

CIS Apple iOS 18 and iPadOS 18 Intune Benchmark

v1.0.0 - 09-30-2025

Terms of Use

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

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

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

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

Table of Contents

Terms of Use	1
Table of Contents	2
Overview	6
Important Usage Information	6
Key Stakeholders.....	6
Apply the Correct Version of a Benchmark	7
Exceptions	7
Remediation	8
Summary.....	8
Target Technology Details	9
Intended Audience	9
Consensus Guidance.....	10
Typographical Conventions	11
Recommendation Definitions	12
Title.....	12
Assessment Status	12
Automated	12
Manual.....	12
Profile.....	12
Description	12
Rationale Statement.....	12
Impact Statement.....	13
Audit Procedure.....	13
Remediation Procedure	13
Default Value	13
References	13
CIS Critical Security Controls® (CIS Controls®).....	13
Additional Information	13
Profile Definitions	14
Acknowledgements.....	15
Recommendations	16
1 Benchmark Guidance	16
2 Recommendations for Unsupervised (BYOD) Devices	17
2.1 App Store, Doc Viewing, Gaming	18
2.1.1 Ensure "Block viewing corporate documents in unmanaged apps" is set to "Yes" (Manual).....	19

2.1.2 Ensure "Treat AirDrop as an unmanaged destination" is set to "Yes" (Manual)	21
2.1.3 Ensure "Allow copy/paste to be affected by managed open-in" is set to "Yes" (Manual)	23
2.2 Built-in Apps	25
2.2.1 Ensure "Block Siri while device is locked" is set to "Yes" (Manual)	26
2.2.2 Ensure "Require Safari fraud warnings" is set to "Yes" (Manual)	28
2.3 Cloud and Storage	30
2.3.1 Ensure "Force encrypted backup" is set to "Yes" (Manual)	31
2.3.2 Ensure "Block managed apps from storing data in iCloud" is set to "Yes" (Manual)	33
2.3.3 Ensure "Block backup of enterprise books" is set to "Yes" (Manual)	35
2.3.4 Ensure "Block notes and highlights sync for enterprise books" is set to "Yes" (Manual)	37
2.3.5 Ensure "Block iCloud Photos sync" is set to "Yes" (Manual)	39
2.3.6 Ensure "Block iCloud Photo Library" is set to "Yes" (Manual)	41
2.3.7 Ensure "Block My Photo Stream" is set to "Yes" (Manual)	43
2.3.8 Ensure "Block Handoff" is set to "Yes" (Manual)	45
2.4 Connected Devices	47
2.4.1 Ensure "Force Apple Watch wrist detection" is set to "Yes" (Manual)	48
2.4.2 Ensure "Require AirPlay outgoing requests pairing password" is set to "Yes" (Manual)	50
2.4.3 Ensure "Block Apple Watch auto unlock" is set to "Yes" (Manual)	52
2.5 General	54
2.5.1 Ensure "Block sending diagnostic and usage data to Apple" is set to "Yes" (Manual)	55
2.5.2 Ensure "Block screenshots and screen recording" is set to "Yes" (Manual)	57
2.5.3 Ensure "Block untrusted TLS certificates" is set to "Yes" (Manual)	59
2.5.4 Ensure "Force limited ad tracking" is set to "Yes" (Manual)	61
2.5.5 Ensure "Block trusting new enterprise app authors" is set to "Yes" (Manual)	63
2.5.6 Ensure "Limit Apple personalized advertising" is set to "Yes" (Manual)	65
2.6 Locked Screen Experience	67
2.6.1 Ensure "Block Control Center access in lock screen" is set to "Yes" (Manual)	68
2.6.2 Ensure "Block Notifications Center access in lock screen" is set to "Yes" (Manual)	70
2.6.3 Ensure "Block Today view in lock screen" is set to "Yes" (Manual)	72
2.6.4 Ensure "Block Wallet notifications in lock screen" is set to "Yes" (Manual)	74
2.7 Password	76
2.7.1 Ensure "Require password" is set to "Yes" (Manual)	77
2.7.2 Ensure "Block simple passwords" is set to "Yes" (Manual)	79
2.7.3 Ensure "Required password type" is set to "Alphanumeric" (Manual)	81
2.7.4 Ensure "Minimum password length" is set to "6" or greater (Manual)	83
2.7.5 Ensure "Maximum minutes after screen lock before password is required" is set to "Immediately" (Manual)	85
2.7.6 Ensure "Maximum minutes of inactivity until screen locks" is set to "2" or less (Manual)	87
2.7.7 Ensure "Block Touch ID and Face ID unlock" is set to "Yes" (Manual)	89
2.8 Wireless	91
2.8.1 Ensure "Block voice dialing while device is locked" is set to "Yes" (Manual)	92
3 Recommendations for Supervised (Organization) Devices	94
3.1 App Store, Doc Viewing, Gaming	95
3.1.1 Ensure "Block viewing corporate documents in unmanaged apps" is set to "Yes" (Manual)	96
3.1.2 Ensure "Treat AirDrop as an unmanaged destination" is set to "Yes" (Manual)	98
3.1.3 Ensure "Allow copy/paste to be affected by managed open-in" is set to "Yes" (Manual)	100
3.1.4 Ensure "Block App Store" is set to "Yes" (Manual)	102
3.1.5 Ensure "Block access to network drive in Files app" is set to "Yes" (Manual)	104
3.2 Built-in Apps	106
3.2.1 Ensure "Block Siri while device is locked" is set to "Yes" (Manual)	107
3.2.2 Ensure "Require Safari fraud warnings" is set to "Yes" (Manual)	109
3.3 Cloud and Storage	111

