APPLE MACOS 12 (MONTEREY) SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

Version 1, Release 4

27 October 2022

Developed by Apple and DISA for the DOD

Trademark Information

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our users, and do not constitute or imply endorsement by the Defense Information Systems Agency (DISA) of any nonfederal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

Page

1. INTRODUCTION 1
1.1 Executive Summary 1
1.2 Authority 1
1.3 Vulnerability Severity Category Code Definitions 1
1.4 STIG Distribution 2
1.5 SRG Compliance Reporting 2
1.6 Document Revisions 2
1.7 Other Considerations 2
1.8 Product Approval Disclaimer 3

2. ASSESSMENT CONSIDERATIONS 4
2.1 Security Assessment Information 4

3. CONCEPTS AND TERMINOLOGY CONVENTIONS 5
3.1 Configuration Profiles 5
3.2 Deploying Configuration Profiles 5
3.3 Apple ID 6
3.4 Applications 6
3.4.1 Apple App Store 7
3.4.2 Calendar 7
3.4.3 Contacts 7
3.4.4 Reminders 7
3.4.5 Notes 7
3.4.6 AirDrop 7
3.4.7 AirPlay 8
3.4.8 Apple Push Notification Service 8
3.4.9 iCloud 8
3.4.10 OpenSSH 8

4. GENERAL SECURITY REQUIREMENTS 9
4.1 Software Updates 9
4.2 Common Access Card (CAC) 9

LIST OF TABLES

Page

Table 1-1: Vulnerability Severity Category Code Definitions 2

1. INTRODUCTION

1.1 Executive Summary

The Apple macOS 12 Security Technical Implementation Guide (STIG) provides security policy and configuration requirements for the use of Apple macOS 12 in the Department of Defense (DOD). Guidance in these documents applies only to Apple macOS 12 and related components on DOD systems and excludes any other components or software running on DOD systems. The Apple macOS 12 STIG is accompanied by supplemental guidance that should be referenced when attempting to implement the Smart Card Policy requirements listed in the STIG. Failure to reference this guidance could result in a total loss of access to the operating system. The Apple macOS 12 STIG presumes operation in an environment compliant with all applicable DOD guidance, especially concerning remote access and network infrastructure.

1.2 Authority

Department of Defense Instruction (DODI) 8500.01 requires that "all IT [information technology] that receives, processes, stores, displays, or transmits DOD information will be […] configured […] consistent with applicable DOD cybersecurity policies, standards, and architectures." The instruction tasks that DISA "develops and maintains control correlation identifiers (CCIs), security requirements guides (SRGs), security technical implementation guides (STIGs), and mobile code risk categories and usage guides that implement and are consistent with DOD cybersecurity policies, standards, architectures, security controls, and validation procedures, with the support of the NSA/CSS [National Security Agency/Central Security Service], using input from stakeholders, and using automation whenever possible." This document is provided under the authority of DODI 8500.01.

Although the use of the principles and guidelines in these SRGs/STIGs provides an environment that contributes to the security requirements of DOD systems, applicable NIST SP 800-53 cybersecurity controls must be applied to all systems and architectures based on the Committee on National Security Systems (CNSS) Instruction (CNSSI) 1253.

1.3 Vulnerability Severity Category Code Definitions

Severity Category Codes (referred to as CAT) are a measure of vulnerabilities used to assess a facility or system security posture. Each security policy specified in this document is assigned a Severity Category Code of CAT I, II, or III.

Table 1-1: Vulnerability Severity Category Code Definitions

Category	DISA Category Code Guidelines
CAT I	Any vulnerability, the exploitation of which will **directly and immediately** result in loss of Confidentiality, Availability, or Integrity.
CAT II	Any vulnerability, the exploitation of which **has a potential** to result in loss of Confidentiality, Availability, or Integrity.
CAT III	Any vulnerability, the existence of which **degrades measures** to protect against loss of Confidentiality, Availability, or Integrity.

