Center for Internet Security®

CIS Apple iOS 10 Benchmark

v1.0.0 - 01-25-2017

Table of Contents

Overview

This document, *Security Configuration Benchmark for Apple iOS 10*, provides prescriptive guidance for establishing a secure configuration posture for the Apple iOS version 10. This guide was tested against the Apple iOS 10 and the Apple Configurator v2.3. This benchmark covers the Apple iOS 10 and all hardware devices on which this iOS is supported. As of the publication of this guidance, mobile devices supported by iOS 10 include the following:

- iPhone 5 and later
- iPad Pro (9.7" and 12.9") and later
- iPad Air and later
- iPad 4th generation
- iPad mini 2 and later
- iPod touch (6th generation) and later

In determining recommendations, the current guidance treats all iOS mobile device platforms as having the same use cases and risk/threat scenarios. In all but a very few cases, configuration steps, default settings, and benchmark recommended settings are identical regardless of hardware platform; for the few cases where variation exists, the benchmark notes the difference within the respective section. To obtain the latest version of this guide, please visit http://benchmarks.cisecurity.org. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

Intended Audience

This document is intended for system and application administrators, security specialists, auditors, help desk, end users, and platform deployment personnel who plan to use, develop, deploy, assess, or secure solutions that incorporate the Apple iOS 10.

Consensus Guidance

This benchmark was created using a consensus review process comprised of subject matter experts. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

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

Typographical Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
`Stylized Monospace font`	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
Monospace font	Used for inline code, commands, or examples. Text should be interpreted exactly as presented.
<italic font in brackets>	Italic texts set in angle brackets denote a variable requiring substitution for a real value.
Italic font	Used to denote the title of a book, article, or other publication.
Note	Additional information or caveats

Scoring Information

A scoring status indicates whether compliance with the given recommendation impacts the assessed target's benchmark score. The following scoring statuses are used in this benchmark:

Scored

Failure to comply with "Scored" recommendations will decrease the final benchmark score. Compliance with "Scored" recommendations will increase the final benchmark score.

Not Scored

Failure to comply with "Not Scored" recommendations will not decrease the final benchmark score. Compliance with "Not Scored" recommendations will not increase the final benchmark score.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1 - Apple iOS 10**

  Items in this profile apply to Apple iOS 10 and intend to:

  - Be practical and prudent.
  - Provide a clear security benefit.
  - Not inhibit the utility of the technology beyond acceptable means.

- **Level 2 - Apple iOS 10**

  This profile extends the "Level 1 - Apple iOS 10" profile. Items in this profile exhibit one or more of the following characteristics:

  - Intended for environments or use cases where security is paramount.
  - Act as defense in depth measures.
  - May negatively inhibit the utility or performance of the technology.

Acknowledgements

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

Editor
Paul Campbell
Mike de Libero , *MDE Development, Inc.*

Contributor
Will Strafach
Jordan Rakoske

Recommendations

1 User Interface Settings

This section provides guidance on the secure configuration of iOS mobile devices using the device user interface.

1.1 System Settings

This section provides guidance on the secure configuration of system settings.

1.1.1 Ensure 'Software Update' returns 'Your software is up to date." (Not Scored)

Profile Applicability:

- Level 1 - Apple iOS 10

Description:

This control ensures that the iOS version installed is current.

Rationale:

Operating system updates often include critical security fixes that reduce the probability of an attacker exploiting the device.

Audit:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Software Update`.
4. Confirm that "Your software is up to date" is returned.

Remediation:

Using Over-the-Air Update:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Software Update`.
4. iOS will automatically check for available updates. If an update is available, tap `Download and Install` when prompted.
5. Do not power off the device until the update is finished.

Using iTunes:

1. Connect the device to the computer.
2. Open iTunes.
3. Click on the device under "Devices" in the source list.
4. Click on `Check for Update`.

5. Click `Download and Install`.
6. Do not disconnect the device until the update is finished.

Default Value:

N/A; an iOS mobile device ships with whichever version of the iOS was current when it was manufactured.

References:

1. iOS: How to update your iPhone, iPad, or iPod touch. Available: http://support.apple.com/kb/HT4623
2. iOS: How to back up and restore your content. Available: http://support.apple.com/kb/HT1766

1.1.2 Ensure 'Passcode Lock' is 'Enabled' (Not Scored)

Profile Applicability:

- Level 1 - Apple iOS 10

Description:

This control determines whether a passcode/password is required before allowing access to the device via the touch screen. It is recommended that a passcode/password be set.

Rationale:

Requiring a passcode/password to unlock the device helps prevent unauthorized access to the device and increases the effort required to use the device or access data stored on it.

Audit:

1. Tap `Settings`.
2. Tap "`Passcode`" or "`Touch ID & Passcode`."
3. Confirm that Passcode Lock is turned on.

Remediation:

1. Tap `Settings`.
2. Tap "`Passcode`" or "`Touch ID & Passcode`."
3. Tap `Turn Passcode On`.
4. Tap in a passcode.
5. Tap `Next`.
6. Tap in the same passcode.
7. Tap `Next`.

Default Value:

Passcode is OFF

1.1.3 Ensure 'Auto-lock' is set to '2 minutes or less' (Not Scored)

Profile Applicability:

- Level 1 - Apple iOS 10

Description:

This control defines the number of minutes the device can be inactive before the display is locked. The recommended setting is 2 minutes or less.

Rationale:

Automatically locking the device after a short period of inactivity reduces the probability of an attacker accessing the device without entering a password.

Audit:

1. Tap `Settings`.
2. Tap `Display & Brightness`.
3. Review the Auto-lock interval and confirm it is set to 2 minutes or less.

Remediation:

1. Tap `Settings`.
2. Tap `Display & Brightness`.
3. Tap `Auto-Lock`.
4. Tap the value to set the Auto-lock interval at `2 Minutes` or less.

Default Value:

2 minutes

1.1.4 Ensure 'Erase Data' is set to 'Enabled' (Not Scored)

Profile Applicability:

- Level 2 - Apple iOS 10

Description:

This control determines whether the device will automatically wipe its contents after excessive (10) failed passcode attempts. It is recommended that this feature be enabled.