3.3.1 Ensure "Force encrypted backup" is set to "Yes" (Manual)	112
3.3.2 Ensure "Block managed apps from storing data in iCloud" is set to "Yes" (Manual)	114
3.3.3 Ensure "Block backup of enterprise books" is set to "Yes" (Manual)	116
3.3.4 Ensure "Block notes and highlights sync for enterprise books" is set to "Yes" (Manual)	118
3.3.5 Ensure "Block iCloud Photos sync" is set to "Yes" (Manual)	120
3.3.6 Ensure "Block iCloud Photo Library" is set to "Yes" (Manual)	122
3.3.7 Ensure "Block My Photo Stream" is set to "Yes" (Manual)	124
3.3.8 Ensure "Block Handoff" is set to "Yes" (Manual)	126
3.3.9 Ensure "Block iCloud backup" is set to "Yes" (Manual)	128
3.3.10 Ensure "Block iCloud document and data sync" is set to "Yes" (Manual)	130
3.3.11 Ensure "Block iCloud Keychain sync" is set to "Yes" (Manual)	132
3.4 Connected Devices	134
3.4.1 Ensure "Force Apple Watch wrist detection" is set to "Yes" (Manual)	135
3.4.2 Ensure "Require AirPlay outgoing requests pairing password" is set to "Yes" (Manual)	137
3.4.3 Ensure "Block Apple Watch auto unlock" is set to "Yes" (Manual)	139
3.4.4 Ensure "Block iBeacon discovery of AirPrint printers" is set to "Yes" (Manual)	141
3.4.5 Ensure "Block access to USB drive in Files app" is set to "Yes" (Manual)	143
3.5 General	145
3.5.1 Ensure "Block sending diagnostic and usage data to Apple" is set to "Yes" (Manual)	146
3.5.2 Ensure "Block screenshots and screen recording" is set to "Yes" (Manual)	148
3.5.3 Ensure "Block untrusted TLS certificates" is set to "Yes" (Manual)	150
3.5.4 Ensure "Force limited ad tracking" is set to "Yes" (Manual)	152
3.5.5 Ensure "Block trusting new enterprise app authors" is set to "Yes" (Manual)	154
3.5.6 Ensure "Limit Apple personalized advertising" is set to "Yes" (Manual)	156
3.5.7 Ensure "Block users from erasing all content and settings on device" is set to "Yes" (Manual)	158
3.5.8 Ensure "Block modification of device name" is set to "Yes" (Manual)	160
3.5.9 Ensure "Block configuration profile changes" is set to "Yes" (Manual)	162
3.5.10 Ensure "Allow activation lock" is set to "Yes" (Manual)	164
3.5.11 Ensure "Force automatic date and time" is set to "Yes" (Manual)	166
3.5.12 Ensure "Block VPN creation" is set to "Yes" (Manual)	168
3.6 Locked Screen Experience	170
3.6.1 Ensure "Block Control Center access in lock screen" is set to "Yes" (Manual)	171
3.6.2 Ensure "Block Notifications Center access in lock screen" is set to "Yes" (Manual)	173
3.6.3 Ensure "Block Today view in lock screen" is set to "Yes" (Manual)	175
3.6.4 Ensure "Block Wallet notifications in lock screen" is set to "Yes" (Manual)	177
3.7 Password	179
3.7.1 Ensure "Require password" is set to "Yes" (Manual)	180
3.7.2 Ensure "Block simple passwords" is set to "Yes" (Manual)	182
3.7.3 Ensure "Required password type" is set to "Alphanumeric" (Manual)	184
3.7.4 Ensure "Minimum password length" is set to "6" or greater (Manual)	186
3.7.5 Ensure "Maximum minutes after screen lock before password is required" is set to "Immediately" (Manual)	188
3.7.6 Ensure "Maximum minutes of inactivity until screen locks" is set to "2" or less (Manual)	190
3.7.7 Ensure "Block Touch ID and Face ID unlock" is set to "Yes" (Manual)	192
3.7.8 Ensure "Block password proximity requests" is set to "Yes" (Manual)	194
3.7.9 Ensure "Block password sharing" is set to "Yes" (Manual)	196
3.7.10 Ensure "Require Touch ID or Face ID authentication for AutoFill of password or credit card information" is set to "Yes" (Manual)	198
3.8 Wireless	200
3.8.1 Ensure "Block voice dialing while device is locked" is set to "Yes" (Manual)	201
3.9 Lock Screen Message	203
3.9.1 Ensure a "Lock Screen Message" has been set (Manual)	204

