Center for Internet Security®

CIS Apple iOS 11 Benchmark

v1.0.0 - 10-17-2017

Table of Contents

Overview

This document, *Security Configuration Benchmark for Apple iOS 11*, provides prescriptive guidance for establishing a secure configuration posture for the Apple iOS version 11. This guide was tested against the Apple iOS 11 and the Apple Configurator v2.5. This benchmark covers the Apple iOS 11 and all hardware devices on which this iOS is supported. As of the publication of this guidance, mobile devices supported by iOS 11 include the following:

• iPhone 5s and later • iPad Pro and later • iPad Air and later • 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://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 11.

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://workbench.cisecurity.org.

Typographical Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
`Stylized Monospace font`	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
Monospace font	Used for inline code, commands, 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 - End-User Owned Devices**

  Items in this profile apply to end-user owned Apple iOS 11 devices and intend to:

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

- **Level 2 - End-User Owned Devices**

  This profile extends the "Level 1 - End-User Owned Devices" profile. Items in this profile apply to end-user owned Apple iOS 11 devices and may:

  - be used for environments or use cases where security is paramount.
  - act as defense in depth measures.
  - negatively inhibit the utility or performance of the technology.

- **Level 1 - Institutionally Owned Devices**

  Items in this profile apply to institutionally owned Apple iOS 11 devices and intend to:

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

- **Level 2 - Institutionally Owned Devices**

  This profile extends the "Level 1 - Institutionally Owned Devices" profile. Items in this profile apply to end-user owned Apple iOS 11 devices and may:

  - be used for environments or use cases where security is paramount.
  - act as defense in depth measures.
  - 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:

Contributor
Jordan Rakoske GSEC, GCWN
Will Strafach
Shawn Geddis
Pierluigi Falcone CISSP, CISM, CCSK, LA27001, SABSA Foundation

Editor
Paul Campbell, Anitian

Recommendations

1 Benchmark Guidance

The release of the *Security Configuration Benchmark for Apple iOS 10* marked a significant change in the CIS guidance for iOS. Since its initial release almost five years ago, the iOS series has focused on the audit and remediation of a single device, with ancillary guidance for the use of Configuration Profiles and Exchange ActiveSync policies. This model of management, and the audit and remediation that goes along with it, has grown unwieldy.

While end-users often only configure a small number of iOS devices, institutions routinely deploy hundreds to tens of thousands. The benchmark was rewritten to provide guidance that addressed both use cases. As a result, Configuration Profiles are now the primary focus. Only four recommendations remain that cannot be audited or remediated via a Configuration Profile (CP). Exchange ActiveSync policies have been removed and are now covered exclusively in the *Security Configuration Benchmark for Microsoft Exchange Server* series. These changes allow for a significantly more manageable approach to implementing the CIS iOS recommendations for deployments at scale.

For those unfamiliar with Configuration Profiles, a CP is simply an XML file that can be loaded onto an iOS device to provide configuration management. Whether you're an individual end-user or the administrator for an enterprise deployment of iOS devices, you can create CPs for free using Apple Configurator. Installing a profile is as simple as connecting a device to the Apple Configurator host vis USB, opening the profile on any iOS device, pushing it via macOS Server's Profile Manager, or deploying it via any modern Mobile Device Management (MDM) console.

Another significant change is the introduction of supervision. Supervision does not refer to management via CP or MDM console. It refers to a specific technical state of an iOS device. It can be enabled through Apple's Device Enrollment Program (DEP) in combination with an MDM, or on a per-device basis using Apple Configurator. Supervision extends the number of configuration options available and is expected to be enabled on all institutionally owned devices.

This release also introduces separate guidance for end-user and institutionally owned devices. The intention is to assess and remediate a CP against only the section that matches its given ownership model. This allows the benchmark to address the differing priorities and requirements appropriate to each case and for an organization to maintain CIS compliance while allowing BYOD. Look to individual recommendations for specific explanations on the implementation chosen.

The Additional Recommendations section includes material for both ownership models. Audits, and in some cases remediation, for these recommendations are available with certain MDM solutions.

Thank you for taking the time to read this benchmark guidance. The CIS iOS Community

2 Configuration Profile Recommendations for End-User Owned Devices

This section provides both level 1 and level 2 recommendations for devices in an unsupervised state. The term "unsupervised" is a specific technical designation in regards to the state of an iOS device and does not mean the device is unmanaged. See the introduction of this benchmark for clarification on the states supervised and unsupervised.

The CIS iOS Community further recommends the use of Apple's Volume Purchase Program (VPP) with end-user owned devices. The VPP allows an institution to more effectively manage app licensing by maintaining full ownership and control over apps deployed to end-user devices, provided they are managed with an MDM solution.

For more information on the VPP Apple program, visit:
https://help.apple.com/deployment/business/

2.1 General

2.1.1 (L1) Ensure a 'Consent Message' has been 'Configured' (Scored)

Profile Applicability:

- Level 1 - End-User Owned Devices

Description:

This recommendation pertains to the configuration of a consent message shown at the time of a configuration profile installation.

Rationale:

In this section of the benchmark, recommendations are for devices that are owned by the end-user. They are voluntarily accepting the configuration profile and should be provided an explicit opportunity to consent.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `General` tab.
4. In the right windowpane, verify that under the heading `Consent Message`, there is an appropriate consent message configured.

From the device, there is no method to determine if the installed configuration profile included a consent message.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `General` tab.
4. In the right windowpane, under the heading `Consent Message`, insert an appropriate consent message.
5. Deploy the Configuration Profile.

2.1.2 (L1) Ensure 'Controls when the profile can be removed' is set to 'Always' (Scored)

Profile Applicability:

- Level 1 - End-User Owned Devices

Description:

This recommendation pertains to the removal of a given configuration profile.

Rationale:

In this section of the benchmark, recommendations are for devices that are owned by the end-user. They are voluntarily accepting the configuration profile and should be able to remove it at will.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `General` tab.
4. In the right windowpane, verify that under the heading `Security`, the menu `Controls when the profile can be removed` is set to `Always`.

Or, from the device:

1. Tap Settings.
2. Tap General.
3. Tap Profile.
4. Tap <*Profile Name*>.
5. Verify `Delete Profile` is displayed near the bottom of the screen.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `General` tab.

4. In the right windowpane, under the heading `Security`, set the menu `Controls when the profile can be removed` to `Always`.
5. Deploy the Configuration Profile.

2.2 Restrictions

2.2.1 Functionality

2.2.1.1 (L1) Ensure 'Allow voice dialing while device is locked' is set to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - End-User Owned Devices

Description:

This recommendation pertains to initiating phone calls while a device is locked. Voice dialing is handled separate from Siri.

Rationale:

Allowing calls from a locked device may allow for the impersonation of the device owner.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, verify that under the tab `Functionality`, the checkbox for `Allow voice dialing while device is locked` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Profile`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Voice dialing while locked not allowed` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, under the tab `Functionality`, `uncheck` the checkbox for `Allow voice dialing while device is locked`.
5. Deploy the Configuration Profile.

CIS Controls:

16.5 Ensure Workstation Screen Locks Are Configured

Configure screen locks on systems to limit access to unattended workstations.

2.2.1.2 (L1) Ensure 'Allow Siri while device is locked' is set to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - End-User Owned Devices

Description:

This recommendation pertains to access to Siri while the device is locked.

Rationale:

Access to Siri on a locked device may allow unauthorized users to access information otherwise not available to them. Siri has access to messaging, contacts, and a variety of other data.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, verify that under the tab `Functionality`, the checkbox for `Allow Siri while device is locked` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Profile`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Siri while locked not allowed` is displayed

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.

4. In the right windowpane, under the tab `Functionality`, `uncheck` the checkbox for `Allow Siri while device is locked`.
5. Deploy the Configuration Profile.

Impact:

End-user must unlock the device before interacting with Siri.

CIS Controls:

16.5 Ensure Workstation Screen Locks Are Configured
Configure screen locks on systems to limit access to unattended workstations.

2.2.1.3 (L1) Ensure 'Allow managed apps to store data in iCloud' is set to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - End-User Owned Devices

Description:

This recommendation pertains to managed apps storing and syncing data through iCloud.

Rationale:

This recommendation addresses data leakage. It prevents a user from installing an app that is managed by the organization on a personal device and having iCloud sync the managed app data to the personal, non-managed app.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, verify that under the tab `Functionality`, the checkbox for `Allow managed apps to store data in iCloud` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Profile`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Managed apps cloud sync not allowed` is displayed

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.

4. In the right windowpane, under the tab `Functionality`, `uncheck` the checkbox for `Allow managed apps to store data in iCloud`.
5. Deploy the Configuration Profile.

Impact:

Syncing managed app data between multiple managed devices will not be possible.

CIS Controls:

13 Data Protection
Data Protection

2.2.1.4 (L1) Ensure 'Force encrypted backups' is set to 'Enabled' (Scored)

Profile Applicability:

- Level 1 - End-User Owned Devices

Description:

This recommendation pertains to encrypting iTunes backups of iOS devices.

Rationale:

Data that are stored securely on an iOS device may be trivially accessed from a local computer backup. Forcing the encryption of backups protects data from being compromised if the local host computer is compromised.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, verify that under the tab `Functionality`, the checkbox for `Force encrypted backups` is `checked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Profile`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Encrypted backups enforced` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, under the tab `Functionality`, `check` the checkbox for `Force encrypted backups`.

5. Deploy the Configuration Profile.

Impact:

End-users must configure a password for the encrypted backup; the complexity of which is not managed.

Notes:

This function does not apply to iCloud backups. iCloud backups are encrypted in transit and at rest by Apple.