Rationale:

Excessive passcode failures typically indicate that the device is out of the physical control of its owner. Upon such an event, erasing data on the phone will help to ensure the confidentiality of information stored on the device is protected when facing a novice attacker.

Audit:

1. Tap `Settings`.
2. Tap "`Passcode`" or "`Touch ID & Passcode`."
3. Enter current passcode as prompted.
4. Confirm that Erase Data is turned on.

Remediation:

1. Tap `Settings`.
2. Tap "`Passcode`" or "`Touch ID & Passcode`."
3. Enter current passcode as prompted.
4. Turn on Erase Data.
5. Tap `Enable` on confirmation dialog.

Default Value:

Erase Data is OFF (Maximum number of failed attempts is not configured)

1.1.5 Ensure 'Access on Lock Screen' is 'Disabled' for Control Center (Not Scored)

Profile Applicability:

- Level 1 - Apple iOS 10

Description:

This control disables access to the Control Center on the Lock Screen.

Rationale:

Disabling access to the Control Center on the Lock Screen can potentially mitigate future variations of iOS lock screen bypass exploits that may be possible for attacker who have gained physical access to the device.

Audit:

1. Tap `Settings`.
2. Tap `Control Center`.
3. Confirm that Access on Lock Screen is turned off.

Remediation:

1. Tap `Settings`.
2. Tap `Control Center`.
3. Turn off Access on Lock Screen.

Default Value:

Access on Lock Screen: On

1.1.6 Ensure 'Ask to Join Networks' is 'Disabled' (Not Scored)

Profile Applicability:

- Level 2 - Apple iOS 10

Description:

This control addresses whether the device will display a list of all available Wi-Fi networks that the user can choose from when the device is trying to access the Internet and is not in range of a Wi-Fi network it has previously used. It is recommended that "Ask to Join Networks" be turned off.

Rationale:

Requiring the user to manually configure and join a Wi-Fi network reduces the risk of inadvertently joining a similarly named yet untrusted network (i.e. "default" vice "defualt").

Audit:

1. Tap `Settings`.
2. Tap `Wi-Fi`.
3. Confirm that Ask to Join Networks is turned off.

Remediation:

1. Tap `Settings`.
2. Tap `Wi-Fi`.
3. Turn off Ask to Join Networks (see note below).

Note: Wi-Fi must be turned on for the above Wi -Fi configuration option to appear.

1.1.7 Ensure 'Auto-Join' is set to 'Disabled' for all Wi-Fi networks (Not Scored)

Profile Applicability:

- Level 2 - Apple iOS 10

Description:

Enabling Wi-Fi Auto-Join for a Wi-Fi network configures the device to remember the network and login information and automatically reconnect to that Wi-Fi network whenever the device is in range. It is recommended that Wi-Fi Auto-Join be turned off for all network connections where security is paramount.

Rationale:

Auto-Join may expose credentials at unexpected times and locations (e.g., if forms-based authentication occurs over unencrypted HTTP, or a spoofed SSID is encountered), and for Wi-Fi networks that require HTTP(S) forms authentication, this feature will cause credentials to persist on disk, potentially placing the confidentiality of the credentials at risk if physical custody of the device is lost.

Audit:

1. Tap `Settings`.
2. Tap `Wi-Fi`.
3. From the Choose a Network list, locate the network SSID and tap the Detail Disclosure button next to the network to review.
4. Confirm that Auto-Join is turned off.
5. Repeat steps 3 and 4 for each network SSID.

Remediation:

1. Tap `Settings`.
2. Tap `Wi-Fi`.
3. From the Choose a Network list, locate the network SSID and tap the Detail Disclosure button next to the network to change.
4. Turn off Auto-Join (see note below).
5. Repeat steps 3 and 4 for each network SSID.

Note: This feature is primarily applicable to the automatic joining of subscription Wi-Fi networks. Wi-Fi must be turned on and the Wi-Fi network must be in range for it to appear in the list of available networks to configure. The Wi-Fi network must require network

login credentials and must be remembered or currently connected for the Auto-Join option to be present.

References:

1. iPhone, iPad, iPod touch: Understanding subscription Wi-Fi networks. Available: http://support.apple.com/kb/HT3867

1.1.8 Ensure 'AirDrop Discoverability' is set to 'Disabled' (Not Scored)

Profile Applicability:

- Level 2 - Apple iOS 10

Description:

This setting keeps your device from being discoverable to everyone, including contacts.

This setting only applies to the following devices:

- iPhone 5 or later
- iPad (4th generation)
- iPad mini (1st generation) or later
- iPad Air (1st generation) or later
- iPod Touch (5th generation) or later

Rationale:

Turning off AirDrop discoverability prevents the device from making itself discoverable to other devices for AirDrop functionality. It is recommended to restrict device discoverability when this functionality is not needed.

Audit:

1. Swipe up from the bottom of the home screen to display the Control Center.
2. Confirm that the text next to the AirDrop symbol states simply "AirDrop" (and not AirDrop: Everyone or AirDrop: Contacts Only).

Remediation:

1. Swipe up from the bottom of the home screen to display the Control Center.
2. Tap the AirDrop field at the bottom of the Control Center panel.
3. Tap `Off` on the menu dialog.

Default Value:

AirDrop: Off

References:

1. http://support.apple.com/kb/HT5887

1.1.9 Ensure 'Wi-Fi' is set to 'Disabled' when not necessary (Not Scored)

Profile Applicability:

- Level 2 - Apple iOS 10

Description:

This configuration item determines whether the iOS device uses local Wi-Fi networks to connect to the Internet and other networks. It is recommended that Wi-Fi be disabled when not needed or when security is paramount.

Rationale:

Disabling the Wi-Fi interface reduces the remote attack surface of the device.

Audit:

1. Tap `Settings`.
2. Tap `Wi-Fi`.
3. Confirm that Wi-Fi is turned off.

Remediation:

1. Tap `Settings`.
2. Tap `Wi-Fi`.
3. Turn off Wi-Fi.

1.1.10 Ensure 'VPN' is set to 'Disabled' when not necessary (Not Scored)

Profile Applicability:

- Level 1 - Apple iOS 10

Description:

iOS devices can natively connect to VPNs that use the L2TP over IPSec, PPTP, or Cisco IPSec protocols. VPN connections can be established over both Wi-Fi and cellular data network connections. It is recommended that VPN connections be disabled when not in use.