3.10 Additional Recommendations	206
3.10.1 Ensure the ability to remove the management profile does not exist (Manual)	207
3.10.2 Ensure the ability to sync with computers has been blocked (Manual)	209
4 Recommendations for Compliance Policies	211
4.1 Ensure "Jailbroken devices" is set to "Block" (Manual).....	212
4.2 Ensure "Minimum OS version" or "Minimum OS build version" has been defined (Manual)	214
4.3 Ensure "Mark device noncompliant" is set to "Immediately" (Manual)	216
4.4 Ensure "Send email to end user" is set to "3 days" or less (Manual).....	218
4.5 Ensure all devices are marked as "compliant" (Manual).....	220
4.6 Ensure "Mark devices with no compliance policy assigned as" is set to "Not compliant" (Manual).....	222
4.7 Ensure "Compliance status validity period (days)" is set to "7" or less (Manual)	224
Appendix: Summary Table	226
Appendix: CIS Controls v7 IG 1 Mapped Recommendations	234
Appendix: CIS Controls v7 IG 2 Mapped Recommendations	237
Appendix: CIS Controls v7 IG 3 Mapped Recommendations	242
Appendix: CIS Controls v7 Unmapped Recommendations	247
Appendix: CIS Controls v8 IG 1 Mapped Recommendations	248
Appendix: CIS Controls v8 IG 2 Mapped Recommendations	253
Appendix: CIS Controls v8 IG 3 Mapped Recommendations	258
Appendix: CIS Controls v8 Unmapped Recommendations	263
Appendix: Change History	264

Overview

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

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

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

Important Usage Information

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

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

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

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

Key Stakeholders

Cybersecurity is a collaborative effort, and cross functional cooperation is imperative within an organization to discuss, test, and deploy Benchmarks in an effective and efficient way. The Benchmarks are developed to be best practice configuration guidelines applicable to a wide range of use cases. In some organizations, exceptions to specific Recommendations will be needed, and this team should work to prioritize the problematic Recommendations based on several factors like risk, time, cost, and labor. These exceptions should be properly categorized and documented for auditing purposes.

Apply the Correct Version of a Benchmark

Benchmarks are developed and tested for a specific set of products and versions and applying an incorrect Benchmark to a system can cause the resulting pass/fail score to be incorrect. This is due to the assessment of settings that do not apply to the target systems. To assure the correct Benchmark is being assessed:

- **Deploy the Benchmark applicable to the way settings are managed in the environment:** An example of this is the Microsoft Windows family of Benchmarks, which have separate Benchmarks for Group Policy, Intune, and Stand-alone systems based upon how system management is deployed. Applying the wrong Benchmark in this case will give invalid results.
- **Use the most recent version of a Benchmark:** This is true for all Benchmarks, but especially true for cloud technologies. Cloud technologies change frequently and using an older version of a Benchmark may have invalid methods for auditing and remediation.

Exceptions

The guidance items in the Benchmarks are called recommendations and not requirements, and exceptions to some of them are expected and acceptable. The Benchmarks strive to be a secure baseline, or starting point, for a specific technology, with known issues identified during Benchmark development are documented in the Impact section of each Recommendation. In addition, organizational, system specific requirements, or local site policy may require changes as well, or an exception to a Recommendation or group of Recommendations (e.g. A Benchmark could Recommend that a Web server not be installed on the system, but if a system's primary purpose is to function as a Webserver, there should be a documented exception to this Recommendation for that specific server).