CIS Controls:

10.3 Properly Protect Backups
Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.

2.2.1.5 (L2) Ensure 'Allow users to accept untrusted TLS certificates' is set to 'Disabled' (Scored)

Profile Applicability:

- Level 2 - End-User Owned Devices

Description:

This recommendation pertains to the acceptance of untrusted TLS certificates.

Rationale:

iOS devices maintain a list of trusted TLS certificate roots. An organization may add their own certificates to the list by way of a configuration profile. Allowing users to bypass that list and accept self-signed or otherwise unverified certificates may increase the likelihood of an incident.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, verify that under the tab `Functionality`, that the checkbox for `Allow users to accept untrusted TLS certificates` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Profile`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Establishing untrusted TLS connections not allowed` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.

3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, under the tab `Functionality`, `uncheck` the checkbox for `Allow users to accept untrusted TLS certificates`.
5. Deploy the Configuration Profile.

Impact:

The device automatically rejects untrusted HTTPS certificates without prompting the user. Services using self-signed certificates will not function.

2.2.1.6 (L1) Ensure 'Allow documents from managed sources in unmanaged destinations' is set to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - End-User Owned Devices

Description:

This recommendation pertains to Apple's managed app implementation.

The terms "managed" and "unmanaged" refer to app classifications made through Managed Open In, a feature of iOS 7 and later. Managed Open In provides for data containerization. Institutionally provisioned apps are designated managed. Apps elected by the end user are designated unmanaged.

Rationale:

Limiting data transfer from the managed institutional app space to the user space may prevent data leakage.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, verify that under the tab `Functionality`, the checkbox for `Allow documents from managed sources in unmanaged destinations` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Profile`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Opening documents from managed to unmanaged apps not allowed` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, under the tab `Functionality`, `uncheck` the checkbox for `Allow documents from managed sources in unmanaged destinations`.
5. Deploy the Configuration Profile.

CIS Controls:

14.4 Protect Information With Access Control Lists

All information stored on systems shall be protected with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

2.2.1.7 (L1) Ensure 'Allow documents from unmanaged sources in managed destinations' is set to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - End-User Owned Devices

Description:

This recommendation pertains to Apple's managed app implementation.

The terms "managed" and "unmanaged" refer to app classifications made through Managed Open In, a feature of iOS 7 and later. Managed Open In provides for data containerization. Institutionally provisioned apps are designated managed. Apps elected by the end user are designated unmanaged.

Rationale:

Limiting data transfer from the unmanaged user app space to the managed institutional space limits institutional resources from being employed for personal use.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, verify that under the tab `Functionality`, the checkbox for `Allow documents from unmanaged sources in managed destinations` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Profile`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Opening documents from unmanaged to managed apps not allowed` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, under the tab `Functionality`, `uncheck` the checkbox for `Allow documents from unmanaged sources in managed destinations`.
5. Deploy the Configuration Profile.

CIS Controls:

14.4 Protect Information With Access Control Lists

All information stored on systems shall be protected with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

2.2.1.8 (L1) Ensure 'Treat AirDrop as unmanaged destination' is set to 'Enabled' (Scored)

Profile Applicability:

- Level 1 - End-User Owned Devices

Description:

This recommendation pertains to AirDrop in the context of Apple's managed app implementation.

The terms "managed" and "unmanaged" refer to app classifications made through Managed Open In, a feature of iOS 7 and later. Managed Open In provides for data containerization. Institutionally provisioned apps are designated managed. Apps elected by the end user are designated unmanaged.

Rationale:

When AirDrop is allowed as a managed destination, sensitive data may be moved out of the managed app space to an unmanaged device.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, verify that under the tab `Functionality`, the checkbox for `Treat AirDrop as unmanaged destination` is `checked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Profile`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Sharing managed documents using AirDrop not allowed` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, under the tab `Functionality`, `check` the checkbox for `Treat AirDrop as unmanaged destination`.
5. Deploy the Configuration Profile.

Notes:

Note that the feature specifically mentions destination and not source. Following this recommendation does not prevent AirDrop connections into the managed app space, only AirDrop connections out of the managed app space.

CIS Controls:

14.4 Protect Information With Access Control Lists
All information stored on systems shall be protected with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

2.2.1.9 (L2) Ensure 'Allow Handoff' is set to 'Disabled' (Scored)

Profile Applicability:

- Level 2 - End-User Owned Devices

Description:

This recommendation pertains to Apple's Handoff data sharing mechanism.

Rationale:

Handoff does not enforce managed app boundaries. This allows managed app data to be moved to the unmanaged app space on another device, which may result in data leakage.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, verify that under the tab `Functionality`, the checkbox for `Allow Handoff` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Profile`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Handoff not allowed` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, under the tab `Functionality`, `uncheck` the checkbox for `Allow Handoff`.
5. Deploy the Configuration Profile.

Impact:

End-users may be inconvenienced by disabling Handoff on their personal devices.

CIS Controls:

14.4 Protect Information With Access Control Lists
All information stored on systems shall be protected with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

2.2.1.10 (L1) Ensure 'Force Apple Watch wrist detection' is set to 'Enabled' (Scored)

Profile Applicability:

- Level 1 - End-User Owned Devices

Description:

This recommendation pertains to configuring wrist detection on paired Apple Watches.

Rationale:

Wrist detection prevents a removed Apple Watch from providing access to information not otherwise available.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, verify that under the tab `Functionality`, the checkbox for `Force Apple Watch wrist detection` is `checked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Profile`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Wrist detection enforced on Apple Watch` is displayed

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.

4. In the right windowpane, under the tab `Functionality`, `check` the checkbox for `Force Apple Watch wrist detection`.
5. Deploy the Configuration Profile.

CIS Controls:

14.4 Protect Information With Access Control Lists

All information stored on systems shall be protected with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

2.2.1.11 (L1) Ensure 'Show Control Center in Lock screen' is set to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - End-User Owned Devices

Description:

This recommendation pertains to the display of Control Center on the lock screen.

Rationale:

When a device is lost or stolen, the Control Center may be used to enable airplane mode; thus preventing locating or erasing the device. Disabling Control Center forces a malicious actor to power down the device, which then discards the encryption key in memory. This makes some attacks based on physical possession more difficult.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, verify that under the tab `Functionality`, the checkbox for `Show Control Center in Lock screen` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Profile`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Control Center on lock screen not allowed` is displayed

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.

3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, under the tab `Functionality`, `uncheck` the checkbox for `Show Control Center in Lock screen`.
5. Deploy the Configuration Profile.

CIS Controls:

16.5 Ensure Workstation Screen Locks Are Configured

Configure screen locks on systems to limit access to unattended workstations.

2.2.1.12 (L1) Ensure 'Show Notification Center in Lock screen' is set to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - End-User Owned Devices

Description:

This recommendation pertains to the display of Notification Center on the lock screen.

Rationale:

Communications between the operating system and apps to a user should be controlled to prevent data leakage or exploitation. For example, some two-factor authentication apps will present to the notification center on lock screen the option to allow a login from a new device.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, verify that under the tab `Functionality`, the checkbox for `Show Notification Center in Lock screen` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Profile`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Notifications view on lock screen not allowed` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.

3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, under the tab `Functionality`, `uncheck` the checkbox for `Show Notification Center in Lock screen`.
5. Deploy the Configuration Profile.

Notes:

The per-app notification settings described later in the benchmark can be used in lieu of disabling Notification Center at the lock screen. This should only be done if there is confidence that all apps producing sensitive notifications can be managed.

CIS Controls:

16.5 Ensure Workstation Screen Locks Are Configured
Configure screen locks on systems to limit access to unattended workstations.

2.2.2 Apps

2.2.2.1 (L1) Ensure 'Force fraud warning' is set to 'Enabled' (Scored)

Profile Applicability:

- Level 1 - End-User Owned Devices

Description:

This recommendation pertains to Safari's feature for warning end-users about visiting suspected fraudulent websites.

Rationale:

Fraudulent websites masquerade as legitimate instances of financial, business, or other sites. They are designed to capture user credentials, often through phishing campaigns. Safari's fraudulent website warning feature helps protect end-users from such sites.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, verify that under the tab `Apps`, the checkbox for `Force fraud warning` is `checked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Profile`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Safari fraud warning enforced` is displayed.

Remediation:

1. Open Apple Configurator.

2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, under the tab `Apps`, `check` the checkbox for `Force fraud warning`.
5. Deploy the Configuration Profile.

CIS Controls:

7 Email and Web Browser Protections
Email and Web Browser Protections

2.2.2.2 (L1) Ensure 'Accept cookies' is set to 'From websites I visit' or `From current website only` (Scored)

Profile Applicability:

- Level 1 - End-User Owned Devices

Description:

This recommendation pertains to the acceptance of third-party cookies.

Rationale:

The HEIST cookie exploit allows for retrieving data from cookies stored on a device. Cookies often follow poor coding practices and often include authentication properties. Limiting acceptance of cookies to only those from sites intentionally visited reduces the likelihood of exploit.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, verify that under the tab `Apps`, the menu for `Accept cookies` is set to `From websites I visit` or `From current website only`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Profile`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Cookie policy enforced` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.

3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, under the tab `Apps`, set the `Accept cookies` menu to `From websites I visit` or `From current website only`.
5. Deploy the Configuration Profile.

Notes:

`From websites I visit` accepts cookies from the current domain, and any domain you've visited. `From current website only` only accepts cookies from the current domain.

CIS Controls:

7 Email and Web Browser Protections
Email and Web Browser Protections

2.3 Domains

2.3.1 (L1) Ensure 'Managed Safari Web Domains' is `Configured` (Not Scored)

Profile Applicability:

- Level 1 - End-User Owned Devices

Description:

This recommendation pertains to whether Safari, and MDM deployed browsers, will consider certain URL patterns as for managed app spaces only.