Rationale:

If the device has a VPN connection configured, it should only be turned on when VPN access is required. If the VPN is left on, the user may not be mindful of the nature of the information they are transmitting on the network. Additionally, malicious or exploited iPhone applications may access VPN resources.

Audit:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN`.
4. Confirm that VPN is turned off.

Remediation:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN`.
4. Turn off VPN if turned on.

1.1.11 Ensure 'Bluetooth' is set to 'Disabled' when not necessary (Not Scored)

Profile Applicability:

- Level 1 - Apple iOS 10

Description:

Bluetooth allows devices to connect wirelessly to headsets, car kits, and other accessories for various Bluetooth profile functionality. It is recommended that Bluetooth be disabled when not in use.

Rationale:

Disabling Bluetooth when not needed reduces the remote attack surface of the device and prevents discovery of and connection to Bluetooth services.

Audit:

1. Tap `Settings`.
2. Tap `Bluetooth`.
3. Confirm that Bluetooth is turned off.

Remediation:

1. Tap `Settings`.
2. Tap `Bluetooth`.
3. Turn off Bluetooth.

1.1.12 Ensure 'Personal Hotspot' is set to 'Disabled' when not necessary (Not Scored)

Profile Applicability:

- Level 2 - Apple iOS 10

Description:

Personal Hotspot allows certain iOS devices with cellular data connections to be configured to share an active Cellular Data connection via Wi-Fi, Bluetooth, or USB (see Note). It is recommended that Personal Hotspot be disabled when not needed or where security is paramount.

Rationale:

Disabling the Personal Hotspot makes the hotspot unavailable to unauthorized access attempts and reduces the overall remote attack surface of the device.

Audit:

1. Tap `Settings`.
2. Tap `Cellular` or `Cellular Data`, as applicable.
3. Check if `Personal Hotspot` is present.
   a) If present,
      i. Tap `Personal Hotspot`.
      ii. Confirm that `Personal Hotspot` is turned off.
   b) Alternatively, if `Set Up Personal Hotspot` is present, then Personal Hotspot is not configured.

Remediation:

1. Tap `Settings`.
2. Tap `Cellular` or `Cellular Data`, as applicable.
3. Tap `Personal Hotspot`.
4. Turn off Personal Hotspot.

1.1.13 Ensure 'Location Services' is set to 'Disabled' (Not Scored)

Profile Applicability:

- Level 2 - Apple iOS 10

Description:

Location Services allows applications such as Maps, Internet, and Camera to gather and use data indicating the user's location. It is recommended that Location Services be disabled in environments where security is paramount.

Rationale:

Disabling location services reduces the capability of an attacker to determine or track the user's location via websites, locally installed applications or other means.

Audit:

1. Tap `Settings`.
2. Tap `Privacy`.
3. Tap `Location Services`.
4. Confirm that Location Services is turned off.

Remediation:

1. Tap `Settings`.
2. Tap `Privacy`.
3. Tap `Location Services`.
4. Turn off Location Services.
5. Tap `Turn off` on confirmation dialog.

Note: Location services can also be disabled/enabled on a per-app basis within the Location Services configuration menu referenced above.

1.1.14 Ensure 'Notifications' are set to 'Disabled' on Lock Screen (Not Scored)

Profile Applicability:

- Level 2 - Apple iOS 10

Description:

This setting prevents notifications from any source from being displayed when the iOS device is passcode locked. It is recommended that View in Lock Screen be disabled for all apps for which message confidentiality is desired and in environments where security is paramount.

Rationale:

Parties who do not know the passcode lock should not have read access to the notifications displayed by the device.

Audit:

1. Tap `Settings`.
2. Tap Touch ID & Passcode or Passcode.
3. In the ALLOW ACCESS ON LOCK SCREEN section, confirm that Notifications View is turned off.

Remediation:

1. Tap `Settings`.
2. Tap Touch ID & Passcode or Passcode.
3. In the ALLOW ACCESS ON LOCK SCREEN section, turn off "Notifications".

1.1.15 Ensure 'Automatic Downloads' of 'App Updates' is set to 'Enabled' (Not Scored)

Profile Applicability:

- Level 1 - Apple iOS 10

Description:

This control ensures that the application software remains current via automatic download and installation of app updates over-the-air.

Rationale:

App updates often include critical security fixes that reduce the probability of an attacker exploiting vulnerabilities in apps.

Audit:

1. Tap `Settings`.
2. Tap `iTunes & App Store`.
3. Confirm that Updates is turned on in the Automatic Downloads configuration list.

Remediation:

1. Tap `Settings`.
2. Tap `iTunes & App Store`.
3. Turn on Updates in the Automatic Downloads configuration list.

Default Value:

Updates: Off

1.1.16 Ensure 'Find My iPhone/iPad' is set to 'Enabled' (Not Scored)

Profile Applicability:

- Level 1 - Apple iOS 10

Description:

This control enables the remote tracking, remote wiping, remote custom message display, and Activation Lock features of the iOS device.

Rationale:

Enabling Find my iPhone/iPad enables the abilities both to locate the device via the Find My iPhone iCloud application or iOS app and to display a custom message with phone number on the Lock screen, as well as prevents the taking of key actions with the iOS device without the entry of the associated Apple ID password, including preventing the erasure of device content and settings from the device via the Settings app, and the restoring of the device, through the Activation Lock feature.

Audit:

1. Tap `Settings`.
2. Tap `iCloud`.
3. Confirm that Find My iPhone or Find my iPad, as applicable, is turned on.

Remediation:

1. Tap `Settings`.
2. Tap `iCloud`.
3. Turn on Find My iPhone or Find my iPad, as applicable.
4. Tap `OK` on confirmation dialog.