In the end, exceptions to some Benchmark Recommendations are common and acceptable, and should be handled as follows:

- The reasons for the exception should be reviewed cross-functionally and be well documented for audit purposes.
- A plan should be developed for mitigating, or eliminating, the exception in the future, if applicable.
- If the organization decides to accept the risk of this exception (not work toward mitigation or elimination), this should be documented for audit purposes.

It is the responsibility of the organization to determine their overall security policy, and which settings are applicable to their unique needs based on the overall risk profile for the organization.

Remediation

CIS has developed [Build Kits](#) for many technologies to assist in the automation of hardening systems. Build Kits are designed to correspond to Benchmark's "Remediation" section, which provides the manual remediation steps necessary to make that Recommendation compliant to the Benchmark.

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

The following is a reasonable remediation approach to follow:

- CIS Build Kits, or internally developed remediation methods should never be applied to production systems without proper testing.
- Proper testing consists of the following:
 - Understand the configuration (including installed applications) of the targeted systems. Various parts of the organization may need different configurations (e.g., software developers vs standard office workers).
 - Read the Impact section of the given Recommendation to help determine if there might be an issue with the targeted systems.
 - Test the configuration changes with representative lab system(s). If issues arise during testing, they can be resolved prior to deploying to any production systems.
 - When testing is complete, initially deploy to a small sub-set of production systems and monitor closely for issues. If there are issues, they can be resolved prior to deploying more broadly.
 - When the initial deployment above is completed successfully, iteratively deploy to additional systems and monitor closely for issues. Repeat this process until the full deployment is complete.

Summary

Using the Benchmarks Certified tools, working as a team with key stakeholders, being selective with exceptions, and being careful with remediation deployment, it is possible to harden large numbers of deployed systems in a cost effective, efficient, and safe manner.

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

CIS-CAT® Pro is also available to CIS [SecureSuite®](#) members.

Target Technology Details

This document, Security Configuration Benchmark for Intune Apple iOS 18 and iPadOS 18, provides prescriptive guidance for establishing a secure configuration posture for both Apple iOS and iPadOS version 18 via enrollment within Microsoft Intune. This guide was tested against Apple iOS 18 and iPadOS 18 using Microsoft Intune MDM enrollment. This benchmark covers Apple iOS 18 and iPadOS 18 on all supported devices.

The current guidance considers iOS and iPadOS devices as having the same use cases and threat scenarios when determining recommendations. In nearly all instances, the configuration steps, default settings, and benchmark recommended settings are identical regardless of hardware platform or operating system. For the few cases where variation exists, the benchmark notes differences 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 support@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 management of Apple iOS 18 or iPadOS 18 devices via MDM enrollment within Microsoft Intune.

Consensus Guidance

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

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

Typographical Conventions

The following typographical conventions are used throughout this guide:

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

Recommendation Definitions

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

Title

Concise description for the recommendation's intended configuration.

Assessment Status

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

Automated

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

Manual

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

Profile

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

Description

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

Rationale Statement

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

Impact Statement

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

Audit Procedure

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

Remediation Procedure

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

Default Value

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

References

Additional documentation relative to the recommendation.

CIS Critical Security Controls® (CIS Controls®)

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

Additional Information

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

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1 - Unsupervised Devices**

Items in this profile apply to unsupervised (end-user owned/BYOD) Apple iOS 17 and iPadOS 17 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 - Unsupervised Devices**

This profile extends the "Level 1 - Unsupervised Devices" profile. Items in this profile apply to unsupervised (end-user owned/BYOD) Apple iOS 17 and iPadOS 17 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 - Supervised Devices**

Items in this profile apply to supervised (fully managed) Apple iOS 17 and iPadOS 17 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 - Supervised Devices**

This profile extends the "Level 1 - Supervised Devices" profile. Items in this profile apply to supervised (fully managed) Apple iOS 17 and iPadOS 17 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:

Author

Lewis Hardy

Contributor

Ron Colvin, Ron Colvin

Kari Byrd

Phil Bain

Lewis Hardy

Editor

Pierluigi Falcone CISSP, CISM, CRISC, GSTRT, CCSK, LA27001, SABSA Foundation

Edward Byrd , Center for Internet Security, New York

Recommendations

1 Benchmark Guidance

Intune is a cloud endpoint management service produced by Microsoft. Intune supports Apple iOS and iPadOS operating system software. Due to the near identical code base, use cases, threat scenarios, and a shared configuration management mechanism within Intune, the CIS Community offers guidance for both operating systems within this single Intune MDM benchmark.