Rationale:

Sensitive files available from a website may be downloaded into the unmanaged app spaces by default. By configuring the specific domains that Safari should consider managed, an institution may support the secure containerization of their data.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Domains` tab.
4. In the right windowpane, verify that under `Managed Safari Web Domains` each appropriate URL pattern is configured.

Remediation:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Domains` tab.
4. In the right windowpane, under `Managed Safari Web Domains` enter the appropriate URL pattern(s).
5. Deploy the Configuration Profile.

Notes:

For improved effectiveness, this recommendation should be paired with the blacklisting of web browsers not deployed through the MDM.

CIS Controls:

14.4 Protect Information With Access Control Lists
All information stored on systems shall be protected with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

2.4 Passcode

2.4.1 (L1) Ensure 'Allow simple value' is set to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - End-User Owned Devices

Description:

This recommendation pertains to passcode requirements. A simple passcode is defined as containing repeated characters, or increasing/decreasing characters (such as 123 or CBA).

Rationale:

Simple passcodes include repeating, ascending, or descending character sequences that are more easily guessed.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Passcode` tab.
4. In the right windowpane, verify that the checkbox for `Allow simple value` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Profile`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Tap `Passcode`.
7. Confirm `Simple passcodes allowed` displays `No`.

Remediation:

1. Open Apple Configurator.

2. Open the Configuration Profile.
3. In the left windowpane, click on the `Passcode` tab.
4. In the right windowpane, `uncheck` the checkbox for `Allow simple value`.
5. Deploy the Configuration Profile.

CIS Controls:

16 Account Monitoring and Control
Account Monitoring and Control

2.4.2 (L1) Ensure 'Minimum passcode length' is set to '6' or greater (Scored)

Profile Applicability:

- Level 1 - End-User Owned Devices

Description:

This recommendation pertains to minimum passcode length.

Rationale:

Requiring at least six character minimum length provides reasonable assurance against passcode attacks.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Passcode` tab.
4. In the right windowpane, verify that the `Minimum passcode length` is set to `6`, or greater.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Profile`.
4. Tap `<_Profile Name_>`.
5. Tap `Passcode`.
6. Confirm `Minimum length` displays `6`, or greater.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Passcode` tab.
4. In the right windowpane, set the `Minimum passcode length` to `6`, or greater.

5. Deploy the Configuration Profile.

CIS Controls:

16.12 Use Long Passwords For All User Accounts
Where multi-factor authentication is not supported, user accounts shall be required to use long passwords on the system (longer than 14 characters).

2.4.3 (L1) Ensure 'Maximum Auto-Lock' is set to '2 minutes' or less (Scored)

Profile Applicability:

- Level 1 - End-User Owned Devices

Description:

This recommendation pertains to the maximum number of minutes a device may remain inactive before auto-locking.

NOTE: This recommendation refers to maximum auto-lock, consistent with the interface language, but iOS devices treat it as auto-lock at exactly 2 minutes.

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:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Passcode` tab.
4. In the right windowpane, verify that the `Maximum Auto-Lock` is set to `2 minutes`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Profile`.
4. Tap `<_Profile Name_>`.
5. Tap `Passcode`.
6. Confirm `Max inactivity` displays `2 minutes`.

Remediation:

1. Open Apple Configurator.

2. Open the Configuration Profile.
3. In the left windowpane, click on the `Passcode` tab.
4. In the right windowpane, set the `Maximum Auto-Lock` to `2 minutes`.
5. Deploy the Configuration Profile.

Notes:

This is not enforced during certain activities; such as watching movies.

CIS Controls:

16.4 Automatically Log Off Users After Standard Period Of Inactivity
Regularly monitor the use of all accounts, automatically logging off users after a standard period of inactivity.

2.4.4 (L1) Ensure 'Maximum grace period for device lock' is set to 'Immediately' (Scored)

Profile Applicability:

- Level 1 - End-User Owned Devices

Description:

This recommendation pertains to the amount of time after the device has been locked that it may be unlocked without entering a passcode. Devices with TouchID enabled do not allow a grace period.

Rationale:

Setting the maximum grace period to immediately ensures that a locked device will never be accessible without TouchID or entering a passcode.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Passcode` tab.
4. In the right windowpane, verify that `Maximum grace period for device lock` is set to `Immediately`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Profile`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Tap `Passcode`.
7. Confirm `Max grace period` displays `Immediately`.

Remediation:

1. Open Apple Configurator.

2. Open the Configuration Profile.
3. In the left windowpane, click on the `Passcode` tab.
4. In the right windowpane, set the `Maximum grace period for device lock` to `Immediately`.
5. Deploy the Configuration Profile.

CIS Controls:

16.5 Ensure Workstation Screen Locks Are Configured

Configure screen locks on systems to limit access to unattended workstations.

2.4.5 (L1) Ensure 'Maximum number of failed attempts' is set to '6' (Scored)

Profile Applicability:

- Level 1 - End-User Owned Devices

Description:

This recommendation pertains to the number of attempted logins before the automatic deletion of a device's cryptographic key.

Rationale:

Excessive incorrect passcode attempts typically indicate that the owner has lost physical control of the device. Upon such an event, erasing the encryption key will help to ensure the confidentiality of information stored on the device.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Passcode` tab.
4. In the right windowpane, verify that `Maximum number of failed attempts` is set to `6`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Profile`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Tap `Passcode`.
7. Confirm `Max failed attempts` displays `6`.

Remediation:

1. Open Apple Configurator.

2. Open the Configuration Profile.
3. In the left windowpane, click on the `Passcode` tab.
4. In the right windowpane, set the `Maximum number of failed attempts` to `6`.
5. Deploy the Configuration Profile.

CIS Controls:

16.7 Configure Account Lockouts

Use and configure account lockouts such that after a set number of failed login attempts the account is locked for a standard period of time.

2.5 VPN

2.5.1 (L1) Ensure 'VPN' is 'Configured' (Not Scored)

Profile Applicability:

- Level 1 - End-User Owned Devices

Description:

This recommendation pertains to establishing a virtual private network (VPN) connection as appropriate.

Rationale:

The network a device connects to provides important services that may be exploited by a malicious actor. Establishing a VPN mitigates the associated risks by encrypting data in transit and using known good network services, such as DNS.

Audit:

This audit procedure cannot be accomplished with a checkbox verification. As mentioned below, a per-app VPN configuration is the preferred solution, but a system-wide VPN is also acceptable. The auditor will need to determine which solution, and to what extent in the per-app VPN case, is appropriate.
From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `VPN` tab.
4. In the right windowpane, enter an appropriate VPN configuration.
5. Deploy the Configuration Profile.

From the device,

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN`.
4. Inspect the configuration.

Remediation:

This remediation procedure cannot be accomplished with a checkbox. As mentioned below, a per-app VPN configuration is the preferred solution, but a system-wide VPN is also acceptable. An appropriate solution will need to be determined and implemented.
From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `VPN` tab.
4. In the right windowpane, enter an appropriate VPN configuration.
5. Deploy the Configuration Profile.

From the device,

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN`.
4. Enter an appropriate VPN configuration.

References:

1. https://developer.apple.com/library/content/featuredarticles/iPhoneConfigurationProfileRef/Introduction/Introduction.html#//apple_ref/doc/uid/TP40010206-CH1-SW37
2. https://developer.apple.com/library/content/featuredarticles/iPhoneConfigurationProfileRef/Introduction/Introduction.html#//apple_ref/doc/uid/TP40010206-CH1-SW27

Notes:

iOS 11 supports both per-app VPN and system-wide VPN. Per-app configuration is preferred because it is always on, managed entirely through the CP and/or MDM, and invisible to the end-user.

CIS Controls:

14.2 Encrypt All Sensitive Information Over Less-trusted Networks
All communication of sensitive information over less-trusted networks should be encrypted. Whenever information flows over a network with a lower trust level, the information should be encrypted.

2.6 Mail

2.6.1 (L1) Ensure 'Allow user to move messages from this account' is set to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - End-User Owned Devices

Description:

This recommendation pertains to whether a message can be moved from an institutionally configured mail account. Also, it limits forwarding or replying from a different account than that which the message originated.

NOTE: This recommendation only applies if an institutionally configured mail account resides on the iOS device.

Rationale:

Permitting the movement of messages from a managed account to an unmanaged account may result in data leakage.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Mail` tab.
4. In the right windowpane, verify that the checkbox for `Allow user to move messages from this account` is `unchecked`.

From the device, there is no audit mechanism.

Remediation:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Mail` tab.

4. In the right windowpane, check the checkbox for `Allow user to move messages from this account`.

Default Value:

Message movement, forwarding, and reply is unrestricted.

CIS Controls:

14.4 Protect Information With Access Control Lists
All information stored on systems shall be protected with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

2.7 Notifications

2.7.1 (L1) Ensure 'Notification Settings' are configured for all 'Managed Apps' (Not Scored)

Profile Applicability:

- Level 1 - End-User Owned Devices

Description:

This recommendation pertains to configuring notification settings on a per app basis.

Rationale:

Notifications may include sensitive data or may allow for privileged actions to take place. All managed apps should include explicit notification settings to address these concerns.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Notifications` tab.
4. In the right windowpane, verify that each managed app includes a configuration entry.

Or, from the device:

1. Tap `Settings`.
2. Tap `Notifications`.
3. Verify that managed apps are grayed out to indicate that their notification settings are managed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Notifications` tab.

