event logs to identify problems and suspicious activity)	N/A
SI-5: Security alerts, advisories, and directives	• Section 2.3.2.3 (Monitoring mailing lists for relevant security bulletins) • Section 2.7 (Subscribing to and monitoring vulnerability notification mailing lists)	N/A

SP 800-53 Control Number and Name	Corresponding Sections in This Publication	Corresponding NIST Baseline Settings
SI-6: Security function verification	• Section 5.3 (Performing central monitoring of security controls)	N/A
SI-7: Software, firmware, and information integrity	• Section 2.7 (Monitoring changes to OS and software settings) • Section 3.2 (Preventing unwanted executables from being installed) • Section 6.5.2 (Using Parental Controls to prevent unwanted executables from running)	N/A
SI-8: Spam protection	• Section 2.3.2.3 (Protecting systems from malicious payloads; using e-mail clients that support spam filtering) • Section 6.7.1 (Configuring e-mail clients to use anti-spam features; configuring e-mail clients not to load remote images automatically) • Section 6.7.2 (Limiting Web browser cookies, including tracking cookies)	N/A
SI-16, Memory protection	• Section 3.8 (Code execution protection)	N/A

2402

Firewall rules for the pf firewall are grouped together in Table 20.

Table 20: pf Firewall Rules

CCE_79446_1_pf_enable_firewall	CCE_79463_6_pf_rule_screen_sharing
CCE_79450_3_pf_rule_ftp	CCE_79452_9_pf_rule_icmp
CCE_79466_9_pf_rule_ssh	CCE_79465_1_pf_rule_smtp
CCE_79467_7_pf_rule_telnet	CCE_79459_4_pf_rule_pop3
CCE_79468_5_pf_rule_tftp	CCE_79460_2_pf_rule_pop3s
CCE_79449_5_pf_rule_finger	CCE_79453_7_pf_rule_imap
CCE_79451_1_pf_rule_http	CCE_79454_5_pf_rule_imaps
CCE_79457_8_pf_rule_nfs	CCE_79461_0_pf_rule_printer_sharing
CCE_79462_8_pf_rule_remote_apple_events	CCE_79448_7_pf_rule_bonjour
CCE_79464_4_pf_rule_smb	CCE_79456_0_pf_rule_mDNSResponder
CCE_79447_9_pf_rule_apple_file_service	CCE_79455_2_pf_rule_itunes_sharing
CCE_79469_3_pf_rule_uucp	CCE_79458_6_pf_rule_optical_drive_sharing

Appendix C. Tools

Appendix C lists tools that may be helpful in configuring, managing, and monitoring the security of macOS systems.

The following table briefly describes a variety of commands that can be used to make configuration changes on macOS. This is not an exhaustive list of all tools available to make configuration changes. In order to fully automate some settings, other commands may be required in addition to those listed below. For more information on these commands, view the manual pages by using the `man` command in Terminal.

Table 21: Built-in Commands Used to Write macOS Configuration Data

Command Name	Description
`chgrp`	This is used to change the group ownership on a file or directory.
`chmod`	This command is used to change a file's permission bits. Modifications can be made to read, write, and execute attributes of a file or directory.
`chown`	This command is used to modify the owner and group owner on a file or directory.
`defaults`	The defaults command is used to modify or read macOS `.plist` configuration files. Modifying configuration files with defaults has a side-effect of resetting permissions and changing ownership metadata to the user who executed the command.
`dscl`	This command is used to modify and read Directory Service data. In this guide, `dscl` is used to modify and read user properties.
`kickstart`	This program is used for modifying remote management settings. This can be used to turn remote management off entirely, or to limit access to specific users.
`launchctl`	This program is responsible for starting and stopping services.
`networksetup`	This command changes the specified network adapter's settings.
`pfctl`	This tool modifies the `pf` firewall rules and behaviors.

Command Name	Description
`PlistBuddy`	This utility provides an alternate method for reading and editing `.plist` files. It allows for the modification of nested keys.
`pmset`	This command changes power management settings for macOS.
`praudit`	This tool allows the reading of BSM formatted log files, such as the ones located in `$AUDIT_LOG_PATH`.
`pwpolicy`	This is used to change password policy requirements for a specific user or for an entire system.
`scutil`	This command is used to modify and read many system settings. In this guide, the command is used to modify the system's name.
`security`	This command-line interface allows an administrator to access the security framework.
`socketfilterfw`	This command controls a variety of software firewall settings. It is used for actions such as disabling the firewall or configuring what applications are allowed through the firewall.
`softwareupdate`	This is the command-line program for viewing available updates and choosing which updates to install.
`spctl`	This command-line program controls Gatekeeper settings and determines what applications are allowed to run.
`systemsetup`	The `systemsetup` command can be used to modify many of the settings found in the System Preferences GUI application. This command is used to modify network time settings in this guide.
`system_profiler`	A tool that returns information about the host system.
`visudo`	This program is used to edit the `/etc/sudoers` file while ensuring the file's proper format.

2415

Appendix D. Resources

Appendix D lists resources that may be useful macOS security references.

Table 22: macOS Security Resources

Online Resource	URL
NIST macOS Setting Baselines and associated resources	https://github.com/usnistgov/applesec
Apple's OS X 10.10 security page	https://web.archive.org/web/20150201073654/http://www.apple.com/osx/what-is/security/
Apple's OS X 10.11 security page	https://web.archive.org/web/20160202045818/http://www.apple.com/osx/what-is/security/
Apple's macOS 10.12 security page	https://web.archive.org/web/20170324155229/http://www.apple.com/macos/security/
Apple Security Updates	https://support.apple.com/en-us/HT201222
CIS macOS Benchmarks	https://benchmarks.cisecurity.org/downloads/browse/index.cfm?category=benchmarks.os.unix.osx
DISA STIG for macOS	http://iase.disa.mil/stigs/os/mac/Pages/mac-os.aspx
TCP and UDP ports used by Apple software products	https://support.apple.com/en-us/HT202944

Appendix E. Acronyms and Abbreviations

Selected acronyms and abbreviations used in the guide are defined below.