For those unfamiliar with using Intune for iOS and iPadOS device management, a Configuration Profile must be created to apply to the device that is to be managed, similar to a traditional software MDM (Mobile Device Management) solution (such as Apple Configurator). This configuration profile is created within Intune, where device restrictions and features can be individually configured. This configuration profile can then apply to devices that have been enrolled within Intune using a scope. The device will then have a management profile present listing restrictions that have been applied to the device. A specific recommendation has been defined in this benchmark that provides guidance on how to make this profile non-removable on supervised devices.

This benchmark defines what these device restrictions and features should be from a security standpoint. Further guidance on securely applying the profile and compliance policy guidance also exists in the benchmark.

This benchmark release continues to separate guidance for Unsupervised (BYOD) and Supervised (Organization) devices. The intention is to scope security control appropriateness by ownership model. This allows the benchmark to address the differing use cases and threat profiles, as well as for an organization to maintain CIS compliance for fully-managed Supervised (organization) devices, while also allowing Unsupervised Bring-Your-Own-Devices (BYOD).

In order to securely manage a corporate device, the device must be supervised. This should be a requirement of all institutionally-owned devices. Supervision is a specific technical state of an iOS or iPadOS device. It does not refer to management via Intune. Devices can be enrolled and supervised through methods such as Apple's Device Enrollment Program (DEP), or on a per-device basis using Apple Configurator.

Unsupervised devices cannot have all the same security restrictions applied due to device security limitations, therefore these devices should be treated as BYOD-only devices with access to limited managed resources.

The Compliance Policy Guideline section includes material for both ownership states.

Thank you for taking the time to read this benchmark guidance.

The CIS Intune iOS and iPadOS Community

2 Recommendations for Unsupervised (BYOD) 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 regarding the state of an iOS or iPadOS device and does not mean the device is unmanaged. See the Benchmark Guidance section of this benchmark for clarification on supervised and unsupervised states.

2.1 App Store, Doc Viewing, Gaming

2.1.1 Ensure "Block viewing corporate documents in unmanaged apps" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Unsupervised Devices

Description:

This prevents viewing corporate documents in unmanaged apps.

Rationale:

By default, depending on per-app policies, the OS might allow corporate documents to be viewed in any app.

Impact:

Third-party keyboards may not function correctly with this restriction set.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **App Store, Doc Viewing, Gaming** heading
6. Verify that **Block viewing corporate documents in unmanaged apps** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **Opening documents from managed to unmanaged apps not allowed** is displayed

Remediation:







From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **App Store, Doc Viewing, Gaming** heading
6. Set **Block viewing corporate documents in unmanaged apps** to **Yes**

Default Value:

Not configured

CIS Controls:

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

2.1.2 Ensure "Treat AirDrop as an unmanaged destination" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Unsupervised Devices

Description:

This forces AirDrop to be considered an unmanaged drop target.

Rationale:

This stops managed apps data from being sent via Airdrop.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **App Store, Doc Viewing, Gaming** heading
6. Verify that **Treat AirDrop as an unmanaged destination** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **Sharing managed documents using AirDrop not allowed** is displayed

Remediation:







From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **App Store, Doc Viewing, Gaming** heading
6. Set **Treat AirDrop as an unmanaged destination** to **Yes**

Default Value:

Not configured

CIS Controls:

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

2.1.3 Ensure "Allow copy/paste to be affected by managed open-in" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Unsupervised Devices

Description:

This enforces copy/paste restrictions based on configured Block viewing corporate documents in unmanaged apps and Block viewing non-corporate documents in corporate apps.

Rationale:

This can ensure that copy/paste restrictions set by managed apps are enforced.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **App Store, Doc Viewing, Gaming** heading
6. Verify that **Allow copy/paste to be affected by managed open-in** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **Copy and paste are managed** is displayed

Remediation:







From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **App Store, Doc Viewing, Gaming** heading
6. Set **Allow copy/paste to be affected by managed open-in** to **Yes**

Default Value:

Not configured

CIS Controls:

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

2.2 Built-in Apps

2.2.1 Ensure "Block Siri while device is locked" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Unsupervised Devices

Description:

This prevents access to Siri when the device is locked.

Rationale:

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

Impact:

The end user must unlock the device before interacting with Siri.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **Built-in apps** heading
6. Verify that **Block Siri while device is locked** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **Siri while locked not allowed** is displayed

Remediation:







From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **Built-in apps** heading
6. Set **Block Siri while device is locked** to **Yes**

Default Value:

Not configured

CIS Controls:

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

2.2.2 Ensure "Require Safari fraud warnings" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Unsupervised Devices

Description:

This enforces the feature to display fraud warnings within the Safari web browser.