Default Value:

Off

References:

1. Find My iPhone, iPad and Mac. Available: http://www.apple.com/icloud/find-my-iphone.html
2. iCloud: Find My iPhone Activation Lock in iOS 7+. Available: http://support.apple.com/kb/ht5818

1.1.17 Ensure 'iCloud Drive' is set to 'Disabled' (Not Scored)

Profile Applicability:

- Level 2 - Apple iOS 10

Description:

This control determines whether iCloud Drive is currently enabled. iCloud Drive is a service provided through Apple's iCloud to store and synchronize documents across multiple devices.

Rationale:

The use of iCloud Drive could compromise the confidentiality of information. Whereas strong controls like password policy enforcement may exist upon the device, a user's iCloud account may be protected by a weak password or one that is shared with others. Thus it is recommended to disable iCloud Drive for environments containing sensitive information.

Audit:

1. Tap `Settings`.
2. Tap `iCloud`.
3. Tap `iCloud Drive`.
4. Confirm that iCloud Drive is turned off.

Remediation:

1. Tap `Settings`.
2. Tap `iCloud`.
3. Tap `iCloud Drive`.
4. Tap to turn off iCloud Drive.

1.1.18 Ensure 'Erase all Content and Settings' is `Executed` prior to releasing device control (Not Scored)

Profile Applicability:

- Level 1 - Apple iOS 10

Description:

This control effectively erases all data, including accounts, from the device's internal storage by securely discarding the block storage encryption key from Effaceable Storage, rendering all data unreadable. Device contents should be securely erased before the device is placed outside of the owner's control.

Rationale:

In normal operations, deleting data on an iOS device renders it inaccessible through the user interface but the data is not erased from the device. Erasing stored data by securely discarding the block storage encryption key before returning, recycling, disposing of, or otherwise placing a device out of the user's control reduces the probability of an attacker subsequently accessing confidential information previously stored on the device.

Audit:

To verify that the iPhone disk has been overwritten, it is necessary to install a warranty-voiding forensics recovery toolkit that is not within the scope of this document. Please review the reference for more information.

Remediation:

1. Make sure iMessage is disabled before wiping the device, by doing the following:
    1. Tap `Settings`
    2. Tap `Messages`
    3. Switch `iMessage` to the off position
2. Tap `Settings`.
3. Tap `General`.
4. Tap `Reset`.
5. Tap `Erase All Contents and Settings`.
6. If passcode is configured on device, enter passcode when prompted.

References:

1. iPhone and iOS Forensics: Investigation, Analysis and Mobile Security for Apple iPhone, iPad and iOS Devices. Available: http://textbooks.elsevier.com/web/product_details.aspx?isbn=9781597496599

1.1.19 Ensure 'SIM Passcode' has been 'Set' (Not Scored)

Profile Applicability:

- Level 2 - Apple iOS 10

Description:

This control protects from the user from having a SIM card stolen and used on another device.

Rationale:

By default it is possible for a malicious user to remove a SIM card from one phone and use it in another phone. This allows for messages, phone calls and other personal correspondence to be intercepted. Adding a password to the SIM card defends against this attack by requiring a user to enter in a password before using the SIM card.

Audit:

1. Tap `Settings`.
2. Tap `Phone`.
3. Tap `SIM PIN`.
4. Confirm that SIM PIN, is turned on.

Remediation:

1. Tap `Settings`.
2. Tap `Phone`.
3. Tap `SIM PIN`.
4. Turn on SIM PIN.
5. Enter in PIN.

Default Value:

Off

1.2 Safari Settings

This section provides guidance on the secure configuration of settings related to the Safari application on the iOS mobile devices.

1.2.1 Ensure 'JavaScript' is set to 'Disabled' (Not Scored)

Profile Applicability:

- Level 2 - Apple iOS 10

Description:

This control disables JavaScript functionality which lets web programmers control elements of the page—for example, a page that uses JavaScript might display the current date and time or cause a linked page to appear in a new pop-up page. It is recommended that JavaScript be disabled in environments where security is paramount.

Rationale:

JavaScript should only be enabled before browsing trusted sites.

Audit:

1. Tap `Settings`.
2. Tap `Safari`.
3. Tap `Advanced`.
4. Confirm that JavaScript is turned off.

Remediation:

1. Tap `Settings`.
2. Tap `Safari`.
3. Tap `Advanced`.
4. Turn off JavaScript.

1.2.2 Ensure 'Fraudulent Website Warning' is set to 'Enabled' (Not Scored)

Profile Applicability:

- Level 1 - Apple iOS 10

Description:

Enabling Fraudulent Website Warning configures Safari to display a warning and prevent the loading of the page when an attempt is made to visit a potentially fraudulent Internet site. It is recommended that the Fraudulent Website Warning feature be enabled.

Rationale:

Enabling a warning can help you avoid accidently visiting some known phishing and other fraudulent sites covered by this feature.

Audit:

1. Tap `Settings`.
2. Tap `Safari`.
3. Confirm that Fraudulent Website Warning is enabled.

Remediation:

1. Tap `Settings`.
2. Tap `Safari`.
3. Turn on Fraudulent Website Warning.

1.2.3 Ensure 'Auto Fill for Contact Information' is set to 'Disabled' (Not Scored)

Profile Applicability:

- Level 2 - Apple iOS 10

Description:

Auto Fill configures the browser to remember information entered into common forms in order to automate the completion of later forms.

Rationale:

Disabling AutoFill can help avoid the storage of sensitive information locally on the device, as well as reduces the likelihood of automated unauthorized use of information on a site in the event unauthorized access is gained to the device.

Audit:

1. Tap `Settings`.
2. Tap `Safari`.
3. Tap `Passwords & AutoFill`.
4. Confirm that AutoFill is turned off for the "Use Contact Info" setting.

Remediation:

1. Tap `Settings`.
2. Tap `Safari`.
3. Tap `AutoFill`.
4. Turn off AutoFill for the "Use Contact Info" setting.

1.2.4 Ensure 'Auto Fill for Names and Passwords' is set to 'Disabled' (Not Scored)

Profile Applicability:

- Level 2 - Apple iOS 10

Description:

Auto Fill configures the browser to remember information entered into common forms in order to automate the completion of later forms.

Rationale:

Disabling AutoFill can help avoid the storage of sensitive credentials locally on the device, as well as reduces the likelihood of automated unauthorized use of credentials on a site in the event unauthorized access is gained to the device.