AES	Advanced Encryption Standard
ARD	Apple Remote Desktop
ASLR	Address Space Layout Randomization
BIOS	Basic Input/Output System
DISA	Defense Information Systems Agency
DNS	Domain Name System
DoS	Denial of Service
EFI	Extensible Firmware Interface
EULA	End User License Agreement
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
GB	Gigabyte
GUI	Graphical User Interface
HFS	Hierarchical File System
ICMP	Internet Control Message Protocol
IM	Instant Messaging
IP	Internet Protocol
IPsec	Internet Protocol Security
IPv6	Internet Protocol version 6
IT	Information Technology
ITL	Information Technology Laboratory
LAN	Local Area Network
NAT	Network Address Translation
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol

OMB	Office of Management and Budget
OS	Operating System
OVAL	Open Vulnerability and Assessment Language
P2P	Peer-to-Peer
PC	Personal Computer
PII	Personally Identifiable Information
PIV	Personal Identity Verification
POP3	Post Office Protocol 3
SCAP	Security Content Automation Protocol
SFTP	Secure File Transfer Protocol
SIP	System Integrity Protection
S/MIME	Secure/Multipurpose Internet Mail Extensions
SMTP	Simple Mail Transfer Protocol
SOHO	Small Office/Home Office
SP	Special Publication
SSH	Secure Shell
SSLF	Specialized Security-Limited Functionality
STIG	Security Technical Implementation Guide
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
USB	Universal Serial Bus
XD	Execute Disable

2422

Appendix F. Terminal Command Variables

Many terminal commands explained in this document use variables, which are described below. They must be replaced with a value in order to have the desired effect.

Table 23: Terminal Command Variable Descriptions

Variable	Description
`$AUDIT_LOG_PATH`	This value is the location of the path to audit logs specified in the `/etc/security/audit_control` file. It is located on the line beginning with `dir:`
`$DEVICE_NAME`	This variable is used for configuring wireless network settings and represents the Wi-Fi adapter to be configured. It can be retrieved from the system by running this command: `networksetup -listnetworkserviceorder`
`$HOST_ID`	This should be replaced with a non-identifying name that will be used for each type of name for a single computer. The different name types are `LocalHostName`, `HostName`, `ComputerName`, and `NetBIOSName`.
`$HW_UUID`	This is the unique hardware-based identifier for the system. This value can be obtained by using this command: `system_profiler SPHardwareDataType 2> /dev/null | grep 'Hardware UUID' | awk ' { print $3 }'`
`$PROFILE_VALUE`	Since not all security configurations use the same values, this variable is a placeholder for the actual profile's value. The values for the Standalone, Managed, and SSLF profiles are given in the table along with the terminal command.
`$SHELL_FILES_PATH`	The location of the shell files as specified in the `/etc/shells` file.
`$USER`	For some settings that require a specific username to run, this variable is used. Replace this variable with the desired username.
`$USER_GROUP`	This variable should be replaced with the group name for which the user is a member.

Appendix G. Special Files

Below is a list of files that must be edited manually because there are no provided tools.

Table 24: Files Requiring Manual Editing

File name	Description
`/etc/sudoers`	This file needs to be modified in order to set restrictions on the `sudo` command. For SSLF systems, NIST recommends that authentication should be required for each `sudo` command, and `sudo` sessions should not persist across Terminal windows. Editing the `/etc/sudoers` file manually can lead to mistakes that may make the file unreadable to the system. To make changes to this file, edit it using the `visudo` command. An administrator can type `sudo visudo` into Terminal to begin editing `/etc/sudoers`. When saving changes to the file, `visudo` will validate that all additions are formatted properly. See Appendix J.3 for enhancing `sudo` security.
`/etc/ssh/sshd_config`	This file contains configuration information and security settings for the SSH daemon (server).
`/etc/security/audit_control`	This file contains the values for configuring audit logs, which includes log retention, log size, and the type of information that is recorded.
`/etc/autofs.conf`	This file holds the configuration information for the `automount` service.

Appendix H. Process Restarting

Some settings may require certain processes to be restarted in order for the desired result to be achieved. In most cases, restarting processes causes the setting changes to take effect immediately, rather than after restarting the system. macOS 10.12 uses preference caching, which can prevent changed preferences from taking effect properly without restarting the `cfprefsd` process. The table below gives the names of processes and the settings related to those processes.

Table 25: Settings Requiring Process Restart

Setting	Related Process Names
Show filename extensions	`cfprefsd`, `Finder`
Show hidden files	
Disable AirDrop	
Disable blank CD actions	`cfprefsd`, `SystemUIServer`
Disable blank DVD actions	
Disable music CD actions	
Disable picture CD actions	
Disable video DVD actions	
Show Bluetooth status in menu bar	
Disallow Bluetooth devices to wake the computer	`cfprefsd`, `UserEventAgent`
Restrict screen sharing to no users	`cfprefsd`, `opendirectoryd`
Show Safari status bar	`cfprefsd`
Disable Bonjour advertising	
Disable remote Apple events for specific users	
Screen saver grace period	`cfprefsd`, `Dock`
Start screen saver hot corner	
Desktop idle time	
Auto hide Dock	
Disable Siri	`Siri`, `cfprefsd`

As a convenience, all of the above processes are listed below:

- `cfprefsd`
- `Dock`

- `Finder`
- `Siri`
- `SystemUIServer`
- `UserEventAgent`

Appendix I. File Attributes

I.1. System Integrity Protection (SIP)

NIST recommends that SIP remain enabled, which is the default state.