Rationale:

Fraudulent websites masquerade as legitimate instances of financial, business, or other sensitive 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.

For increased security, the Safari web browser should be used to enforce fraud warnings.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **Built-in apps** heading
6. Verify that **Require Safari fraud warnings** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **Safari fraud warning enforced** is displayed

Remediation:





From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **Built-in apps** heading
6. Set **Require Safari fraud warnings** to **Yes**

Default Value:

Not configured

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.4 <u>Restrict Unnecessary or Unauthorized Browser and Email Client Extensions</u> Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.			
v7	7.2 <u>Disable Unnecessary or Unauthorized Browser or Email Client Plugins</u> Uninstall or disable any unauthorized browser or email client plugins or add-on applications.			

2.3 Cloud and Storage

2.3.1 Ensure "Force encrypted backup" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Unsupervised Devices

Description:

This requires device backups to be stored in an encrypted state.

Rationale:

Data that are stored securely on an iOS or iPadOS 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.

Impact:

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

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **Cloud and Storage** heading
6. Verify that **Force encrypted backup** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **Encrypted backups enforced** is displayed

Remediation:







From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **Cloud and Storage** heading
6. Set **Force encrypted backup** to **Yes**

Default Value:

Not configured

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	11.3 <u>Protect Recovery Data</u> Protect recovery data with equivalent controls to the original data. Reference encryption or data separation, based on requirements.			
v7	10.4 <u>Ensure Protection of Backups</u> 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.			

2.3.2 Ensure "Block managed apps from storing data in iCloud" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Unsupervised Devices

Description:

This prevents managed apps from storing and syncing data to the user's iCloud account.

Rationale:

This recommendation addresses intentional or unintentional data leakage. It prevents a user from installing an application that is managed by the organization on a personal device and allowing iCloud to sync the managed application's data to the personal, non-managed application.

Impact:

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

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **Cloud and Storage** heading
6. Verify that **Block managed apps from storing data in iCloud** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **Managed apps cloud sync not allowed** is displayed

Remediation:






From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **Cloud and Storage** heading
6. Set **Block managed apps from storing data in iCloud** to **Yes**

Default Value:

Not configured

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.3 Address Unauthorized Software Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.			
v7	13.4 Only Allow Access to Authorized Cloud Storage or Email Providers Only allow access to authorized cloud storage or email providers.			

2.3.3 Ensure "Block backup of enterprise books" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Unsupervised Devices

Description:

This prevents backing up of enterprise books.

Rationale:

This recommendation addresses intentional or unintentional data leakage. It prevents a user from backing up enterprise books (documents handled by the Books application).

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **Cloud and Storage** heading
6. Verify that **Block backup of enterprise books** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **Backing up enterprise books not allowed** is displayed

Remediation:






From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **Cloud and Storage** heading
6. Set **Block backup of enterprise books** to **Yes**

Default Value:

Not configured

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.3 Address Unauthorized Software Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.			
v7	13.4 <u>Only Allow Access to Authorized Cloud Storage or Email Providers</u> Only allow access to authorized cloud storage or email providers.			

2.3.4 Ensure "Block notes and highlights sync for enterprise books" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Unsupervised Devices

Description:

This prevents syncing notes and highlights in enterprise books.

Rationale:

Notes and highlights of text created within enterprise books may contain sensitive information that should not be backed up.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **Cloud and Storage** heading
6. Verify that **Block notes and highlights sync for enterprise books** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **Synchronizing enterprise books notes and highlights not allowed** is displayed

Remediation:






From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **Cloud and Storage** heading
6. Set **Block notes and highlights sync for enterprise books** to **Yes**

Default Value:

Not configured

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.3 Address Unauthorized Software Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.			
v7	13.4 Only Allow Access to Authorized Cloud Storage or Email Providers Only allow access to authorized cloud storage or email providers.			

2.3.5 Ensure "Block iCloud Photos sync" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Unsupervised Devices

Description:

This prevents photo stream syncing to iCloud.

Rationale:

This stops the ability to share pictures and screenshots to cloud storage that can be accessed outside your organization's network or devices.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **Cloud and Storage** heading
6. Verify that **Block iCloud Photos sync** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **Photo Stream not allowed** is displayed

Remediation:






From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **Cloud and Storage** heading
6. Set **Block iCloud Photos sync** to **Yes**

Default Value:

Not configured

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.3 Address Unauthorized Software Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.			
v7	13.4 <u>Only Allow Access to Authorized Cloud Storage or Email Providers</u> Only allow access to authorized cloud storage or email providers.			