4. In the right windowpane, click `Configure` and/or click the + to add notification settings on a per-app basis.
5. Deploy the Configuration Profile.

CIS Controls:

14 Controlled Access Based on the Need to Know
Controlled Access Based on the Need to Know

3 Configuration Profile Recommendations for Institutionally Owned Devices

This section provides both level 1 and level 2 recommendations for devices in a supervised state. The term “supervised” is a specific technical designation in regards to the state of an iOS device and is generally only applied to institutionally owned devices. See the introduction of this benchmark for clarification on the states supervised and unsupervised.

The CIS iOS Community further recommends the use of Apple's Device Enrollment Program (DEP) and Volume Purchase Program (VPP) with institutionally owned devices. The DEP associates devices owned by an institution with its MDM server(s). The association occurs during setup when the iOS device contacts an Apple activation server. This ensures that all devices owned by an institution are being managed by its MDM solution, and allows for the distribution of iOS devices brand new or restored to factory default because they will receive configuration at activation. The VPP allows an institution to more effectively manage app licensing by maintaining full ownership and control over apps deployed within the organization. This can be especially useful for shared devices where managing AppleID app ownership is impractical.

For more information on these two Apple programs, visit:
https://help.apple.com/deployment/business/

3.1 General

3.1.1 (L1) Ensure 'Controls when the profile can be removed' is set to 'Never' (Scored)

Profile Applicability:

- Level 1 - Institutionally Owned Devices

Description:

This recommendation pertains to the removal of a given configuration profile.

Rationale:

In this section of the benchmark, recommendations are for devices that are owned by the institution. Removal of the configuration profile should be at the discretion of the institution, not the end-user, in order to prevent weakening the device's security and exposing its data.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `General` tab.
4. In the right windowpane, verify that under the heading `Security`, the menu `Controls when the profile can be removed` is set to `Never`.

Or, from the device:

1. Tap Settings.
2. Tap General.
3. Tap Profile.
4. Tap `<_Profile Name_>`.
5. Verify `Delete Profile` is **not** displayed near the bottom of the screen.

Remediation:

1. Open Apple Configurator.

2. Open the Configuration Profile.
3. In the left windowpane, click on the `General` tab.
4. In the right windowpane, under the heading `Security`, set the menu `Controls when the profile can be removed` to `Never`.
5. Deploy the Configuration Profile.

CIS Controls:

5.1 Minimize And Sparingly Use Administrative Privileges

Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

3.2 Restrictions

3.2.1 Functionality

3.2.1.1 (L2) Ensure 'Allow screenshots and screen recording' is set to 'Disabled' (Not Scored)

Profile Applicability:

- Level 2 - Institutionally Owned Devices

Description:

This recommendation pertains to limiting screenshots and screen recordings.

Rationale:

Sensitive information may be displayed through a managed app that could be captured by screen shot or screen recording into the unmanaged space inadvertently or intentionally by a malicious insider.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, verify that under the tab `Functionality`, the checkbox for `Allow screenshots and screen recording` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Profile`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `TBD` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, under the tab `Functionality`, `uncheck` the checkbox for `Allow screenshots and screen recording`.
5. Deploy the Configuration Profile.

Impact:

Screenshots will be unavailable for troubleshooting.

CIS Controls:

14.4 Protect Information With Access Control Lists
All information stored on systems shall be protected with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

3.2.1.2 (L1) Ensure 'Allow voice dialing while device is locked' is set to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - Institutionally Owned Devices

Description:

This recommendation pertains to initiating phone calls while a device is locked. Voice dialing is handled separate from Siri.

Rationale:

Allowing calls from a locked device may allow for the impersonation of the device owner.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, verify that under the tab `Functionality`, the checkbox for `Allow voice dialing while device is locked` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Profile`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Voice dialing while locked not allowed` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.

4. In the right windowpane, under the tab `Functionality`, `uncheck` the checkbox for `Allow voice dialing while device is locked`.
5. Deploy the Configuration Profile.

CIS Controls:

16.5 Ensure Workstation Screen Locks Are Configured
Configure screen locks on systems to limit access to unattended workstations.

3.2.1.3 (L1) Ensure 'Allow Siri while device is locked' is set to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - Institutionally Owned Devices

Description:

This recommendation pertains to access to Siri while the device is locked.

Rationale:

Access to Siri on a locked device may allow unauthorized users to access information otherwise not available to them. Siri has access to messaging, contacts, and a variety of other data.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, verify that under the tab `Functionality`, the checkbox for `Allow Siri while device is locked` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Profile`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Siri while locked not allowed` is displayed

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.

4. In the right windowpane, under the tab `Functionality`, `uncheck` the checkbox for `Allow Siri while device is locked`.
5. Deploy the Configuration Profile.

Impact:

End-user must unlock the device before interacting with Siri.

CIS Controls:

16.5 Ensure Workstation Screen Locks Are Configured
Configure screen locks on systems to limit access to unattended workstations.

3.2.1.4 (L1) Ensure 'Allow iCloud backup' is set to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - Institutionally Owned Devices

Description:

This recommendation pertains to allowing iCloud backup.

Rationale:

iCloud backups are encrypted in transit and at rest within Apple's infrastructure, but there is no protection against restoring a backup to an unmanaged device. This allows for data leakage.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, verify that under the tab `Functionality`, that the checkbox for `Allow iCloud backup` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Profile`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `iCloud backup not allowed` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, under the tab `Functionality`, `uncheck` the checkbox for `Allow iCloud backup`.

5. Deploy the Configuration Profile.

Notes:

This recommendation is exclusively for institutionally owned devices. If an institution is relying on BYOD, those devices should not contain sensitive material necessary to protect at this level.

CIS Controls:

14 Controlled Access Based on the Need to Know
Controlled Access Based on the Need to Know

3.2.1.5 (L1) Ensure 'Allow iCloud documents & data' is set to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - Institutionally Owned Devices

Description:

This recommendation pertains to the storage and sync of data through iCloud from institutionally owned devices.

Rationale:

Institutionally owned devices are often connected to personal iCloud accounts. This is expected and normal. The data from institutionally owned devices though should not co-mingle with the end-user's personal data. This poses a potential avenue of data leakage.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, verify that under the tab `Functionality`, that the checkbox for `Allow iCloud documents & data` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Profile`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `iCloud documents & data not allowed` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.

3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, under the tab `Functionality`, `uncheck` the checkbox for `Allow iCloud documents & data`.
5. Deploy the Configuration Profile.

CIS Controls:

14 Controlled Access Based on the Need to Know
Controlled Access Based on the Need to Know

3.2.1.6 (L1) Ensure 'Allow iCloud Keychain' is set to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - Institutionally Owned Devices

Description:

This recommendation pertains to iCloud performing Keychain synchronization.

Rationale:

It is normal and expected for end-users to enter their personal iCloud credentials onto institutionally owned devices. Because of this, iCloud Keychain presents an unnecessary risk to credentials because they may be shared onto jailbroken or otherwise compromised devices.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, verify that under the tab `Functionality`, the checkbox for `Allow iCloud Keychain` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Profile`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `iCloud Keychain not allowed` is displayed

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.

4. In the right windowpane, under the tab `Functionality`, `uncheck` the checkbox for `Allow iCloud Keychain`.
5. Deploy the Configuration Profile.

Notes:

This recommendation is not intended as advice against using the Keychain locally on an institutionally owned device. Nor is it intended to be taken as a recommendation to prevent iCloud Keychain from being used on end-user owned devices.

CIS Controls:

14 Controlled Access Based on the Need to Know
Controlled Access Based on the Need to Know

3.2.1.7 (L1) Ensure 'Allow managed apps to store data in iCloud' is set to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - Institutionally Owned Devices

Description:

This recommendation pertains to managed apps storing and syncing data through iCloud.

Rationale:

This recommendation addresses data leakage. It prevents a user from installing the app that is managed by the organization on a personal device and having iCloud sync the managed app data to the personal, non-managed app.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, verify that under the tab `Functionality`, the checkbox for `Allow managed apps to store data in iCloud` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Profile`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Managed apps cloud sync not allowed` is displayed

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.

4. In the right windowpane, under the tab `Functionality`, `check` the checkbox for `Allow managed apps to store data in iCloud`.
5. Deploy the Configuration Profile.

Impact:

Data created on the device may be lost if the end user has not transferred it to another device.

CIS Controls:

14 Controlled Access Based on the Need to Know
Controlled Access Based on the Need to Know

3.2.1.8 (L1) Ensure 'Force encrypted backups' is set to 'Enabled' (Scored)

Profile Applicability:

- Level 1 - Institutionally Owned Devices

Description:

This recommendation pertains to encrypting iTunes backups of iOS devices.

Rationale:

Data that are stored securely on an iOS device may be trivially accessed from a local computer. Forcing the encryption of backups significantly reduces the likelihood of sensitive data being compromised if the local host computer is compromised.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, verify that under the tab `Functionality`, the checkbox for `Force encrypted backups` is `checked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Profile`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Encrypted backups enforced` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, under the tab `Functionality`, `check` the checkbox for `Force encrypted backups`.

5. Deploy the Configuration Profile.

Impact:

End-users must configure a password for the encrypted backup; the complexity of which is not managed.

CIS Controls:

10.3 Properly Protect Backups
Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.

3.2.1.9 (L1) Ensure 'Allow Erase All Content and Settings' is set to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - Institutionally Owned Devices

Description:

This recommendation pertains to the factory reset functionality of iOS devices.

Rationale:

An institutionally owned device should not allow an end user to destroy data.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, verify that under the tab `Functionality`, that the checkbox for `Allow Erase All Content and Settings` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Profile`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Erase content and settings not allowed` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, under the tab `Functionality`, `uncheck` the checkbox for `Allow Erase All Content and Settings`.