SIP status can be queried with the Terminal command `csrutil status`. In specific circumstances, SIP may be temporarily disabled. The SIP state can only be modified when the system is operating in recovery mode. In a recovery mode Terminal, `csrutil disable` can be used to turn off SIP (enabled with `csrutil enable`). Disabling SIP allows an administrator full access to the file system and therefore to any protected system settings. Changes made to protected files while SIP is disabled will be enforced by SIP after SIP is re-enabled. Subsequent system updates, however, may overwrite such configuration changes.

The following files and folders are protected by SIP:

/Applications/App Store.app
/Applications/Automator.app
/Applications/Calculator.app
/Applications/Calendar.app
/Applications/Chess.app
/Applications/Contacts.app
/Applications/Dashboard.app
/Applications/Dictionary.app
/Applications/DVD Player.app
/Applications/FaceTime.app
/Applications/Font Book.app
/Applications/Game Center.app
/Applications/Image Capture.app
/Applications/Launchpad.app
/Applications/Mail.app
/Applications/Maps.app
/Applications/Messages.app
/Applications/Mission Control.app
/Applications/Notes.app
/Applications/Photo Booth.app
/Applications/Photos.app
/Applications/Preview.app
/Applications/QuickTime Player.app
/Applications/Reminders.app
/Applications/Safari.app
/Applications/Siri.app
/Applications/Stickies.app
/Applications/System Preferences.app
/Applications/TextEdit.app
/Applications/Time Machine.app
/Applications/Utilities/Activity Monitor.app

/Applications/Utilities/AirPort Utility.app
/Applications/Utilities/Audio MIDI Setup.app
/Applications/Utilities/Bluetooth File Exchange.app
/Applications/Utilities/Boot Camp Assistant.app
/Applications/Utilities/ColorSync Utility.app
/Applications/Utilities/Console.app
/Applications/Utilities/Digital Color Meter.app
/Applications/Utilities/Disk Utility.app
/Applications/Utilities/Feedback Assistant.app
/Applications/Utilities/Grab.app
/Applications/Utilities/Grapher.app
/Applications/Utilities/Keychain Access.app
/Applications/Utilities/Migration Assistant.app
/Applications/Utilities/Script Editor.app
/Applications/Utilities/System Information.app
/Applications/Utilities/Terminal.app
/Applications/Utilities/VoiceOver Utility.app
/Library/Application Support/com.apple.TCC
/Library/Filesystems/NetFSPlugins/Staged
/Library/Filesystems/NetFSPlugins/Valid
/Library/Preferences/SystemConfiguration/com.apple.Boot.plist
/System
/System/Library/Assets
/System/Library/Caches
/System/Library/Extensions
/System/Library/Extensions/*
/System/Library/LaunchDaemons/com.apple.UpdateSettings.plist
/System/Library/PreinstalledAssets
/System/Library/Speech
/System/Library/User Template
/bin
/private/var/db/datadetectors
/private/var/db/dyld
/private/var/folders
/sbin
/usr
/usr/libexec/cups
/usr/local
/usr/share/man
/usr/share/snmp
/etc
/tmp
/var

I.2. Permissions and Ownership

System files need to be protected from unauthorized modification. On macOS 10.12, SIP only allows Apple-sanctioned programs to change these files. Normally, file properties can be modified using programs such as `chmod`, `chown`, and `chgrp`. System files and directories include, but are not limited to, those found in `/etc`, `/bin`, `/usr/bin`, `/sbin`, and `/usr/sbin`. Note that all files and folders must belong to a valid owner and group. Typically, a user or group becomes invalid when it is deleted from the system, and files they owned were not removed.

New files created on a system have default file permissions applied. These default file permissions are controlled by the system's `umask` value. The `umask` value specifies the permissions that new files will **not** have. For example, a `umask` of `022` will result in a file with mode `755`. The `umask` configuration command is available in Appendix J.17.

Table 26 lists the recommended permissions and ownership information for a variety of macOS files. A "-" represents no recommended change from the default value for that column. A "`*`" in the path means that all files in the directory should have the specified permissions and ownership values applied to them. See the man page for `chmod` for more details. Note that permissions can be reduced below the recommended values but may cause loss of functionality.

Table 26: Recommended File Permissions and Ownership

File/Directory Name	Permission	Owner	Group
`~/*`	-	`$USER`	`$USER_GROUP`
Home directories	`go-rwx`	-	-

Appendix J. Terminal Configuration Commands

This appendix provides the terminal commands needed to configure a system through an automated process. It is broken down into sections based on the categories of the settings. Some of the recommended baseline settings are already achieved by the default system configuration. These settings have been omitted from this appendix, but can be found in the companion spreadsheet.

J.1. Disabling Hardware Components

Note that moving kernel extension (`kext`) files is no longer possible on macOS 10.12 because SIP blocks access.

Table 27: Disabling Hardware Components

Device Name	Disable Through Configuration
Bluetooth	`defaults write /Library/Preferences/com.apple.Bluetooth.plist ControllerPowerState -bool false` This setting is only recommended for SSLF systems.
Wi-Fi[42]	`networksetup -setairportpower en1 off` Where `en1` is the Wi-Fi adapter name. This setting is only recommended for SSLF systems.
Infrared (IR)	`defaults write /Library/Preferences/com.apple.driver.AppleIRController.plist DeviceEnabled -bool false`

J.2. Finder Preferences

Table 28: Finder Preferences

Setting Name	Terminal Commands
*Show filename extensions	`defaults write ~/Library/Preferences/.GlobalPreferences.plist AppleShowAllExtensions -bool true`
*Show hidden files	`defaults write ~/Library/Preferences/com.apple.finder.plist AppleShowAllFiles -bool true` This setting is only recommended for SSLF systems.