1.4 STIG Distribution

Parties within the DOD and federal government's computing environments can obtain the applicable STIG from the DOD Cyber Exchange website at https://cyber.mil/. This site contains the latest copies of STIGs, SRGs, and other related security information. Those without a Common Access Card (CAC) that has DOD Certificates can obtain the STIG from https://public.cyber.mil/.

1.5 SRG Compliance Reporting

All technical NIST SP 800-53 requirements were considered while developing this STIG. Requirements that are applicable and configurable will be included in the final STIG. A report marked Controlled Unclassified Information (CUI) will be available for items that did not meet requirements. This report will be available to component Authorizing Official (AO) personnel for risk assessment purposes by request via email to: disa.stig_spt@mail.mil.

1.6 Document Revisions

Comments or proposed revisions to this document should be sent via email to the following address: disa.stig_spt@mail.mil. DISA will coordinate all change requests with the relevant DOD organizations before inclusion in this document. Approved changes will be made in accordance with the DISA maintenance release schedule.

1.7 Other Considerations

DISA accepts no liability for the consequences of applying specific configuration settings made on the basis of the SRGs/STIGs. It must be noted that the configuration settings specified should be evaluated in a local, representative test environment before implementation in a production environment, especially within large user populations. The extensive variety of environments makes it impossible to test these configuration settings for all potential software configurations.

For some production environments, failure to test before implementation may lead to a loss of required functionality. Evaluating the risks and benefits to a system's particular circumstances and requirements is the system owner's responsibility. The evaluated risks resulting from not

applying specified configuration settings must be approved by the responsible AO. Furthermore, DISA implies no warranty that the application of all specified configurations will make a system 100 percent secure.

Security guidance is provided for the DOD. While other agencies and organizations are free to use it, care must be given to ensure that all applicable security guidance is applied at both the device hardening level and the architectural level due to the fact that some settings may not be configurable in environments outside the DOD architecture.

1.8 Product Approval Disclaimer

The existence of a STIG does not equate to DOD approval for the procurement or use of a product.

STIGs provide configurable operational security guidance for products being used by the DOD. STIGs, along with vendor confidential documentation, also provide a basis for assessing compliance with cybersecurity controls/control enhancements, which supports system assessment and authorization (A&A) under the DOD Risk Management Framework (RMF). Department of Defense AOs may request available vendor confidential documentation for a product that has a STIG for product evaluation and RMF purposes from disa.stig_spt@mail.mil. This documentation is not published for general access to protect the vendor's proprietary information.

AOs have the purview to determine product use/approval in accordance with (IAW) DOD policy and through RMF risk acceptance. Inputs into acquisition or pre-acquisition product selection include such processes as:

- National Information Assurance Partnership (NIAP) evaluation for National Security Systems (NSS) (https://www.niap-ccevs.org/) IAW CNSSP #11.
- National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) (https://csrc.nist.gov/groups/STM/cmvp/) IAW Federal/DOD mandated standards.
- DOD Unified Capabilities (UC) Approved Products List (APL) (https://www.disa.mil/network-services/ucco) IAW DODI 8100.04.

2. ASSESSMENT CONSIDERATIONS

2.1 Security Assessment Information

DOD personnel or contractors should review this section when preparing for or conducting Apple macOS 12 security assessments. To perform an assessment, a reviewer requires access to the Apple macOS 12 systems subject to the review.

The STIG references multiple configuration profiles as part of the implementation guidance for the STIG requirements. These configuration profiles should be validated by the organization prior to implementation on the system and are not part of the assessment phase.

3. CONCEPTS AND TERMINOLOGY CONVENTIONS

3.1 Configuration Profiles

A configuration profile is an XML file that applies configuration information to an Apple macOS 12 system. The use of multiple profiles (e.g., Passcode Policy, Restrictions, Login Window, etc.) allows for flexible updates without affecting standard configurations. If a configuration profile is removed from the system, all the settings defined by the profile are removed.