Audit:

1. Tap `Settings`.
2. Tap `Safari`.
3. Tap `AutoFill`.
4. Confirm that AutoFill is turned off for the "Names and Passwords" item.

Remediation:

1. Tap `Settings`.
2. Tap `Safari`.
3. Tap `AutoFill`.
4. Turn off AutoFill for the "Names and Passwords" item.

1.2.5 Ensure 'Auto Fill for Credit Card Information' is set to 'Disabled' (Not Scored)

Profile Applicability:

- Level 2 - Apple iOS 10

Description:

Auto Fill configures the browser to remember information entered into common forms in order to automate the completion of later forms.

Rationale:

Disabling AutoFill can help avoid the storage of sensitive information locally on the device, as well as reduces the likelihood of automated unauthorized use of information on a site in the event unauthorized access is gained to the device.

Audit:

1. Tap `Settings`.
2. Tap `Safari`.
3. Tap `AutoFill`.
4. Confirm that AutoFill is turned off for the "Credit Cards" setting.

Remediation:

1. Tap `Settings`.
2. Tap `Safari`.
3. Tap `AutoFill`.
4. Turn off AutoFill for the "Credit Cards" setting.

Default Value:

Auto Fill for Credit Card Information: Off

1.2.6 Ensure 'Saved Password Information' is routinely 'Deleted' (Not Scored)

Profile Applicability:

- Level 2 - Apple iOS 10

Description:

The Safari configuration provides a repository to store information, including website username and password details, that can be to support Safari Auto Fill capability. Saved password information is stored in the device keychain and/or iCloud keychain. The Safari configuration interface requires the input of the device passcode prior to granting access to stored website password details; website and user name details can be viewed without the additional passcode prompt.

Rationale:

Deleting saved website credential information from the browser configuration helps prevent unauthorized access to such sensitive data in the event unauthorized access is gained to the device. Note that if you have enabled iCloud Keychain, you may be deleting credentials that are used by other devices.

Audit:

1. Tap `Settings`.
2. Tap `Safari`.
3. Tap `AutoFill`.
4. Tap `Passwords`.
5. Confirm that no websites are listed.

Remediation:

1. Tap `Settings`.
2. Tap `Safari`.
3. Tap `AutoFill`.
4. Tap `Passwords`.
5. Tap `Edit` on the Navigation bar.
6. Tap the listed website credential entries to select them for deletion.
7. Tap `Delete` on the Navigation bar.
8. Tap `Delete` to confirm on the Action Sheet dialog.
9. Enter the iOS device passcode as prompted.
10. Repeat steps 6 through 9 for any remaining password entries.

Default Value:

Password Information: Not saved

1.2.7 Ensure 'Saved Credit Cards' contains no entries (Not Scored)

Profile Applicability:

- Level 2 - Apple iOS 10

Description:

The Safari configuration provides a repository to store information, including Credit Card details, that can be to support Safari Auto Fill capability. Saved credit card information is stored in the device keychain and/or iCloud keychain. The Safari configuration interface requires the input of the device passcode prior to granting access to stored Credit Card details.

Rationale:

Deleting saved Credit Card information from the browser configuration helps prevent unauthorized access to such sensitive data in the event unauthorized access is gained to the device.

Audit:

1. Tap `Settings`.
2. Tap `Safari`.
3. Tap `AutoFill`.
4. Tap `Saved Credit Cards`.
5. Confirm that no credit card details are listed.

Remediation:

1. Tap `Settings`.
2. Tap `Safari`.
3. Tap `AutoFill`.
4. Tap `Saved Credit Cards`.
5. Tap `Edit` on the Navigation bar.
6. Tap the listed credit card entries to select them for deletion.
7. Tap `Delete` on the Navigation bar.
8. Tap `Delete` to confirm on the Action Sheet dialog.
9. Enter the iOS device passcode as prompted.
10. Repeat steps 6 through 9 for any remaining credit card entries.

Default Value:

Credit Card Information: Not saved

1.2.8 Ensure 'Private Browsing' is used when necessary (Not Scored)

Profile Applicability:

- Level 2 - Apple iOS 10

Description:

Enabling Private Browsing for a browser session prevents tracking of history of web pages visited, searches performed, and (if configured) certain AutoFill information.

Rationale:

Enabling Private Browsing can protect certain private information and block some websites from tracking browser activity.

Audit:

1. Tap the Safari app to launch it.
2. Observe if the top and bottom Safari menu bars are dark gray instead of the usual white color.
3. Tap the Safari tab button at the lower right of the screen.
4. Observe if the Private text button is surrounded by a gray background.

Remediation:

1. Tap the Safari app to launch it.
2. Tap the Safari tab button at the lower right of the screen.
3. Tap `Private`.
4. Select "Close All" or "Keep All" on the "Close All Pages?" dialog box.

Default Value:

Private Browsing: N/A (no longer a configuration setting); by default, Private Browsing is not activated for Safari web sessions.

1.2.9 Ensure 'Do Not Track' is set to 'Enabled' (Not Scored)

Profile Applicability:

- Level 2 - Apple iOS 10

Description:

This setting instructs Safari to communicate the preference not to be tracked to websites to which it connects.

Rationale:

Enabling Do Not Track instructs the iOS 7+ Safari browser to send an optional header in HTTP requests made from the app that indicates a preference not to be tracked by websites. This optional header is voluntary in nature, having no method to enforce adherence and providing no guarantee that web sites will honor the preference. However, a large number of websites do honor it so there is privacy benefit in enabling it.