* This setting requires a process restart to take effect. See Appendix H for a list of the specific processes that must be restarted.

[42] Run the command `networksetup -listnetworkserviceorder` to view the short device names.

J.3. User Account Types

Table 29: User Account Settings

Setting Name	Terminal Commands
Set `sudo` authentication frequency	`echo "Defaults timestamp_timeout=0" >> /etc/sudoers` This setting is only recommended for SSLF systems. Change the value if the line already exists.

J.4. Login Window

Table 30: Login Window GUI Settings

Setting Name	Terminal Commands
Hide users list	`defaults write /Library/Preferences/com.apple.loginwindow.plist SHOWFULLNAME -bool true`
Disable password hints	`defaults write /Library/Preferences/com.apple.loginwindow.plist RetriesUntilHint -int 0`
Disable fast user switching	`defaults write /Library/Preferences/.GlobalPreferences MultipleSessionEnabled -bool false` This setting is only recommended for Managed and SSLF systems.

Table 31: Login Window Terminal Settings

Setting Name	Terminal Commands
Disable console login	`defaults write /Library/Preferences/com.apple.loginwindow.plist DisableConsoleAccess -bool true`
Hide admin accounts on login window	`defaults write /Library/Preferences/com.apple.loginwindow.plist HideAdminUsers -bool true`
Hide local user accounts on login window	`defaults write /Library/Preferences/com.apple.loginwindow.plist HideLocalUsers -bool true`

Setting Name	Terminal Commands
Hide mobile users on login window	`defaults write /Library/Preferences/com.apple.loginwindow.plist HideMobileAccounts -bool true`
Hide network users on login window	`defaults write /Library/Preferences/com.apple.loginwindow.plist IncludeNetworkUser -bool false`

J.5. Password Policy

The `pwpolicy` program uses a `.plist` file for policy configuration. The NIST-recommended password policy is available as a `.plist` file on the GitHub repository listed in the resources in Appendix D.

The `plist` policy file is applied for all users with the following command:

```
pwpolicy -setaccountpolicies /full/path/to/policyTempFile
```

The policy temp file can be removed after it is applied.

Alternatively, the `pwpolicy` `.plist` file can be generated and customized using the following process. First, the `.plist` file array needs to be created only once for each of the following policy categories. These commands do not need to be run on a per-setting basis.

```
/usr/libexec/PlistBuddy –c “Add :policyCategoryPasswordContent array”
/full/path/to/policyTempFile

/usr/libexec/PlistBuddy –c “Add :policyCategoryPasswordChange array”
/full/path/to/policyTempFile

/usr/libexec/PlistBuddy –c “Add :policyCategoryAuthentication array”
/full/path/to/policyTempFile
```

Each setting needs to have an array index different than the others, in increasing order, starting with index 0. These commands must be run for each setting, substituting the values from Table 32.

```
/usr/libexec/PlistBuddy –c “Add :$policy_category:$index:policyContent string
$policy_content” /full/path/to/policyTempFile

/usr/libexec/PlistBuddy –c “Add :$policy_category:$index:policyIdentifier string
$policy_identifier” /full/path/to/policyTempFile

/usr/libexec/PlistBuddy –c “Add :$policy_category:$index:policyParameters dict”
/full/path/to/policyTempFile

/usr/libexec/PlistBuddy –c “Add
:$policy_category:$index:policyParameters:$parameter_name integer  $parameter_value”
/full/path/to/policyTempFile
```

2605

2606 **Table 32: Password Policy Settings**

Password Rule	Policy Variable Substitutions

Maximum age	`$policy_category` = `policyCategoryPasswordChange`
	`$policy_content` = `policyAttributeCurrentTime > policyAttributeLastPasswordChangeTime + (policyAttributeExpiresEveryNDays * 24 * 60 * 60)`
	`$policy_identifier` = `Password expires every 60 days`
	`$parameter_name` = `policyAttributeExpiresEveryNDays`
	`$parameter_value` = `60`

Minimum length	`$policy_category` = `policyCategoryPasswordContent`
	`$policy_content` = `policyAttributePassword matches \'(.){12,}\'`
	`$policy_identifier` = `Contains at least 12 characters`
	`$parameter_name` = `minimumChars`
	`$parameter_value` = `12`

Require alphabetic character	`$policy_category` = `policyCategoryPasswordContent`
	`$policy_content` = `policyAttributePassword matches \'(.*[a-zA-Z].*)\'`
	`$policy_identifier` = `Contains at least 1 alphabetic character`
	`$parameter_name` = `minimumAlphaCharacters`
	`$parameter_value` = `1`

Require numeric character	`$policy_category` = `policyCategoryPasswordContent`
	`$policy_content` = `policyAttributePassword matches \'(.*[0-9].*)\'`
	`$policy_identifier` = `Contains at least 1 numeric character`
	`$parameter_name` = `minimumNumericCharacters`
	`$parameter_value` = `1`

Require symbolic character	`$policy_category` = `policyCategoryPasswordContent`
	`$policy_content` = `policyAttributePassword matches \'(.*[^0-9a-zA-Z].*)\'`
	`$policy_identifier` = `Contains at least 1 symbolic character`
	`$parameter_name` = `minimumSymbolicCharacters`
	`$parameter_value` = `1`

Password Rule	Policy Variable Substitutions

Failed login lockout	`$policy_category` = `policyCategoryAuthentication`
	`$policy_content` = `(policyAttributeFailedAuthentications < policyAttributeMaximumFailedAuthentications) OR (policyAttributeCurrentTime > policyAttributeLastFailedAuthenticationTime + lockoutDuration * 60)`
	`$policy_identifier` = `3 failed login attempts lock user accounts for 15 minutes`
	`$parameter_name` = `lockoutDuration`
	`$parameter_value` = `15`
	`$parameter_name2` = `policyAttributeMaximumFailedAuthentications`
	`$parameter_value2` = `3`