5. Deploy the Configuration Profile.

Notes:

An end-user may still employ Apple's Find My iPhone/iPad service to perform an Erase All Content and Settings. This also sets an activation lock on the device. Activation lock may be blocked using an MDM solution, but not via CP.

For more information, see https://support.apple.com/en-us/HT202804

CIS Controls:

5.1 Minimize And Sparingly Use Administrative Privileges
Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

3.2.1.10 (L2) Ensure 'Allow users to accept untrusted TLS certificates' is set to 'Disabled' (Scored)

Profile Applicability:

- Level 2 - Institutionally Owned Devices

Description:

This recommendation pertains to the acceptance of untrusted TLS certificates.

Rationale:

iOS devices maintain a list of trusted TLS certificate roots. An organization may add their own certificates to the list by way of a configuration profile. Allowing users to bypass that list and accept self-signed or otherwise unverified certificates may increase the likelihood of an incident.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, verify that under the tab `Functionality`, the checkbox for `Allow users to accept untrusted TLS certificates` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Profile`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Establishing untrusted TLS connections not allowed` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.

3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, under the tab `Functionality`, `uncheck` the checkbox for `Allow users to accept untrusted TLS certificates`.
5. Deploy the Configuration Profile.

Impact:

The device automatically rejects untrusted HTTPS certificates without prompting the user.

3.2.1.11 (L1) Ensure 'Allow installing configuration profiles' is set to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - Institutionally Owned Devices

Description:

This recommendation pertains to the installation of additional configuration profiles.

Rationale:

This recommendation allows an institution to ensure that only the configuration profiles they provide are loaded onto the device.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, verify that under the tab `Functionality`, that the checkbox for `Allow installing configuration profiles` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Profile`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Installing configuration profiles not allowed` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.

4. In the right windowpane, under the tab `Functionality`, `uncheck` the checkbox for `Allow installing configuration profiles`.
5. Deploy the Configuration Profile.

Impact:

Some services, like wifi hotspot networks, may be prevented from working by blocking their configuration profiles.

CIS Controls:

5.1 Minimize And Sparingly Use Administrative Privileges
Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

3.2.1.12 (L1) Ensure 'Allow adding VPN configurations' is set to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - Institutionally Owned Devices

Description:

This recommendation pertains to the addition of user-defined VPN configurations.

Rationale:

This recommendation allows an institution to ensure that only the VPN configurations they provide are loaded onto the device.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, verify that under the tab `Functionality`, that the checkbox for `Allow adding VPN configurations` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Profile`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `VPN creation not allowed` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.

4. In the right windowpane, under the tab `Functionality`, `uncheck` the checkbox for `Allow adding VPN configurations`.
5. Deploy the Configuration Profile.

CIS Controls:

9 Limitation and Control of Network Ports, Protocols, and Services
Limitation and Control of Network Ports, Protocols, and Services

3.2.1.13 (L2) Ensure 'Allow modifying cellular data app settings' is set to 'Disabled' (Scored)

Profile Applicability:

- Level 2 - Institutionally Owned Devices

Description:

This recommendation pertains to modifying the use of cellular data by apps.

Rationale:

It is appropriate for an institution to have remote locating and erasure capability with their devices. Forcing cellular data to remain active is a means of supporting this goal.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, verify that under the tab `Functionality`, that the checkbox for `Allow modifying cellular data app settings` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Profile`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Changing app cellular data usage not allowed` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.

4. In the right windowpane, under the tab `Functionality`, `uncheck` the checkbox for `Allow modifying cellular data app settings`.
5. Deploy the Configuration Profile.

CIS Controls:

5.1 Minimize And Sparingly Use Administrative Privileges

Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

3.2.1.14 (L2) Ensure 'Allow pairing with non-Configurator hosts' is set to 'Disabled' (Scored)

Profile Applicability:

- Level 2 - Institutionally Owned Devices

Description:

This recommendation pertains to allowing data communication with a host computer.

Rationale:

Host pairing is a process by which an iOS device creates a cryptographically verified connection with a trusted host computer. By disabling the addition of new host pairings, a variety of hardware based attacks on the device are blocked.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, verify that under the tab `Functionality`, that the checkbox for `Allow pairing with non-Configurator hosts` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Profile`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Pairing with iTunes not allowed` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.

4. In the right windowpane, under the tab `Functionality`, `uncheck` the checkbox for `Allow pairing with non-Configurator hosts`.
5. Deploy the Configuration Profile.

Impact:

An end-user will not be able to sync media to and from the device.

Notes:

On the Apple Configurator host, there are two important data. The login keychain will include the host's identity certificate. It may be exported. The escrow keybags related to each device will be found in /var/db/lockdown. It is important that both these be backed up for continuity of device management. They may also be duplicated to other Macs to allow management of the configured devices.

CIS Controls:

15.7 Disable Peer-to-peer Wireless Capabilities
Disable peer-to-peer wireless network capabilities on wireless clients.

3.2.1.15 (L1) Ensure 'Allow documents from managed sources in unmanaged destinations' is set to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - Institutionally Owned Devices

Description:

This recommendation pertains to Apple's managed app implementation.

The terms "managed" and "unmanaged" refer to app classifications made through Managed Open In, a feature of iOS 7 and later. Managed Open In provides for data containerization. Institutionally provisioned apps are designated managed. Apps elected by the end user are designated unmanaged.

Rationale:

Limiting data transfer from the managed institutional app space to the user space may prevent data leakage.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, verify that under the tab `Functionality`, the checkbox for `Allow documents from managed sources in unmanaged destinations` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Profile`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Opening documents from managed to unmanaged apps not allowed` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, under the tab `Functionality`, `uncheck` the checkbox for `Allow documents from managed sources in unmanaged destinations`.
5. Deploy the Configuration Profile.

CIS Controls:

14.4 Protect Information With Access Control Lists

All information stored on systems shall be protected with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

3.2.1.16 (L1) Ensure 'Allow documents from unmanaged sources in managed destinations' is set to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - Institutionally Owned Devices

Description:

This recommendation pertains to Apple's managed app implementation.

The terms "managed" and "unmanaged" refer to app classifications made through Managed Open In, a feature of iOS 7 and later. Managed Open In provides for data containerization. Institutionally provisioned apps are designated managed. Apps elected by the end user are designated unmanaged.

Rationale:

Limiting data transfer from the unmanaged user app space to the managed institutional space limits institutional resources from being employed for personal use.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, verify that under the tab `Functionality`, the checkbox for `Allow documents from unmanaged sources in managed destinations` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Profile`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Opening documents from unmanaged to managed apps not allowed` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, under the tab `Functionality`, `uncheck` the checkbox for `Allow documents from unmanaged sources in managed destinations`.
5. Deploy the Configuration Profile.

CIS Controls:

14.4 Protect Information With Access Control Lists

All information stored on systems shall be protected with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

3.2.1.17 (L1) Ensure 'Treat AirDrop as unmanaged destination' is set to 'Enabled' (Scored)

Profile Applicability:

- Level 1 - Institutionally Owned Devices

Description:

This recommendation pertains to AirDrop in the context of Apple's managed app implementation.

The terms "managed" and "unmanaged" refer to app classifications made through Managed Open In, a feature of iOS 7 and later. Managed Open In provides for data containerization. Institutionally provisioned apps are designated managed. Apps elected by the end user are designated unmanaged.

Rationale:

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, verify that under the tab `Functionality`, the checkbox for `Treat AirDrop as unmanaged destination` is `checked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Profile`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Sharing managed documents using AirDrop not allowed` is displayed.

Remediation:

1. Open Apple Configurator.

2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, under the tab `Functionality`, `check` the checkbox for `Treat AirDrop as unmanaged destination`.
5. Deploy the Configuration Profile.

CIS Controls:

14.4 Protect Information With Access Control Lists

All information stored on systems shall be protected with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

3.2.1.18 (L1) Ensure 'Allow Handoff' is set to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - Institutionally Owned Devices

Description:

This recommendation pertains to Apple's Handoff data sharing mechanism.

Rationale:

Handoff does not enforce managed app boundaries. This allows managed app data to be moved to the unmanaged app space on another device, which may result in data leakage.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, verify that under the tab `Functionality`, the checkbox for `Allow Handoff` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Profile`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Handoff not allowed` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, under the tab `Functionality`, `uncheck` the checkbox for `Allow Handoff`.
5. Deploy the Configuration Profile.

Impact:

End-users may be inconvenienced by disabling Handoff on their personal devices.

CIS Controls:

14.4 Protect Information With Access Control Lists
All information stored on systems shall be protected with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

3.2.1.19 (L1) Ensure 'Force Apple Watch wrist detection' is set to 'Enabled' (Scored)

Profile Applicability:

- Level 1 - Institutionally Owned Devices

Description:

This recommendation pertains to configuring wrist detection on paired Apple Watches.

Rationale:

Wrist detection prevents a removed Apple Watch from providing access to information not otherwise available.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, verify that under the tab `Functionality`, the checkbox for `Force Apple Watch wrist detection` is `checked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Profile`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Wrist detection enforced on Apple Watch` is displayed

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.

4. In the right windowpane, under the tab `Functionality`, `check` the checkbox for `Force Apple Watch wrist detection`.
5. Deploy the Configuration Profile.

CIS Controls:

14.4 Protect Information With Access Control Lists

All information stored on systems shall be protected with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

3.2.1.20 (L1) Ensure 'Allow setting up new nearby devices' is set to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - Institutionally Owned Devices

Description:

This recommendation pertains to Apple's *Quick Start* setup feature.