Audit:

1. Tap `Settings`.
2. Tap `Safari`.
3. Confirm that Do Not Track is turned on.

Remediation:

1. Tap `Settings`.
2. Tap `Safari`.
3. Turn on Do Not Track.

Default Value:

Do No Track: Off

References:

1. Do Not Track - Universal Web Tracking Opt Out. Available: http://donottrack.us/
2. W3C Tracking Protection Working Group. Available: http://www.w3.org/2011/tracking-protection/
3. IETF Internet-Draft: Do Not Track: A Universal Third-Party Web Tracking Opt Out, March 7, 2011. Available: http://tools.ietf.org/html/draft-mayer-do-not-track-00
4. Do Not Track | Electronic Frontier Foundation. Available: https://www.eff.org/issues/do-not-track

2 Apple Configuration Settings

This section provides guidance on the secure configuration of iOS mobile devices with the Apple Configurator Utility, version 2.3. The Apple Configurator is a download available via the Mac App Store from Apple at https://itunes.apple.com/us/app/apple-configurator-2/id1037126344?mt=12 that lets users create, maintain, and sign configuration profiles, track and install provisioning profiles and authorized applications, and capture device information including console logs.

2.1 System Settings

This section provides guidance on the secure configuration of system settings.

2.1.1 Ensure 'Security Profile Removal' is set to 'With Authorization' (Scored)

Profile Applicability:

- Level 1 - Apple iOS 10

Description:

The device can be configured to always allow the removal of a profile, to allow the removal of a profile only with a profile-specific password, or to never allow the removal of a profile, on a per-profile basis. By default, the Apple Configurator allows the profile to be removed by the user. To ensure profile settings remain in effect, profile removal must be disallowed.

Rationale:

Restricting the removal of a configuration profile is necessary to enforce the settings contained within the respective profile. If a user can circumvent profile requirements simply by uninstalling the profile, the continued enforcement of profile controls cannot be assured and intended device security is highly reduced.

Audit:

1. Open the configuration profile XML file.
2. Search for `<key>PayloadRemovalDisallowed</key>`.
3. Observe if the next line is <true/>.
4. Search for <key>RemovalPassword</key>.
5. Observe whether this value is present and whether a value is set.

Remediation:

1. Open Apple Configurator.
2. Open or create a Profile.
3. Click on the `General` tab in the left windowpane.
4. Click on the `Security` drop-down menu in the right window pane.
5. Select `With Authorization`.
6. Install the configuration profile on the device.

2.1.2 Ensure 'allowHostPairing' is set to 'false' (Not Scored)

Profile Applicability:

- Level 2 - Apple iOS 10

Description:

This control allows for limits iOS device-to-computer pairing. Specifically, it limits connection only to the supervision host. This may be a desirable state in a high security environment.

Rationale:

By deploying a configuration payload with "allowHostPairing" set to "false", the device can only pair with the computer that provides supervision. This limits forms of data exfiltration and other physical possession exploits.

Audit:

1. Open the configuration profile XML file.
2. Search for `<key>allowHostPairing</key>`.
3. Confirm if the next line is <false/>.

Remediation:

1. Open Apple Configurator.
2. `Open or create a Profile.`
3. Click on the `Restrictions` tab in the left windowpane.
4. Uncheck the checkbox for on the `Allow pairing with non-Configurator hosts (supervised only)` drop-down menu in the right window pane.
5. Install the configuration profile on the device.

Impact:

An iOS device with the allowHostPairing key set to false will not be able to sync or backup to devices except its supervision host.

2.1.3 Ensure 'iCloud Drive' is set to 'Disabled' (Not Scored)

Profile Applicability:

- Level 2 - Apple iOS 10

Description:

Rationale:

Audit:

Remediation:

1. Open Apple Configurator.
2. `Open or create a Profile.`
3. Click on the `Restrictions` tab in the left windowpane.
4. Uncheck the checkbox for on the `Security` drop-down menu in the right window pane.
5. Select `With Authorization`.
6. Install the configuration profile on the device.

2.2 Passcode Settings

This section provides guidance on the secure configuration of passcode settings.

2.2.1 Ensure 'forcePIN' is set to 'true' (Scored)

Profile Applicability:

- Level 1 - Apple iOS 10

Description:

This control determines whether a password is required before allowing access to the device via the touch screen.

Rationale:

Requiring a password to unlock the device helps prevent unauthorized access to the device and increases the effort required to use the device or access data stored on it.

Audit:

1. Open the configuration profile XML file.
2. Search for `<key>forcePIN</key>`.
3. Observe if the next line is `<true/>`.

Remediation:

1. Open Apple Configurator.
2. Open or create a `Profile`.
3. Click on the `Passcode` tab in the left windowpane.
4. If a passcode is not currently required, you will be prompted to Configure Passcode Policy. Click on the `Configure` button in the prompt.
5. Install the configuration profile on the device.

Default Value:

By default, a passcode is not required to unlock the device.

2.2.2 Ensure 'Allow simple value' is set to 'false' (Scored)

Profile Applicability:

- Level 1 - Apple iOS 10

Description:

iOS devices can be configured via the iPCU to check passwords upon entry to disallow the use of repeating, ascending, and/or descending character sequences. By default, simple passcode values are permitted and checks for repeating, ascending, and descending character sequences are not performed. It is recommended that such sequences be disallowed for the passcode.

Rationale:

Simple passcodes such as those with repeating, ascending, or descending character sequences are easily guessed. Preventing the selection of passwords containing such sequences increases the complexity of the passcode and reduces the ease with which an attacker may attempt to guess the passcode in order to gain access to the device.

Audit:

1. Open the configuration profile XML file.
2. Search for `<key>allowSimple</key>`.
3. Observe if the next line is `<false/>`.

Remediation:

1. Open Apple Configurator.
2. Open or create a `Profile`.
3. Click on the `Passcode` tab in the left windowpane.
4. Click to uncheck the checkbox for `Allow simple value` in the right windowpane.
5. Install the configuration profile on the device.

Default Value:

Allow Simple Value: Enabled

2.2.3 Ensure 'requireAlphanumeric' is set to 'true' (Scored)

Profile Applicability:

- Level 2 - Apple iOS 10

Description:

This control determines whether alphanumeric characters (alphabetic and non-alphanumeric values in addition to numerals) are required for the passcode that protects access to the device via the touch screen.

Rationale:

Requiring a mix of alphabetical and numerical characters increases the complexity of the passcode and therefore the difficulty of determining the password by an attacker seeking unauthorized access.

Audit:

1. Open the configuration profile XML file.
2. Search for <key>requireAlphanumeric</key>.
3. Observe if the next line is <true/>.