Password history restriction	`$policy_category` = `policyCategoryPasswordContent`
	`$policy_content` = `none policyAttributePasswordHashes in policyAttributePasswordHistory`
	`$policy_identifier` = `Last 15 passwords cannot be reused`
	`$parameter_name` = `policyAttributeHistoryDepth`
	`$parameter_value` = `15`

Upper and lowercase characters	`$policy_category` = `policyCategoryPasswordContent`
	`$policy_content` = `policyAttributePassword matches \'(.*[a-z].*[A-Z].*)| (.*[A-Z].*[a-z].*)\'`
	`$policy_identifier` = `Contains at least 1 upper and 1 lower case character`
	`$parameter_name` = `minimumMixedCaseInstances`
	`$parameter_value` = `1`

Password cannot contain username	This setting did not work as documented during informal testing.

Password cannot contain any guessable patterns – contains less than 3 sequential characters	`$policy_category` = `policyCategoryPasswordContent`
	`$policy_content` = `policyAttributeSequentialCharacters < policyAttributeMaximumSequentialCharacters`
	`$policy_identifier` = `Contains less than 3 sequential characters`
	`$parameter_name` = `policyAttributeMaximumSequentialCharacters`
	`$parameter_value` = `3`

Password cannot contain any guessable patterns – contains less than 3 consecutive characters	`$policy_category` = `policyCategoryPasswordContent`
	`$policy_content` = `policyAttributeConsecutiveCharacters < policyAttributeMaximumConsecutiveCharacters`
	`$policy_identifier` = `Contains less than 3 consecutive characters`
	`$parameter_name` = `policyAttributeMaximumConsecutiveCharacters`
	`$parameter_value` = `3`

2607

J.6. Session Locking

Table 33: Session Locking Settings

Setting Name	Terminal Command
*Screen saver grace period	`defaults write ~/Library/Preferences/ByHost/com.apple.screensaver.$HW_UUID.plist askForPasswordDelay -int 5`
*Start screen saver hot corner[43]	`defaults write ~/Library/Preferences/com.apple.dock.plist wvous-$CORNER-corner -int 5`
*No prevent screen saver hot corner	For any corner that would prevent the screen saver, run the following command for that corner: `defaults write ~/Library/Preferences/com.apple.dock.plist wvous-$CORNER-corner -int 1`
*Desktop idle time	`defaults write ~/Library/Preferences/com.apple.dock.plist idleTime -int 1200`

* This setting requires a process restart to take effect. See Appendix H for a list of the specific processes that must be restarted.

J.7. Firewalls

Table 34: Application Firewall Settings

Setting Name	Terminal Command
Turn on firewall	`/usr/libexec/ApplicationFirewall/socketfilterfw --setglobalstate on`
Turn on firewall and block all incoming connections	`/usr/libexec/ApplicationFirewall/socketfilterfw --setblockall on` This setting is only recommended for SSLF systems.
Automatically allow signed builtin software to receive incoming connections	`/usr/libexec/ApplicationFirewall/socketfilterfw --setallowedsigned on`
Automatically allow signed downloaded software to receive incoming connections	`/usr/libexec/ApplicationFirewall/socketfilterfw --setallowedsignedapp on`
Enable firewall logging detail level	`/usr/libexec/ApplicationFirewall/socketfilterfw –setloggingopt detail`

[43] Use one of the codes "`bl`," "`br`," "`tl`," or "`tr`" in place of `$CORNER`; where "`bl`" is bottom left, "`tr`" is top right, etc.

The `pf` firewall is separate from the application firewall and offers finer-grained controls. Before making changes to `pf` settings, be sure to back up the `/etc/pf.conf` file. The `pf` firewall must be configured to run automatically on system startup in order to maintain persistence. The `pf` firewall needs to be directed to a configuration file with the desired anchor points. An anchor point allows a set of firewall rules to be loaded from another file. An anchor is first defined and then loaded from a specified file.

Firewall rules must be constructed and placed in a custom anchor file specified in `/etc/pf.conf`. For example, incoming SSH connections can be blocked with the following rule: `block in proto { tcp udp } to any port 22`. This instructs `pf` to block incoming traffic using the TCP or UDP protocols destined for any IP address on port 22. The full set of recommendations for `pf` firewall rules is available in Table 2. The Terminal configuration commands are available below in Table 35.

Table 35: pf Firewall Settings

Action	Terminal Command
Turn on firewall	`pfctl –e`

Run firewall automatically on system startup	`cp /System/Library/LaunchDaemons/com.apple.pfctl.plist /Library/LaunchDaemons/sam.pfctl.plist`
	`/usr/libexec/PlistBuddy -c "Add :ProgramArguments:1 string -e" /Library/LaunchDaemons/sam.pfctl.plist`
	`/usr/libexec/PlistBuddy -c "Set :Label sam.pfctl" /Library/LaunchDaemons/sam.pfctl.plist`
	`launchctl enable system/sam.pfctl`
	`launchctl bootstrap system /Library/LaunchDaemons/sam.pfctl.plist`

Define and add custom anchor to config file	`echo 'anchor "sam_pf_anchors"' >> /etc/pf.conf` `echo 'load anchor "sam_pf_anchors" from "/etc/pf.anchors/sam_pf_anchors"' >> /etc/pf.conf`
Load a `pf` configuration	`pfctl –f /etc/pf.conf`

J.8. Sharing Services

Table 36: Sharing Settings

Setting Name	Terminal Command

*Disable remote Apple events for specific users	`defaults write /private/var/db/dslocal/nodes/Default/groups/com.apple.access_remote_ae.plist users –array "";`
	
	`defaults delete /private/var/db/dslocal/nodes/Default/groups/com.apple.access_remote_ae.plist groupmembers;`
	
	`defaults delete /private/var/db/dslocal/nodes/Default/groups/com.apple.access_remote_ae.plist nestedgroups`

* This setting requires a process restart to take effect. See Appendix H for a list of the specific processes that must be restarted.