Several configuration profiles are included with the STIG:

- Apple macOS 12 STIG Restrictions Policy (used to apply generic restrictions)
- Apple macOS 12 STIG Passcode Policy (used to enforce password requirements)
- Apple macOS 12 STIG Login Window Policy (used to enforce login window requirements)
- Apple macOS 12 STIG Test Smart Card Policy (used to verify the correct function of MFA tokens)
- Apple macOS 12 STIG Smart Card Policy (used to enforce smart card requirements)
- Apple macOS 12 STIG Custom Policy (used to apply other requirements)

These configuration profiles include settings for STIG requirements as indicated by the Fix action.

Prior to implementation, organizations should first check that each configuration profile contains the correct content. Once content validation is complete, the organization should import the configuration profiles into the Apple macOS 12 management tool of their choice and sign each profile to ensure integrity and nonrepudiation of source. The signed profiles can then be deployed as appropriate.

3.2 Deploying Configuration Profiles

There are several ways to deploy configuration profiles depending on the use case, quantity of Apple macOS 12 systems, and workflow. macOS, like iOS, is managed using Configuration Profiles. Configuration Profiles are XML documents containing settings in the form of key/value pairs.

For basic information about using configuration profiles to standardize settings on Mac computers, visit https://support.apple.com/guide/mac-help/configuration-profiles-standardize-settings-mh35561/mac.

For information on Configuration Profiles for macOS, see the Configuration Profile Reference (https://developer.apple.com/business/documentation/Configuration-Profile-Reference.pdf) and the Deployment Reference (https://support.apple.com/guide/deployment/welcome/web).

3.3 Apple ID

An Apple ID is a user's username for the iTunes Store, App Store, iCloud, and other Apple services. In the DOD, an Apple ID is needed on an Apple macOS 12 system for two purposes:

- Downloading and updating App Store apps and Apple macOS 12 maintenance content
- Downloading content from the iTunes Store

The use of Apple IDs does not pose a significant IA risk when applications containing DOD-sensitive information are managed appropriately. Apple IDs are not designed to be managed by an organization, and no tools are provided to accomplish such administration. DOD organizations should avoid issuing organizationally generated Apple IDs, including custom email addresses, just for the purpose of Apple macOS 12 system administration.

To obtain an Apple ID, the user must agree to Apple's Terms and Conditions. DOD cannot serve as a proxy for a user's acceptance of the Terms and Conditions. Users can create an Apple ID on the Apple macOS 12 system or online at https://appleid.apple.com. An Apple knowledge base article at https://support.apple.com/kb/HT2534 explains how to create an Apple ID without a credit card. It is recommended that each user use his or her primary DOD email address for the Apple ID. However, it is acceptable to use a previously created personal Apple ID on Government-furnished Apple macOS 12 systems, provided that this ID is not a member of a Family Sharing group.

Apple IDs are protected by passcodes to prevent unauthorized use. The Apple ID passcodes are distinct from the Apple macOS 12 system unlock passcode. Organizations have no technical means to reset passcodes or enforce password complexity rules on Apple ID passcodes. Users should be encouraged to select Apple ID passcodes within DOD guidelines. For example, the following rules should be used:

- Be at least 15 characters long
- Contain at least one uppercase alphabetic character
- Have at least one lowercase alphabetic character
- Have at least one numeric character
- Have at least one special character (e.g., ~ ! @ # $ % ^ & * ( ) _ + = - ‘ [ ] / ? > <)

Apple sends clear-text messages containing the name of the Apple macOS 12 system to the Apple ID email address. For this reason, Apple macOS 12 system names should not reveal a DOD affiliation, personally identifiable information (PII), or other sensitive information.

3.4 Applications

This section will discuss the Apple App Store and applications bundled with Apple macOS 12. Disabled apps should be evaluated against mission needs and should only be allowed if approved by the AO.

3.4.1 Apple App Store

The App Store is an application distribution platform for commercially available Apple macOS 12 apps. Apps in the App Store are reviewed by Apple and digitally signed for use on Apple macOS 12 systems. The App Store application on the Apple macOS 12 system must be enabled to install and update commercially available apps, even if the organization's preferred method is to obtain apps through other means. To avoid installing unauthorized apps, users should be discouraged from obtaining apps directly from the App Store. Not all of the applications in the App Store are appropriate for use on Government-furnished equipment (GFE). DOD organizations must establish their own app vetting and approval processes to determine which applications are appropriate for their use cases.