2.3.6 Ensure "Block iCloud Photo Library" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Unsupervised Devices

Description:

This prevents photo Library syncing to iCloud.

Rationale:

This stops the ability to share pictures and screenshots to cloud storage that can be accessed outside your organization's network or devices.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **Cloud and Storage** heading
6. Verify that **Block iCloud Photo Library** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **iCloud Photos not allowed** is displayed

Remediation:






From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **Cloud and Storage** heading
6. Set **Block iCloud Photo Library** to **Yes**

Default Value:

Not configured

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.3 Address Unauthorized Software Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.			
v7	13.4 Only Allow Access to Authorized Cloud Storage or Email Providers Only allow access to authorized cloud storage or email providers.			

2.3.7 Ensure "Block My Photo Stream" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Unsupervised Devices

Description:

This disables iCloud Photo Sharing.

Rationale:

This stops the ability to share pictures and screenshots to cloud storage that can be accessed outside your organization's network or devices.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **Cloud and Storage** heading
6. Verify that **Block My Photo Stream** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **Shared Streams not allowed** is displayed

Remediation:






From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **Cloud and Storage** heading
6. Set **Block My Photo Stream** to **Yes**

Default Value:

Not configured

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.3 Address Unauthorized Software Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.			
v7	13.4 <u>Only Allow Access to Authorized Cloud Storage or Email Providers</u> Only allow access to authorized cloud storage or email providers.			

2.3.8 Ensure "Block Handoff" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Unsupervised Devices

Description:

This prevents Apple's Handoff data-sharing mechanism, allowing users to carry on tasks on another iOS/iPadOS or macOS device.

Rationale:

Impact:

Handoff does not enforce managed application boundaries. This allows managed application data to be moved to the unmanaged application space on another device, which may allow for intentional or unintentional data leakage.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **Cloud and Storage** heading
6. Verify that **Block Handoff** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **Handoff not allowed** is displayed

Remediation:







From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **Cloud and Storage** heading
6. Set **Block Handoff** to **Yes**

Default Value:

Not configured

CIS Controls:

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

2.4 Connected Devices

2.4.1 Ensure "Force Apple Watch wrist detection" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Unsupervised Devices

Description:

This restriction forces wrist detection to be enabled to paired Apple Watches. When enforced, the Apple Watch won't display notifications when it's not being worn. The Apple Watch will also lock itself when it has been removed from a user's wrist.

Rationale:

Wrist detection prevents a removed Apple Watch from providing access to information not otherwise available. It will also automatically lock if the watch was removed.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **Connected devices** heading
6. Verify that **Force Apple Watch wrist detection** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **Wrist detection enforced on Apple Watch** is displayed

Remediation:







From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **Connected devices** heading
6. Set **Force Apple Watch wrist detection** to **Yes**

Default Value:

Not configured

CIS Controls:

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

2.4.2 Ensure "Require AirPlay outgoing requests pairing password" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Unsupervised Devices

Description:

This restriction enforces the requirement of a pairing password when using AirPlay to stream content to a new Apple device.

Rationale:

This will mitigate the risk of accidental casting of content to an incorrect screen. It will also reduce the effectiveness of a spoofing style attack.

Impact:

Users will have to authenticate to new Airplay devices via a password before first use.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **Connected devices** heading
6. Verify that **Require AirPlay outgoing requests pairing password** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **AirPlay outgoing requests pairing password enforced** is displayed

Remediation:







From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **Connected devices** heading
6. Set **Require AirPlay outgoing requests pairing password** to **Yes**

Default Value:

Not configured

CIS Controls:

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

2.4.3 Ensure "Block Apple Watch auto unlock" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Unsupervised Devices

Description:

This will restrict users from being able to automatically unlock their Apple Watch when they unlock their iOS/iPadOS device.

Rationale:

If an Apple Watch is connected to the user's iOS/iPadOS device, but is not on their person, this could result in the user unintentionally unlocking their Apple Watch, allowing access to sensitive information on the device.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **Connected devices** heading
6. Verify that **Block Apple Watch auto unlock** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **Phone auto unlock not allowed** is displayed

Remediation:







From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **Connected devices** heading
6. Set **Block Apple Watch auto unlock** to **Yes**

Default Value:

Not configured

CIS Controls:

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

2.5 General

2.5.1 Ensure "Block sending diagnostic and usage data to Apple" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Unsupervised Devices

Description:

Apple provides a mechanism to send diagnostic and analytics data back to them in order to help improve the platform. This information sent to Apple may contain internal organizational information that should not be disclosed to third parties.