J.9. SSH Daemon

SSH daemon (server) settings are stored in /etc/ssh/sshd_config.

Table 37: SSH Settings

Key Name	Value
`LoginGraceTime`	`30`
`Ciphers`	`aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,aes192-cbc,aes256-cbc,3des-cbc`
`MACs`	`hmac-sha2-256,hmac-sha2-512,hmac-sha1`
`ChallengeResponseAuthentication`	`no`
`PubkeyAuthentication`	`no`
`DenyUsers`	`*`
`ClientAliveInterval`	`900`
`maxAuthTries`	`4`

Key Name	Value
`PermitRootLogin`	`no`
`ClientAliveCountMax`	`0`

J.10. Wireless Networking

Table 38: Wireless Networking Settings

Setting Name	Terminal Command
Don't open Bluetooth setup assistant if no keyboard detected	`defaults write /Library/Preferences/com.apple.Bluetooth.plist BluetoothAutoSeekKeyboard -bool false` This setting is only recommended for SSLF systems.
Don't open Bluetooth setup assistant if no mouse or trackpad detected	`defaults write /Library/Preferences/com.apple.Bluetooth.plist BluetoothAutoSeekPointingDevice -bool false` This setting is only recommended for SSLF systems.
*Show Bluetooth status in menu bar	`defaults write ~/Library/Preferences/com.apple.systemuiserver.plist menuExtras -array-add "/System/Library/CoreServices/Menu\ Extras/Bluetooth.menu"`
*Disallow Bluetooth devices to wake the computer	`defaults write ~/Library/Preferences/ByHost/com.apple.Bluetooth.$HW_UUID.plist RemoteWakeEnabled -bool false`
*Disable AirDrop	`defaults write ~/Library/Preferences/com.apple.NetworkBrowser.plist DisableAirDrop -bool true`

* This setting requires a process restart to take effect. See Appendix H for a list of the specific processes that must be restarted.

J.11. Network Services

Table 39: Network Services Settings

Setting Name	Terminal Command
Change LocalHostName	`scutil --set LocalHostName $HOST_ID`
Change HostName	`scutil --set HostName $HOST_ID`
Change ComputerName	`scutil --set ComputerName $HOST_ID`
Change NetBIOSName	`defaults write /Library/Preferences/SystemConfiguration/com.apple.smb.server.plist NetBIOSName $HOST_ID`
*Disable Bonjour advertising	`defaults write /System/Library/LaunchDaemons/com.apple.mDNSResponder.plist ProgramArguments -array-add "-NoMulticastAdvertisements"`
Use 2 DNS servers[44]	`networksetup -setdnsservers [networkservice] server1, server2`

Use Network Time Protocol (NTP)	`systemsetup -setnetworktimeserver $ADDRESS`
	
	`systemsetup -setusingnetworktime on`

*Restrict screen sharing to no users	`defaults write /private/var/db/dslocal/nodes/Default/groups/com.apple.access_screensharing.plist users -array ""`
	
	`defaults delete /private/var/db/dslocal/nodes/Default/groups/com.apple.access_screensharing.plist groupmembers`
	
	`defaults delete /private/var/db/dslocal/nodes/Default/groups/com.apple.access_screensharing.plist nestedgroups`

Restrict remote management to specific users	`/System/Library/CoreServices/RemoteManagement/ARDAgent.app/Contents/Resources/kickstart –quiet –configure -allowAccessFor –specifiedUsers –access -off`

* This setting requires a process restart to take effect. See Appendix H for a list of the specific processes that must be restarted.

[44] [network service] is one of the services listed from running the command `networksetup –listallnetworkservices`.

J.12. CD and DVD Preferences

Table 40: CD and DVD Settings

Setting Name	Terminal Command
*Disable blank CD actions	`defaults write ~/Library/Preferences/com.apple.digihub.plist com.apple.digihub.blank.cd.appeared -dict action -int 1`
*Disable blank DVD actions	`defaults write ~/Library/Preferences/com.apple.digihub.plist com.apple.digihub.blank.dvd.appeared -dict action -int 1`
*Disable music CD actions	`defaults write ~/Library/Preferences/com.apple.digihub.plist com.apple.digihub.cd.music.appeared -dict action -int 1`
*Disable picture CD actions	`defaults write ~/Library/Preferences/com.apple.digihub.plist com.apple.digihub.cd.picture.appeared -dict action -int 1`
*Disable video DVD actions	`defaults write ~/Library/Preferences/com.apple.digihub.plist com.apple.digihub.dvd.video.appeared -dict action -int 1`

* This setting requires a process restart to take effect. See Appendix H for a list of the specific processes that must be restarted.

J.13. Privacy

Table 41: Privacy Settings

Setting Name	Terminal Command
Disable location services	`defaults write /private/var/db/locationd/Library/Preferences/ByHost/com.apple.locationd.$HW_UUID.plist LocationServicesEnabled -bool false; launchctl bootout system/com.apple.locationd` This setting is only recommended for SSLF systems.
Disable sending of diagnostic data to Apple	`defaults write ~/Library/Preferences/ByHost/com.apple.SubmitDiagInfo.$HW_UUID.plist AutoSubmit -bool false`

Setting Name	Terminal Command
*Disable Siri	`defaults write ~/Library/Preferences/com.apple.assistant.support.plist "Assistant Enabled" -int 0`
Disable lookup suggestions	`defaults write ~/Library/Preferences/com.apple/lookup.shared.plist LookupSuggestionsDisabled -int 1`

* This setting requires a process restart to take effect. See Appendix H for a list of the specific processes that must be restarted.