Rationale:

This recommendation prevents an institutionally owned device from transferring configuration and content to another device.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, verify that under the tab `Functionality`, that the checkbox for `Allow setting up new nearby devices` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Profile`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Proximity Setup to a new device is not allowed` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.

4. In the right windowpane, under the tab `Functionality`, `uncheck` the checkbox for `Allow setting up new nearby devices`.
5. Deploy the Configuration Profile.

Notes:

For more information on *Quick Start*, see: https://support.apple.com/en-us/HT201269

CIS Controls:

13 Data Protection
Data Protection

3.2.1.21 (L1) Ensure 'Show Control Center in Lock screen' is set to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - Institutionally Owned Devices

Description:

This recommendation pertains to the display of Control Center on the lock screen.

Rationale:

When a device is lost or stolen, the Control Center may be used to enable airplane mode; thus preventing locating or erasing the device. It forces a malicious actor to power down the device, which then discards the encryption key in memory. This makes other attacks based on physical possession more difficult.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, verify that under the tab `Functionality`, the checkbox for `Show Control Center in Lock screen` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Profile`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Control Center view on lock screen not allowed` is displayed

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.

3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, under the tab `Functionality`, `uncheck` the checkbox for `Show Control Center in Lock screen`.
5. Deploy the Configuration Profile.

CIS Controls:

16.5 Ensure Workstation Screen Locks Are Configured

Configure screen locks on systems to limit access to unattended workstations.

3.2.1.22 (L1) Ensure 'Show Notification Center in Lock screen' is set to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - Institutionally Owned Devices

Description:

This recommendation pertains to the display of Notification Center on the lock screen.

Rationale:

Communications between the operating system and apps to a user should be controlled to prevent data leakage or exploitation. For example, some two-factor authentication apps will present to the notification center on lock screen the option to allow a login from a new device.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, verify that under the tab `Functionality`, the checkbox for `Show Notification Center in Lock screen` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Profile`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Notifications view on lock screen not allowed` is displayed

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.

3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, under the tab `Functionality`, `uncheck` the checkbox for `Show Notification Center in Lock screen`.
5. Deploy the Configuration Profile.

Notes:

The per-app notification settings described later in the benchmark can be used in lieu of disabling Notification Center at the lock screen. This should only be done if there is confidence that all apps producing sensitive notifications can be managed.

CIS Controls:

16.5 Ensure Workstation Screen Locks Are Configured
Configure screen locks on systems to limit access to unattended workstations.

3.2.2 Apps

3.2.2.1 (L1) Ensure 'Force fraud warning' is set to 'Enabled' (Scored)

Profile Applicability:

- Level 1 - Institutionally Owned Devices

Description:

This recommendation pertains to Safari's feature for warning end-users about visiting suspected fraudulent websites.

Rationale:

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

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, verify that under the tab `Apps`, the checkbox for `Force fraud warning` is `checked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Profile`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Safari fraud warning enforced` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.

3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, under the tab `Apps`, `check` the checkbox for `Force fraud warning`.
5. Deploy the Configuration Profile.

CIS Controls:

7 Email and Web Browser Protections
Email and Web Browser Protections

3.2.2.2 (L1) Ensure 'Accept cookies' is set to 'From websites I visit' or `From current website only` (Scored)

Profile Applicability:

- Level 1 - Institutionally Owned Devices

Description:

This recommendation pertains to the acceptance of third-party cookies.

Rationale:

The HEIST cookie exploit allows for retrieving data from cookies stored on a device. Cookies often follow poor coding practices and often include authentication properties. Limiting acceptance of cookies to only those from sites intentionally visited reduces the likelihood of exploit.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, verify that under the tab `Apps`, the menu for `Accept cookies` is set to `From websites I visit` or `From current website only`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Profile`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Cookie policy enforced` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.

3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, under the tab `Apps`, set the `Accept cookies` menu to `From websites I visit` or `From current website only`.
5. Deploy the Configuration Profile.

Notes:

`From websites I visit` accepts cookies from the current domain, and any domain you've visited. `From current website only` only accepts cookies from the current domain.

CIS Controls:

7 Email and Web Browser Protections
Email and Web Browser Protections

3.3 Domains

3.3.1 (L1) Ensure 'Managed Safari Web Domains' is `Configured` (Not Scored)

Profile Applicability:

- Level 1 - Institutionally Owned Devices

Description:

This recommendation pertains to whether Safari, and MDM deployed browsers, will consider certain URL patterns as for managed app spaces only.

Rationale:

Sensitive files available from a website may be downloaded into the unmanaged app spaces by default. By configuring the specific domains that Safari should consider managed, an institution may support the secure containerization of their data.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Domains` tab.
4. In the right windowpane, verify that under `Managed Safari Web Domains` each appropriate URL pattern is configured.

Remediation:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Domains` tab.
4. In the right windowpane, under `Managed Safari Web Domains` enter the appropriate URL pattern(s).
5. Deploy the Configuration Profile.

Notes:

For improved effectiveness, this recommendation should be paired with the blacklisting of web browsers not deployed through the MDM.

CIS Controls:

14.4 Protect Information With Access Control Lists
All information stored on systems shall be protected with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

3.4 Passcode

3.4.1 (L1) Ensure 'Allow simple value' is set to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - Institutionally Owned Devices

Description:

This recommendation pertains to passcode requirements. A simple passcode is defined as containing repeated characters, or increasing/decreasing characters (such as 123 or CBA).

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:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Passcode` tab.
4. In the right windowpane, verify that the checkbox for `Allow simple value` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Profile`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Tap `Passcode`.
7. Confirm `Simple passcodes allowed` displays `No`.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Passcode` tab.
4. In the right windowpane, `uncheck` the checkbox for `Allow simple value`.
5. Deploy the Configuration Profile.

CIS Controls:

16 Account Monitoring and Control
Account Monitoring and Control

3.4.2 (L1) Ensure 'Minimum passcode length' is set to '6' or greater (Scored)

Profile Applicability:

- Level 1 - Institutionally Owned Devices

Description:

This recommendation pertains to minimum passcode length.

Rationale:

Requiring at least six character minimum length provides reasonable assurance against passcode attacks.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Passcode` tab.
4. In the right windowpane, verify that the `Minimum passcode length` is set to `6`, or greater.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Profile`.
4. Tap `<_Profile Name_>`.
5. Tap `Passcode`.
6. Confirm `Minimum length` displays `6`, or greater.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Passcode` tab.
4. In the right windowpane, set the `Minimum passcode length` to `6`, or greater.

5. Deploy the Configuration Profile.

CIS Controls:

16.12 Use Long Passwords For All User Accounts
Where multi-factor authentication is not supported, user accounts shall be required to use long passwords on the system (longer than 14 characters).

3.4.3 (L1) Ensure 'Maximum Auto-Lock' is set to '2 minutes' or less (Scored)

Profile Applicability:

- Level 1 - Institutionally Owned Devices

Description:

This recommendation pertains to the maximum number of minutes a device may remain inactive before auto-locking.

NOTE: This entry refers to maximum auto-lock, consistent with the interface language, but iOS devices treat it as auto-lock at 2 minutes.

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:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Passcode` tab.
4. In the right windowpane, verify that the `Maximum Auto-Lock` is set to `2 minutes`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Profile`.
4. Tap `<_Profile Name_>`.
5. Tap `Passcode`.
6. Confirm `Max inactivity` displays `2 minutes`.

Remediation:

1. Open Apple Configurator.

2. Open the Configuration Profile.
3. In the left windowpane, click on the `Passcode` tab.
4. In the right windowpane, set the `Maximum Auto-Lock` to `2`.
5. Deploy the Configuration Profile.

Impact:

This is not enforced during certain activities; such as watching movies.

CIS Controls:

16.4 Automatically Log Off Users After Standard Period Of Inactivity
Regularly monitor the use of all accounts, automatically logging off users after a standard period of inactivity.

3.4.4 (L1) Ensure 'Maximum grace period for device lock' is set to 'Immediately' (Scored)

Profile Applicability:

- Level 1 - Institutionally Owned Devices

Description:

This recommendation pertains to the amount of time after the device has been locked that it may be unlocked without TouchID or entering a passcode.

Rationale:

Setting the maximum grace period to immediately ensures that a locked device will never be accessible without TouchID or entering a passcode.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Passcode` tab.
4. In the right windowpane, verify that `Maximum grace period for device lock` is set to `Immediately`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Profile`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Tap `Passcode`.
7. Confirm `Max grace period` displays `Immediately`.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.

3. In the left windowpane, click on the `Passcode` tab.
4. In the right windowpane, set the `Maximum grace period for device lock` to `Immediately`.
5. Deploy the Configuration Profile.

CIS Controls:

16.5 Ensure Workstation Screen Locks Are Configured

Configure screen locks on systems to limit access to unattended workstations.

3.4.5 (L1) Ensure 'Maximum number of failed attempts' is set to '6' (Scored)

Profile Applicability:

- Level 1 - Institutionally Owned Devices

Description:

This recommendation pertains to the number of attempted logins before the automatic deletion of a device's cryptographic key.

Rationale:

Excessive incorrect passcode attempts typically indicate that the owner has lost physical control of the device. Upon such an event, erasing the encryption key will help to ensure the confidentiality of information stored on the device.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Passcode` tab.
4. In the right windowpane, verify that `Maximum number of failed attempts` is set to `6`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Profile`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Tap `Passcode`.
7. Confirm `Max failed attempts` is set to `6`.

Remediation:

1. Open Apple Configurator.

2. Open the Configuration Profile.
3. In the left windowpane, click on the `Passcode` tab.
4. In the right windowpane, set the `Maximum number of failed attempts` to `6`.
5. Deploy the Configuration Profile.