Applications purchased with an Apple ID are available to other Apple macOS 12 systems configured with the same Apple ID. Previously purchased applications will not automatically download on a new device when an existing Apple ID is first associated with it. Users should be discouraged from subsequently synchronizing applications across personally owned and Government-furnished Apple macOS 12 systems. To prevent applications acquired for personal use from automatically downloading on a Government-furnished Apple macOS 12 system, the user should turn off "Automatically download apps purchased on other Macs" from the App Store setting pane in System Preferences.

3.4.2 Calendar

The Calendar app is disabled, per the STIG. This app is disabled due to connectivity to iCloud, which cannot be adequately controlled.

3.4.3 Contacts

The Contacts app is disabled, per the STIG. This app is disabled due to connectivity to iCloud, which cannot be adequately controlled.

3.4.4 Reminders

The Reminders app is disabled, per the STIG. This app is disabled due to connectivity to iCloud, which cannot be adequately controlled.

3.4.5 Notes

The Notes app is disabled, per the STIG. This app is disabled due to connectivity to iCloud, which cannot be adequately controlled.

3.4.6 AirDrop

The AirDrop service is disabled, per the STIG, and is not approved for use in the DOD.

3.4.7 AirPlay

AirPlay allows a user to wirelessly stream content from the Apple macOS 12 system to hardware that supports the AirPlay protocol, such as Apple TV. The contents of AirPlay streams are protected by multiple security protocols. To ensure that users only send content to the intended Apple TV, the Apple TV should be configured to use an onscreen code. Users will need to enter the code each time they want to transmit from their Apple macOS 12 system to the Apple TV.

3.4.8 Apple Push Notification Service

Apple Push Notification Service (APNS) is an encrypted and authenticated communication tool allowed for use in the DOD.

3.4.9 iCloud

Currently, the Apple iCloud service does not have FedRAMP certification. Its use in the DOD is not authorized on Apple macOS 12 systems.

3.4.10 OpenSSH

The implementation of OpenSSH that is included with macOS does not use a FIPS 140-2 validated cryptographic module. Organizations can reference FIPS 140-2 Annex A for a list of FIPS 140-2 approved algorithms that can be configured for use with OpenSSH (https://csrc.nist.gov/csrc/media/publications/fips/140/2/final/documents/fips1402annexa.pdf). OpenSSH should not be used unless approved by the AO.

4. GENERAL SECURITY REQUIREMENTS

4.1 Software Updates

Keeping Apple macOS 12 up to date ensures that it has the latest enhancements and security controls in place. This STIG requires that all updates come from an approved source. Apple is considered a DOD-approved source. Apple-provided updates can be installed on Apple macOS 12 systems when available, with the exception that users should not install the next major release until authorized to do so. This STIG assumes that the latest version of Apple macOS 12 is installed.

4.2 Common Access Card (CAC)

CACs include embedded private keys to perform several functions, such as digitally signing email, decrypting email, authenticating to DOD public key-enabled websites, and authenticating to virtual private network (VPN) concentrators. In Apple macOS 12, hard token (smart card) transactions are handled by third-party applications as well as the native set of components.

Any smart card that supports the personal identity verification (PIV) standard is supported natively by Apple macOS 12. Access to smart card items is possible using the keychain interface. Applications can install additional drivers for smart cards that are not natively supported. Smart card certificates are automatically added to a user's keychain when a smart card is inserted. Smart card certificates can be listed using the "list-smartcards" or "export-smartcard" commands. Keychain Access GUI cannot be used to manipulate or list these certificates.

To fulfill the functions performed with CACs, there are a variety of applications that have CAC support (for example: DOD PKI-enabled web browser, S/MIME email client, and VPN). CAC readers are available for Apple macOS 12 systems.