J.14. Auditing

Table 42: Auditing Settings

Setting Name	Terminal Command
Set audit control flags	`sed -i.bk 's/^flags.*/flags:lo,ad,-all,fd,fm,^-fa,^-fc,^-cl/' /etc/security/audit_control; rm /etc/security/audit_control.bk`
Audit log max file size	`sed -i.bk 's/^filesz.*/filesz:80M/' /etc/security/audit_control; rm /etc/security/audit_control.bk`
Audit log retention	`sed -i.bk 's/^expire-after.*/expire-after:30d AND 5G/' /etc/security/audit_control; rm /etc/security/audit_control.bk`

J.15. Power Management

Although most power management settings do not directly affect security, they are still important for effective system use. The one important setting to note is "Display sleep idle time," which must have a value greater than or equal to the "Desktop idle time" setting in Appendix J.6. If the screen goes to sleep before the session locks, it creates a false sense of security.

Table 43: Power Management Settings

Setting Name	Terminal Command
Disable computer sleep	`pmset -c sleep 0`
Disable wake for network access	`pmset -a womp 0`

Setting Name	Terminal Command
Display sleep idle time	`pmset -a displaysleep 20`

J.16. Daemons

Table 44: Disabling Daemons

Setting Name	Terminal Command

Disable Bluetooth daemon	`launchctl disable system/com.apple.blued`
	`launchctl bootout system/com.apple.blued`
	This setting is only recommended for SSLF systems and systems where Bluetooth is not used.

Disable Wi-Fi daemon	`launchctl disable system/com.apple.airportd`
	`launchctl bootout system/com.apple.airportd`
	`launchctl disable system/com.apple.airport.wps`
	`launchctl bootout system/com.apple.airport.wps`
	This setting is only recommended for SSLF systems and systems where Wi-Fi is not used.

Disable NFS daemon	`launchctl disable system/com.apple.nfsd`
	`launchctl bootout system/com.apple.nfsd`
	`launchctl disable system/com.apple.lockd`
	`launchctl bootout system/com.apple.lockd`
	`launchctl disable system/com.apple.statd.notify`
	`launchctl bootout system/com.apple.statd.notify`

Disable Apple File Server daemon	`launchctl disable system/com.apple.smbd`
	`launchctl bootout system/com.apple.smbd`
	`launchctl disable system/com.apple.AppleFileServer`
	`launchctl bootout system/com.apple.AppleFileServer`

J.17. Miscellaneous Settings

Table 45: Miscellaneous Settings

Setting Name	Terminal Command
*Show Safari status bar	`defaults write ~/Library/Preferences/com.apple.Safari.plist ShowOverlayStatusBar -bool true`
*Auto hide Dock	`defaults write ~/Library/Preferences/com.apple.dock.plist autohide -bool true` This setting is only recommended for SSLF systems.
*Disable Mission Control Dashboard	`defaults write ~/Library/Preferences/com.apple.dashboard.plist dashboard-enabled-state -int 1` This setting is only recommended for SSLF systems.
Update Apple software	`softwareupdate -ia`

Enable Gatekeeper	`spctl --master-enable`
	
	`spctl --enable`

Set umask for all users	`launchctl config user mask 027`
Terminal secure keyboard entry	`defaults write ~/Library/Preferences/com.apple.Terminal.plist SecureKeyboardEntry -int 1`

Administrator access for system-wide preferences	`security authorizationdb read system.preferences > sam_temp.plist`
	
	`defaults write sam_temp.plist shared -bool false`
	
	`security authorizationdb write system.preferences < sam_temp.plist`
	
	`rm sam_temp.plist`

* This setting requires a process restart to take effect. See Appendix H for a list of the specific processes that must be restarted.

Appendix K. Glossary

For other terms not defined here, please see NISTIR 7298, Glossary of Key Information Security Terms [NISTIR 7298r2].

Application Firewall [SP 800-41r1]	A firewall that uses stateful protocol analysis to analyze network traffic for one or more applications.
Kernel Panic	A system error that cannot be recovered from, and requires the system to be restarted.
Kext File	A Kernel extension file that allows the operating system to make use of hardware components. Files of this type typically have a .kext file extension.
Management Controls [FIPS 200]	The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security.
Operational Controls [FIPS 200]	The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by people (as opposed to systems).
Principle of Least Privilege[45]	The principle that users and programs should only have the necessary privileges to complete their tasks.
Privilege Escalation	The exploitation of a bug or flaw that allows for a higher privilege level than what would normally be permitted.
Production Environment	An environment where functionality and availability must be ensured for the completion of day-to-day activities.
Property List (`.plist`) File	An XML file that is used to store system settings.
Sandboxing [NISTIR 7298r2]	A restricted, controlled execution environment that prevents potentially malicious software, such as mobile code, from accessing any system resources except those for which the software is authorized.
Shell	The command line environment made available to macOS users through the Terminal application.
Stateful Inspection [SP 800-41r1]	Packet filtering that also tracks the state of connections and blocks packets that deviate from the expected state.
Whitelist [NISTIR 7298r2]	A list of discrete entities, such as hosts or applications, that are known to be benign and are approved for use within an organization and/or information system.

[45] J. Saltzer and M. Shroeder, "The Protection of Information in Computer Systems," *Proceedings of the IEEE* vol. 63, issue 9, p. 1278-1308, Sep. 1975, https://doi.org/10.1109/PROC.1975.9939.