CIS Controls:

16.7 Configure Account Lockouts

Use and configure account lockouts such that after a set number of failed login attempts the account is locked for a standard period of time.

3.5 VPN

3.5.1 (L1) Ensure 'VPN' is 'Configured' (Not Scored)

Profile Applicability:

- Level 1 - Institutionally Owned Devices

Description:

This recommendation pertains to establishing a virtual private network (VPN) connection as appropriate.

Rationale:

The network a device connects to provides important services that may be exploited by a malicious actor. Establishing a VPN mitigates the associated risks by encrypting data in transit and using known good network services, such as DNS.

Audit:

This audit procedure cannot be accomplished with a checkbox verification. As mentioned below, a per-app VPN configuration is the preferred solution, but a system-wide VPN is also acceptable. The auditor will need to determine which solution, and to what extent in the per-app VPN case, is appropriate.
From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `VPN` tab.
4. In the right windowpane, enter an appropriate VPN configuration.
5. Deploy the Configuration Profile.

From the device,

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN`.
4. Inspect the configuration.

Remediation:

This remediation procedure cannot be accomplished with a checkbox. As mentioned below, a per-app VPN configuration is the preferred solution, but a system-wide VPN is also acceptable. An appropriate solution will need to be determined and implemented.
From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `VPN` tab.
4. In the right windowpane, enter an appropriate VPN configuration.
5. Deploy the Configuration Profile.

From the device,

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN`.
4. Enter an appropriate VPN configuration.

References:

1. https://developer.apple.com/library/content/featuredarticles/iPhoneConfigurationProfileRef/Introduction/Introduction.html#//apple_ref/doc/uid/TP40010206-CH1-SW37
2. https://developer.apple.com/library/content/featuredarticles/iPhoneConfigurationProfileRef/Introduction/Introduction.html#//apple_ref/doc/uid/TP40010206-CH1-SW27

Notes:

iOS 11 supports both per-app VPN and system-wide VPN. Per-app configuration is preferred because it is always on, managed entirely through the CP and/or MDM, and invisible to the end-user.

CIS Controls:

14.2 Encrypt All Sensitive Information Over Less-trusted Networks
All communication of sensitive information over less-trusted networks should be encrypted. Whenever information flows over a network with a lower trust level, the information should be encrypted.

3.6 Mail

3.6.1 (L1) Ensure 'Allow user to move messages from this account' is set to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - Institutionally Owned Devices

Description:

This recommendation pertains to whether a message can be moved from an institutionally configured mail account. Also, it limits forwarding or replying from a different account than that which the message originated.

NOTE: This recommendation only applies if an institutionally configured mail account resides on the iOS device.

Rationale:

Permitting the movement of messages from a managed account to an unmanaged account may result in data leakage.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Mail` tab.
4. In the right windowpane, verify that the checkbox for `Allow user to move messages from this account` is `unchecked`.

From the device, there is no audit mechanism.

Remediation:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Mail` tab.

4. In the right windowpane, uncheck the checkbox for `Allow user to move messages from this account`.

CIS Controls:

14.4 Protect Information With Access Control Lists

All information stored on systems shall be protected with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

3.7 Notifications

3.7.1 (L1) Ensure 'Notification Settings' are configured for all 'Managed Apps' (Scored)

Profile Applicability:

- Level 1 - Institutionally Owned Devices

Description:

This recommendation pertains to configuring notification settings on a per app basis.

Rationale:

Notifications may include sensitive data or may allow for privileged actions to take place. All managed apps should include explicit notification settings to address these concerns.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Notifications` tab.
4. In the right windowpane, verify that each managed app includes a configuration entry.

Or, from the device:

1. Tap `Settings`.
2. Tap `Notifications`.
3. Verify that managed apps are grayed out to indicate that their notification settings are managed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Notifications` tab.

4. In the right windowpane, click `Configure` and/or click the + to add notification settings on a per-app basis.
5. Deploy the Configuration Profile.

CIS Controls:

14 Controlled Access Based on the Need to Know
Controlled Access Based on the Need to Know

3.8 Lock Screen Message

3.8.1 (L1) Ensure 'If Lost, Return to... Message' is 'Configured' (Not Scored)

Profile Applicability:

- Level 1 - Institutionally Owned Devices

Description:

This recommendation pertains to configuring a lock screen message.

Rationale:

A lock screen message will allow an honest by-stander to more easily return a lost device.

This message need not identify the owner by name, but should reference a phone number or email address to contact. Perhaps the help desk of the organization.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Lock Screen Message` tab.
4. In the right windowpane, verify that in the `"If Lost, Return to..." Message` is configured appropriately.

Or, from the device:

1. Wake the device.
2. Verify on the lock screen that an appropriate message is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Lock Screen Message` tab.

4. In the right windowpane, in the `"If Lost, Return to..." Message` field, configure an appropriate message.
5. Deploy the Configuration Profile.

CIS Controls:

16.5 Ensure Workstation Screen Locks Are Configured

Configure screen locks on systems to limit access to unattended workstations.

4 Additional Recommendations

This section provides both level 1 and level 2 recommendations for configuring iOS devices. These recommendations are not configurable via a CP. They are accessible on the device locally, or through certain MDM solutions.

4.1 (L1) Ensure device is not obviously jailbroken (Scored)

Profile Applicability:

- Level 1 - End-User Owned Devices
- Level 1 - Institutionally Owned Devices

Description:

This recommendation pertains to inspecting a device for the presence of the most common jailbreak indicator.

Rationale:

A jailbroken iOS device may execute arbitrary code, can compromise configuration profile requirements, and opens the device to exploits that are otherwise not possible.

Audit:

1. From the Home Screen, swipe down to open Spotlight.
2. Enter `Cydia`.
3. Confirm the Spotlight results do not contain the `Cydia` app.

Remediation:

Restore the iOS to a known good state from a trusted computer:

1. Open iTunes.
2. Connect the iOS device to the computer with a USB cable.
3. Select your iOS device within iTunes.
4. Select Restore iPhone/iPad.
5. After restoration, set up as a new device or restore from a known good backup.

CIS Controls:

5.1 Minimize And Sparingly Use Administrative Privileges

Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

4.2 (L1) Ensure 'Software Update' returns 'Your software is up to date.' (Scored)

Profile Applicability:

- Level 1 - End-User Owned Devices
- Level 1 - Institutionally Owned Devices

Description:

This recommendation pertains to updating and upgrading the operating system of a given device.

Rationale:

An up-to-date operating system provides the best possible protection against the execution of malicious code.

Audit:

From the device:

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

Remediation:

From the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Software Update`.
4. Tap `Install` or `Download and Install` and then allow device to complete the installation.

CIS Controls:

4 Continuous Vulnerability Assessment and Remediation
Continuous Vulnerability Assessment and Remediation

4.3 (L1) Ensure 'Automatic Downloads' of 'App Updates' is set to 'Enabled' (Scored)

Profile Applicability:

- Level 1 - End-User Owned Devices
- Level 1 - Institutionally Owned Devices

Description:

This recommendation pertains to the automatic installation of app updates.

Rationale:

App updates may patch software vulnerabilities.

Audit:

From the device:

1. Tap `Settings`.
2. Tap `iTunes & App Store`.
3. Verify that under `AUTOMATIC DOWNLOADS`, `Updates` is enabled.

Remediation:

From the device:

1. Tap `Settings`.
2. Tap `iTunes & App Store`.
3. Under `AUTOMATIC DOWNLOADS`, enable `Updates`.

CIS Controls:

4.5 Use Automated Patch Management And Software Update Tools
Deploy automated patch management tools and software update tools for operating system and software/applications on all systems for which such tools are available and safe. Patches should be applied to all systems, even systems that are properly air gapped.

4.4 (L1) Ensure 'Find My iPhone/iPad' is set to 'Enabled' on end-user owned devices (Scored)

Profile Applicability:

- Level 1 - End-User Owned Devices

Description:

This recommendation pertains to remote device locating, locking, and erasure by the end-user.

Rationale:

The ability to locate, lock, and erase a device remotely helps to mitigate impact of device theft and loss, and likelihood of loss.

This is only recommended for end-user owned devices. Institutionally owned devices should not be erasable by end-users.

Audit:

From the device:

1. Tap `Settings`.
2. Tap `<_The User's Name_>` where `Apple ID, iCloud, iTunes & App Store` is displayed beneath.
3. Tap `iCloud`.
4. Tap `Find My iPhone`.
5. Verify `Find My iPhone` and `Send Last Location` are enabled.

Remediation:

From the device:

1. Tap `Settings`.
2. Tap `<_The User's Name_>` where `Apple ID, iCloud, iTunes & App Store` is displayed beneath.
3. Tap `iCloud`.
4. Tap `Find My iPhone`.
5. Enable `Find My iPhone` and `Send Last Location`.

Impact:

Evidence may be destroyed if an end-user performs an erase.

CIS Controls:

14 Controlled Access Based on the Need to Know
Controlled Access Based on the Need to Know

4.5 (L2) Ensure the latest iOS device architecture is used by high-value targets (Not Scored)

Profile Applicability:

- Level 2 - End-User Owned Devices
- Level 2 - Institutionally Owned Devices

Description:

This recommendation pertains to the physical device(s) used by high-value targets.

Rationale:

Physical security exploits against iOS devices are rarely demonstrated within two years of the release of the underlying architecture. For users whose physical iOS device(s) may be targeted, it is prudent to use the most recently released architecture.

Audit:

Ensure the device(s) deployed to high-value targets are of the latest generation architecture.