Remediation:

1. Open Apple Configurator.
2. Open or create a `Profile`.
3. Click on the Passcode tab in the left windowpane.
4. Click to check the checkbox on the `Require alphanumeric value` in the right windowpane.
5. Install the configuration profile on the device.

Default Value:

By default, a passcode complexity policy is not enforced.

2.2.4 Ensure 'Minimum passcode length' is set to at least '6' (Scored)

Profile Applicability:

- Level 1 - Apple iOS 10

Description:

This control specifies the minimum number of characters a passcode can contain. It is recommended that passcode length be at least six (6) characters.

Rationale:

Requiring at least six characters increases the complexity of the passcode an attacker may attempt to brute-force in order to gain access to the device.

Audit:

1. Open the configuration profile XML file.
2. Search for `<key>minLength</key>`.
3. Observe if the next line is <integer>6</integer>.

Remediation:

1. Open Apple Configurator.
2. Open or create a `Profile`.
3. Click on the `Passcode` tab in the left windowpane.
4. Click on the Minimum passcode length drop-down menu in the right windowpane.
5. Select the number "6" or higher.
6. Install the configuration profile on the device.

Default Value:

By default, the minimum passcode length is only four characters.

2.2.5 Ensure 'Minimum number of complex characters' is set to at least '1' (Scored)

Profile Applicability:

- Level 2 - Apple iOS 10

Description:

This configuration item specifies the minimum number of non-alphanumeric characters (such as $, &, and !) that the passcode must contain. It is recommended that at least one non-alphanumeric character be required in the passcode.

Rationale:

Requiring at least one complex character increases the complexity of the passcode an attacker may attempt to brute-force in order to gain access to the device.

Audit:

1. Open the configuration profile XML file.
2. Search for `<key>minComplexChars</key>`.
3. Observe if the next line is `<integer>1</integer>`.

Remediation:

1. Open Apple Configurator.
2. `Open or create a Profile`.
3. Click on the Passcode tab in the left windowpane.
4. Click on the Minimum number of complex characters combo box in the right windowpane.
5. Select the number "1" or higher.
6. Install the configuration profile on the device.

Default Value:

By default, complex characters are not required in the passcode.

References:

1. NIST Special Publication (SP) 800-63-2, Electronic Authentication Guideline. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf

2.2.6 Ensure 'Maximum Auto-Lock' is set to '2 minutes' or less (Scored)

Profile Applicability:

- Level 1 - Apple iOS 10

Description:

This control defines the number of minutes the device can be inactive before requiring the password be reentered. It is recommended that an inactivity timeout of no more than two (2) minutes be set.

Rationale:

Automatically locking the device after a short period of inactivity reduces the probability of an attacker accessing the device without entering a password.

Audit:

1. Open the configuration profile XML file.
2. Search for `<key>maxInactivity</key>`.
3. Review the configured Auto-lock interval to observe if the next line is `<integer>2</integer>` or less.

Remediation:

1. Open Apple Configurator.
2. `Open or create a Profile`.
3. Click on the Passcode tab in the left windowpane.
4. Click on the Maximum Auto-Lock drop-down menu in the right windowpane.
5. Select the number 2 or less to set the Auto-lock interval.
6. Install the configuration profile on the device.

Default Value:

By default, if a passcode is defined, an iPhone or iPod touch device will lock after two minutes of inactivity.

2.2.7 Ensure 'Maximum number of failed attempts' is set to '6' (Scored)

Profile Applicability:

- Level 1 - Apple iOS 10

Description:

This setting determines how many failed passcode attempts can be made before the device is wiped (configurable from 2 to 10).

Rationale:

Excessive passcode failures typically indicate that the device is out of physical control of its owner. Upon such an event, erasing data on the phone will help to ensure the confidentiality of information stored on the device is protected when facing a novice attacker.

Audit:

1. Open the configuration profile XML file.
2. Search for <key>maxFailedAttempts</key>.
3. Observe if the next line is `<integer>6</integer>`.

Remediation:

1. Open Apple Configurator.
2. Open or create a `Profile`.
3. Click on the `Passcode` tab in the left windowpane.
4. Click on the `Maximum number of failed attempts` drop-down menu in the right windowpane.
5. Select the number `6`.
6. Install the configuration profile on the device.

Default Value:

By default, a maximum number of failed attempts is not configured.

2.3 Mail Settings

This section provides guidance on the secure configuration of mail settings.

2.3.1 Ensure 'PreventMove' is set to 'true' (Scored)

Profile Applicability:

- Level 2 - Apple iOS 10

Description:

This control determines whether a message can be moved from one mail account configured on the device to another account.

Rationale:

Permitting the movement of messages from one account to another intentionally or unintentionally can result in the exfiltration or loss of data from sensitive mail systems.

Audit:

1. Open the configuration profile XML file.
2. Search for `<string>MailAccountName</string>` where *MailAccountName* is the name of the mail account for which this restriction needs to be made, to locate the XML element for the configuration item.
3. Locate the child element `<key>PreventMove</key>`.
4. Observe if the next line is `<true/>`.
5. Repeat steps 2 through 4 for each mail account requiring this restriction.

Remediation:

1. Open Apple Configurator.
2. Open or create a `Profile`.
3. Click on the `Mail` option from the payloads list in the left windowpane.
4. In the right windowpane, locate the mail account to configure.
5. Click to uncheck the checkbox for `Allow user to move messages from this account`.
6. Repeat steps 4 and 5 for each mail account requiring this restriction.
7. Install the configuration profile on the device.

Default Value:

PreventMove: False

2.3.2 Ensure 'PreventAppSheet' is set to 'true' (Scored)

Profile Applicability:

- Level 2 - Apple iOS 10

Description:

This control determines whether a mail account can be used for sending messages from iOS apps other than the Mail app.

Rationale:

Permitting apps other than the Mail app to send messages from a mail account can limit an organization's ability to tightly control against the exfiltration or loss of sensitive data from an iOS device.

Audit:

1. Open the configuration profile XML file.
2. Search for `<string>MailAccountName</string>` where *MailAccountName* is the name of the mail account for which this restriction needs to be made, to locate the XML element for the configuration item.
3. Locate the child element `<key>PreventAppSheet</key>`.
4. Observe if the next line is `<true/>`.
5. Repeat steps 2 through 4 for each mail account requiring this restriction.