Appendix L. NIST Document References

[CSD16] Computer Security Division, Applied Cybersecurity Division (2016) *Best Practices for Privileged User PIV Authentication*. (National Institute of Standard and Technology, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.04212016

[FIPS 199] National Institute of Standards and Technology (2004) *Standards for Security Categorization of Federal Information and Information Systems*. (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) 199, February 2004. https://doi.org/10.6028/NIST.FIPS.199

[FIPS 200] National Institute of Standards and Technology (2006) *Minimum Security Requirements for Federal Information and Information Systems*. (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) 200, March 2006. https://doi.org/10.6028/NIST.FIPS.200

[NISTIR 7298r2] Kissel R (ed.) (2013) *Glossary of Key Information Security Terms*. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Internal Report (NISTIR) 7298 Rev. 2, May 2013. https://doi.org/10.6028/NIST.IR.7298r2

[NISTIR 7966] Ylonen T, Turner P, Scarfone KA, Souppaya MP (2015) *Security of Interactive and Automated Access Management Using Secure Shell (SSH)*. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Internal Report (NISTIR) 7966, October 2015. https://doi.org/10.6028/NIST.IR.7966

[SP 800-30r1] Joint Task Force Transformation Initiative (2012) *Guide for Conducting Risk Assessments*. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-30 Rev. 1, September 2012. https://doi.org/10.6028/NIST.SP.800-30r1

[SP 800-34r1] Swanson MA, Bowen P, Phillips AW, Gallup D, Lynes D (2010) *Contingency Planning Guide for Federal Information Systems*. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-34 Rev. 1, May 2010 (Updated 11/11/2010). https://doi.org/10.6028/NIST.SP.800-34r1

[SP 800-37r1] Joint Task Force Transformation Initiative (2014) *Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach*. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-37 Rev. 1, February 2010 (Updated 6/5/2014). https://doi.org/10.6028/NIST.SP.800-37r1

[SP 800-39] Joint Task Force Transformation Initiative (2011) *Managing Information Security Risk: Organization, Mission, and Information System View*. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-39, March 2011. https://doi.org/10.6028/NIST.SP.800-39

[SP 800-40r3] Souppaya MP, Scarfone KA (2013) *Guide to Enterprise Patch Management Technologies*. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-40 Rev. 3, July 2013. https://doi.org/10.6028/NIST.SP.800-40r3

[SP 800-41r1] Scarfone KA, Hoffman P (2009) *Guidelines on Firewalls and Firewall Policy*. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-41 Rev. 1, September 2009. https://doi.org/10.6028/NIST.SP.800-41r1

[SP 800-45v2] Tracy MC, Jansen W, Scarfone KA, Butterfield J (2007) *Guidelines on Electronic Mail Security*. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-45 Version 2, February 2007. https://doi.org/10.6028/NIST.SP.800-45ver2

[SP 800-53r4] Joint Task Force Transformation Initiative (2015) *Security and Privacy Controls for Federal Information Systems and Organizations*. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53 Rev. 4, April 2013 (Updated 1/22/2015). https://doi.org/10.6028/NIST.SP.800-53r4

[SP 800-61r2] Cichonski PR, Millar T, Grance T, Scarfone KA (2012) *Computer Security Incident Handling Guide*. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-61 Rev. 2, August 2012. https://doi.org/10.6028/NIST.SP.800-61r2

[SP 800-63-3] Grassi PA, Garcia ME, Fenton JL (2017) *Digital Identity Guidelines*. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-63-3, June 2017 (Updated 12/1/2017). https://doi.org/10.6028/NIST.SP.800-63-3

[SP 800-70r4] Quinn SD, Souppaya MP, Cook MR, Scarfone KA (2018) *National Checklist Program for IT Products: Guidelines for Checklist Users and Developer*s. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-70 Rev. 4, February 2018. https://doi.org/10.6028/NIST.SP.800-70r4

[SP 800-88r1] Kissel RL, Regenscheid AR, Scholl MA, Stine KM (2014) *Guidelines for Media Sanitization*. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-88 Rev. 1, December 2014. https://doi.org/10.6028/NIST.SP.800-88r1

[SP 800-111] Scarfone KA, Souppaya MP, Sexton M (2007) *Guide to Storage Encryption Technologies for End User Devices*. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-111, November 2007. https://doi.org/10.6028/NIST.SP.800-111

[SP 800-115] Scarfone KA, Souppaya MP, Cody A, Orebaugh AD (2008) *Technical Guide to Information Security Testing and Assessment*. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-115, September 2008. https://doi.org/10.6028/NIST.SP.800-115

[SP 800-117] Quinn SD, Scarfone KA, Barrett MP, Johnson CS (2010) *Guide to Adopting and Using the Security Content Automation Protocol (SCAP) Version 1.0*. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-117, July 2010. https://doi.org/10.6028/NIST.SP.800-117

[SP 800-121r2] Padgette J, Bahr J, Holtmann M, Batra M, Chen L, Smithbey R, Scarfone KA (2017) *Guide to Bluetooth Security*. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-121 Rev. 2, May 2017. https://doi.org/10.6028/NIST.SP.800-121r2

[SP 800-125] Scarfone KA, Souppaya MP, Hoffman P (2011) *Guide to Security for Full Virtualization Technologies*. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-125, January 2011. https://doi.org/10.6028/NIST.SP.800-125

[SP 800-126r2] Waltermire DA, Quinn SD, Scarfone KA, Halbardier AM (2012) *The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.2*. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-126 Rev. 2, September 2011 (Updated 3/19/2012). https://doi.org/10.6028/NIST.SP.800-126r2

[SP 800-153] Souppaya MP, Scarfone KA (2012) *Guidelines for Securing Wireless Local Area Networks (WLANs)*. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-153, February 2012. https://doi.org/10.6028/NIST.SP.800-153

[SP 800-157] Ferraiolo H, Cooper DA, Francomacaro S, Regenscheid AR, Burr WE, Mohler J, Gupta S (2014) *Guidelines for Derived Personal Identity Verification (PIV) Credentials*. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-157, December 2014. https://doi.org/10.6028/NIST.SP.800-157