Remediation:

Replace the device(s).
As of publication, the latest iOS device architectures are:

- iPhone 8 and X using the Apple A11 processor
- iPad Pro 10.5" and 12.9" using the Apple A10X processor

Notes:

Apple provides the following material on identifying iOS device hardware. For iPhone, see: https://support.apple.com/en-us/HT201296. For iPad, see: https://support.apple.com/en-us/HT201471.

The term *high-value targets* is being used to refer to users who may be likely to experience a physical-level device attack. Examples include:

- Politicians

- Journalists
- Activists
- Civilian government or military personnel
- Business executives
- Wealthy individuals

Appendix: Summary Table

Control		Set Correctly	
		Yes	No
1	**Benchmark Guidance**		
2	**Configuration Profile Recommendations for End-User Owned Devices**		
2.1	**General**		
2.1.1	(L1) Ensure a 'Consent Message' has been 'Configured' (Scored)	☐	☐
2.1.2	(L1) Ensure 'Controls when the profile can be removed' is set to 'Always' (Scored)	☐	☐
2.2	**Restrictions**		
2.2.1	**Functionality**		
2.2.1.1	(L1) Ensure 'Allow voice dialing while device is locked' is set to 'Disabled' (Scored)	☐	☐
2.2.1.2	(L1) Ensure 'Allow Siri while device is locked' is set to 'Disabled' (Scored)	☐	☐
2.2.1.3	(L1) Ensure 'Allow managed apps to store data in iCloud' is set to 'Disabled' (Scored)	☐	☐
2.2.1.4	(L1) Ensure 'Force encrypted backups' is set to 'Enabled' (Scored)	☐	☐
2.2.1.5	(L2) Ensure 'Allow users to accept untrusted TLS certificates' is set to 'Disabled' (Scored)	☐	☐
2.2.1.6	(L1) Ensure 'Allow documents from managed sources in unmanaged destinations' is set to 'Disabled' (Scored)	☐	☐
2.2.1.7	(L1) Ensure 'Allow documents from unmanaged sources in managed destinations' is set to 'Disabled' (Scored)	☐	☐
2.2.1.8	(L1) Ensure 'Treat AirDrop as unmanaged destination' is set to 'Enabled' (Scored)	☐	☐
2.2.1.9	(L2) Ensure 'Allow Handoff' is set to 'Disabled' (Scored)	☐	☐
2.2.1.10	(L1) Ensure 'Force Apple Watch wrist detection' is set to 'Enabled' (Scored)	☐	☐
2.2.1.11	(L1) Ensure 'Show Control Center in Lock screen' is set to 'Disabled' (Scored)	☐	☐
2.2.1.12	(L1) Ensure 'Show Notification Center in Lock screen' is set to 'Disabled' (Scored)	☐	☐
2.2.2	**Apps**		
2.2.2.1	(L1) Ensure 'Force fraud warning' is set to 'Enabled' (Scored)	☐	☐
2.2.2.2	(L1) Ensure 'Accept cookies' is set to 'From websites I visit' or `From current website only` (Scored)	☐	☐
2.3	**Domains**		

2.3.1	(L1) Ensure 'Managed Safari Web Domains' is `Configured` (Not Scored)	☐	☐
2.4	**Passcode**		
2.4.1	(L1) Ensure 'Allow simple value' is set to 'Disabled' (Scored)	☐	☐
2.4.2	(L1) Ensure 'Minimum passcode length' is set to '6' or greater (Scored)	☐	☐
2.4.3	(L1) Ensure 'Maximum Auto-Lock' is set to '2 minutes' or less (Scored)	☐	☐
2.4.4	(L1) Ensure 'Maximum grace period for device lock' is set to 'Immediately' (Scored)	☐	☐
2.4.5	(L1) Ensure 'Maximum number of failed attempts' is set to '6' (Scored)	☐	☐
2.5	**VPN**		
2.5.1	(L1) Ensure 'VPN' is 'Configured' (Not Scored)	☐	☐
2.6	**Mail**		
2.6.1	(L1) Ensure 'Allow user to move messages from this account' is set to 'Disabled' (Scored)	☐	☐
2.7	**Notifications**		
2.7.1	(L1) Ensure 'Notification Settings' are configured for all 'Managed Apps' (Not Scored)	☐	☐
3	**Configuration Profile Recommendations for Institutionally Owned Devices**		
3.1	**General**		
3.1.1	(L1) Ensure 'Controls when the profile can be removed' is set to 'Never' (Scored)	☐	☐
3.2	**Restrictions**		
3.2.1	**Functionality**		
3.2.1.1	(L2) Ensure 'Allow screenshots and screen recording' is set to 'Disabled' (Not Scored)	☐	☐
3.2.1.2	(L1) Ensure 'Allow voice dialing while device is locked' is set to 'Disabled' (Scored)	☐	☐
3.2.1.3	(L1) Ensure 'Allow Siri while device is locked' is set to 'Disabled' (Scored)	☐	☐
3.2.1.4	(L1) Ensure 'Allow iCloud backup' is set to 'Disabled' (Scored)	☐	☐
3.2.1.5	(L1) Ensure 'Allow iCloud documents & data' is set to 'Disabled' (Scored)	☐	☐
3.2.1.6	(L1) Ensure 'Allow iCloud Keychain' is set to 'Disabled' (Scored)	☐	☐
3.2.1.7	(L1) Ensure 'Allow managed apps to store data in iCloud' is set to 'Disabled' (Scored)	☐	☐
3.2.1.8	(L1) Ensure 'Force encrypted backups' is set to 'Enabled' (Scored)	☐	☐
3.2.1.9	(L1) Ensure 'Allow Erase All Content and Settings' is set to 'Disabled' (Scored)	☐	☐

3.2.1.10	(L2) Ensure 'Allow users to accept untrusted TLS certificates' is set to 'Disabled' (Scored)	☐	☐
3.2.1.11	(L1) Ensure 'Allow installing configuration profiles' is set to 'Disabled' (Scored)	☐	☐
3.2.1.12	(L1) Ensure 'Allow adding VPN configurations' is set to 'Disabled' (Scored)	☐	☐
3.2.1.13	(L2) Ensure 'Allow modifying cellular data app settings' is set to 'Disabled' (Scored)	☐	☐
3.2.1.14	(L2) Ensure 'Allow pairing with non-Configurator hosts' is set to 'Disabled' (Scored)	☐	☐
3.2.1.15	(L1) Ensure 'Allow documents from managed sources in unmanaged destinations' is set to 'Disabled' (Scored)	☐	☐
3.2.1.16	(L1) Ensure 'Allow documents from unmanaged sources in managed destinations' is set to 'Disabled' (Scored)	☐	☐
3.2.1.17	(L1) Ensure 'Treat AirDrop as unmanaged destination' is set to 'Enabled' (Scored)	☐	☐
3.2.1.18	(L1) Ensure 'Allow Handoff' is set to 'Disabled' (Scored)	☐	☐
3.2.1.19	(L1) Ensure 'Force Apple Watch wrist detection' is set to 'Enabled' (Scored)	☐	☐
3.2.1.20	(L1) Ensure 'Allow setting up new nearby devices' is set to 'Disabled' (Scored)	☐	☐
3.2.1.21	(L1) Ensure 'Show Control Center in Lock screen' is set to 'Disabled' (Scored)	☐	☐
3.2.1.22	(L1) Ensure 'Show Notification Center in Lock screen' is set to 'Disabled' (Scored)	☐	☐
3.2.2	**Apps**		
3.2.2.1	(L1) Ensure 'Force fraud warning' is set to 'Enabled' (Scored)	☐	☐
3.2.2.2	(L1) Ensure 'Accept cookies' is set to 'From websites I visit' or `From current website only` (Scored)	☐	☐
3.3	**Domains**		
3.3.1	(L1) Ensure 'Managed Safari Web Domains' is `Configured` (Not Scored)	☐	☐
3.4	**Passcode**		
3.4.1	(L1) Ensure 'Allow simple value' is set to 'Disabled' (Scored)	☐	☐
3.4.2	(L1) Ensure 'Minimum passcode length' is set to '6' or greater (Scored)	☐	☐
3.4.3	(L1) Ensure 'Maximum Auto-Lock' is set to '2 minutes' or less (Scored)	☐	☐
3.4.4	(L1) Ensure 'Maximum grace period for device lock' is set to 'Immediately' (Scored)	☐	☐
3.4.5	(L1) Ensure 'Maximum number of failed attempts' is set to '6' (Scored)	☐	☐
3.5	**VPN**		
3.5.1	(L1) Ensure 'VPN' is 'Configured' (Not Scored)	☐	☐

3.6	**Mail**		
3.6.1	(L1) Ensure 'Allow user to move messages from this account' is set to 'Disabled' (Scored)	☐	☐
3.7	**Notifications**		
3.7.1	(L1) Ensure 'Notification Settings' are configured for all 'Managed Apps' (Scored)	☐	☐
3.8	**Lock Screen Message**		
3.8.1	(L1) Ensure 'If Lost, Return to... Message' is 'Configured' (Not Scored)	☐	☐
4	**Additional Recommendations**		
4.1	(L1) Ensure device is not obviously jailbroken (Scored)	☐	☐
4.2	(L1) Ensure 'Software Update' returns 'Your software is up to date.' (Scored)	☐	☐
4.3	(L1) Ensure 'Automatic Downloads' of 'App Updates' is set to 'Enabled' (Scored)	☐	☐
4.4	(L1) Ensure 'Find My iPhone/iPad' is set to 'Enabled' on end-user owned devices (Scored)	☐	☐
4.5	(L2) Ensure the latest iOS device architecture is used by high-value targets (Not Scored)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
10/17/17	1.0.0	Initial Release