Remediation:

1. Open Apple Configurator.
2. Open or create `Profile`.
3. Click on the `Mail` option from the payloads list in the left windowpane.
4. In the right windowpane, locate the mail account to configure.
5. Click to check the checkbox for `Use only in Mail`.
6. Repeat steps 4 through 6 for each mail account requiring this restriction.
7. Install the configuration profile on the device.

Default Value:

Use Only in Mail: Disabled

Appendix: Summary Table

Control		Set Correctly	
		Yes	No
1	**User Interface Settings**		
1.1	**System Settings**		
1.1.1	Ensure 'Software Update' returns 'Your software is up to date." (Not Scored)	☐	☐
1.1.2	Ensure 'Passcode Lock' is 'Enabled' (Not Scored)	☐	☐
1.1.3	Ensure 'Auto-lock' is set to '2 minutes or less' (Not Scored)	☐	☐
1.1.4	Ensure 'Erase Data' is set to 'Enabled' (Not Scored)	☐	☐
1.1.5	Ensure 'Access on Lock Screen' is 'Disabled' for Control Center (Not Scored)	☐	☐
1.1.6	Ensure 'Ask to Join Networks' is 'Disabled' (Not Scored)	☐	☐
1.1.7	Ensure 'Auto-Join' is set to 'Disabled' for all Wi-Fi networks (Not Scored)	☐	☐
1.1.8	Ensure 'AirDrop Discoverability' is set to 'Disabled' (Not Scored)	☐	☐
1.1.9	Ensure 'Wi-Fi' is set to 'Disabled' when not necessary (Not Scored)	☐	☐
1.1.10	Ensure 'VPN' is set to 'Disabled' when not necessary (Not Scored)	☐	☐
1.1.11	Ensure 'Bluetooth' is set to 'Disabled' when not necessary (Not Scored)	☐	☐
1.1.12	Ensure 'Personal Hotspot' is set to 'Disabled' when not necessary (Not Scored)	☐	☐
1.1.13	Ensure 'Location Services' is set to 'Disabled' (Not Scored)	☐	☐
1.1.14	Ensure 'Notifications' are set to 'Disabled' on Lock Screen (Not Scored)	☐	☐
1.1.15	Ensure 'Automatic Downloads' of 'App Updates' is set to 'Enabled' (Not Scored)	☐	☐
1.1.16	Ensure 'Find My iPhone/iPad' is set to 'Enabled' (Not Scored)	☐	☐
1.1.17	Ensure 'iCloud Drive' is set to 'Disabled' (Not Scored)	☐	☐
1.1.18	Ensure 'Erase all Content and Settings' is `Executed` prior to releasing device control (Not Scored)	☐	☐
1.1.19	Ensure 'SIM Passcode' has been 'Set' (Not Scored)	☐	☐
1.2	**Safari Settings**		
1.2.1	Ensure 'JavaScript' is set to 'Disabled' (Not Scored)	☐	☐
1.2.2	Ensure 'Fraudulent Website Warning' is set to 'Enabled' (Not Scored)	☐	☐
1.2.3	Ensure 'Auto Fill for Contact Information' is set to 'Disabled'	☐	☐

	(Not Scored)		
1.2.4	Ensure 'Auto Fill for Names and Passwords' is set to 'Disabled' (Not Scored)	☐	☐
1.2.5	Ensure 'Auto Fill for Credit Card Information' is set to 'Disabled' (Not Scored)	☐	☐
1.2.6	Ensure 'Saved Password Information' is routinely 'Deleted' (Not Scored)	☐	☐
1.2.7	Ensure 'Saved Credit Cards' contains no entries (Not Scored)	☐	☐
1.2.8	Ensure 'Private Browsing' is used when necessary (Not Scored)	☐	☐
1.2.9	Ensure 'Do Not Track' is set to 'Enabled' (Not Scored)	☐	☐
2	**Apple Configuration Settings**		
2.1	**System Settings**		
2.1.1	Ensure 'Security Profile Removal' is set to 'With Authorization' (Scored)	☐	☐
2.1.2	Ensure 'allowHostPairing' is set to 'false' (Not Scored)	☐	☐
2.1.3	Ensure 'iCloud Drive' is set to 'Disabled' (Not Scored)	☐	☐
2.2	**Passcode Settings**		
2.2.1	Ensure 'forcePIN' is set to 'true' (Scored)	☐	☐
2.2.2	Ensure 'Allow simple value' is set to 'false' (Scored)	☐	☐
2.2.3	Ensure 'requireAlphanumeric' is set to 'true' (Scored)	☐	☐
2.2.4	Ensure 'Minimum passcode length' is set to at least '6' (Scored)	☐	☐
2.2.5	Ensure 'Minimum number of complex characters' is set to at least '1' (Scored)	☐	☐
2.2.6	Ensure 'Maximum Auto-Lock' is set to '2 minutes' or less (Scored)	☐	☐
2.2.7	Ensure 'Maximum number of failed attempts' is set to '6' (Scored)	☐	☐
2.3	**Mail Settings**		
2.3.1	Ensure 'PreventMove' is set to 'true' (Scored)	☐	☐
2.3.2	Ensure 'PreventAppSheet' is set to 'true' (Scored)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
1/25/2017	1.0.0	Used iOS 9 as a base
1/25/2017	1.0.0	Removed - 1.1.3 Disallow Simple Passcode Ticket #70
1/25/2017	1.0.0	Removed – 1.1.7 Forget Wi-Fi networks to prevent automatic rejoin Ticket #71
1/25/2017	1.0.0	Changed - 2.2.4 Set minimum passcode length – to 6 from 5 Ticket #72
1/25/2017	1.0.0	Removed – 2.2.3 Ensure 'Unmarked Email Domains is 'Populated' Ticket #73
1/25/2017	1.0.0	Add – 2.1.2 Level 2 - Set "allowHostPairing" to False Ticket #64
1/25/2017	1.0.0	Removed – Exchange sections since this is covered by the exchange benchmark Ticket #75