Rationale:

Organizations should have knowledge of what is shared with vendors and other third parties, and should also be in full control of what is disclosed.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **General** heading
6. Verify that **Block sending diagnostic and usage data to Apple** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **Diagnostic submission not allowed** is displayed

Remediation:





From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **General** heading
6. Set **Block sending diagnostic and usage data to Apple** to **Yes**

Default Value:

Not configured

CIS Controls:

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

2.5.2 Ensure "Block screenshots and screen recording" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Unsupervised Devices

Description:

This recommendation limits screen recording and the ability to screenshot from the device.

Rationale:

Sensitive information displayed on the device may be captured by screenshot or screen recording into an unmanaged storage location intentionally or unintentionally by a user.

Impact:

Screenshots and screen recordings will be disabled entirely.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **General** heading
6. Verify that **Block screenshots and screen recording** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **Screen capture not allowed** is displayed

Remediation:







From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **General** heading
6. Set **Block screenshots and screen recording** to **Yes**

Default Value:

Not configured

CIS Controls:

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

2.5.3 Ensure "Block untrusted TLS certificates" is set to "Yes" (Manual)

Profile Applicability:

- Level 2 - Unsupervised Devices

Description:

This recommendation blocks untrusted Transport Layer Security (TLS) certificates.

Rationale:

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

Impact:

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

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **General** heading
6. Verify that **Block untrusted TLS certificates** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **Establishing untrusted TLS connections not allowed** is displayed

Remediation:







From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **General** heading
6. Set **Block untrusted TLS certificates** to **Yes**

Default Value:

Not configured

CIS Controls:

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

2.5.4 Ensure "Force limited ad tracking" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Unsupervised Devices

Description:

This recommendation disables the ad identifier that is used to link advertisement information to a device.

Rationale:

Having this enabled allows ad companies to better track and harvest information from a device.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **General** heading
6. Verify that **Force limited ad tracking** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **Requests to track from apps not allowed** is displayed

Remediation:





From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **General** heading
6. Set **Force limited ad tracking** to **Yes**

Default Value:

Not configured

CIS Controls:

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

2.5.5 Ensure "Block trusting new enterprise app authors" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Unsupervised Devices

Description:

This recommendation disables application installation by end users from outside the Apple App Store or Mobile Device Management (MDM) deployment.

Rationale:

Allowing application installation by end users from outside of the Apple App Store or Mobile Device Management (MDM) may permit a user to intentionally or unintentionally install a malicious application.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **General** heading
6. Verify that **Block trusting new enterprise app authors** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **Trusting enterprise apps not allowed** is displayed

Remediation:







From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **General** heading
6. Set **Block trusting new enterprise app authors** to **Yes**

Default Value:

Not configured

CIS Controls:

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

2.5.6 Ensure "Limit Apple personalized advertising" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Unsupervised Devices

Description:

Apple provides a framework that allows advertisers to target Apple users with advertisements relevant to them and their interests by means of a unique identifier. For such personalized advertisements to be delivered, however, detailed information is collected, correlated, and made available to advertisers. This information is valuable to both advertisers and attackers and has been used with other metadata to reveal users' identities.

Rationale:

Disabling the use of a unique identifier helps hinder the tracking of users, which in turn supports protection of user data.

Impact:

Users will see generic advertising rather than targeted advertising. Apple has warned that this will reduce the number of relevant ads.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **General** heading
6. Verify that **Limit Apple personalized advertising** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **Apple personalized advertising not allowed** is displayed

Remediation:





From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **General** heading
6. Set **Limit Apple personalized advertising** to **Yes**

Default Value:

Not configured

CIS Controls:

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

2.6 Locked Screen Experience

2.6.1 Ensure "Block Control Center access in lock screen" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Unsupervised Devices

Description:

This restriction prevents access to the Control Center on the lock screen. Passcode/Face ID must be set for this to apply.

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. Further information such as media recently played, alarm information, and latest calculator history can also be seen.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **Locked Screen Experience** heading
6. Verify that **Block Control Center access in lock screen** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **Control Center on lock screen not allowed** is displayed

Remediation:







From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **Locked Screen Experience** heading
6. Set **Block Control Center access in lock screen** to **Yes**

Default Value:

Not configured

CIS Controls:

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

2.6.2 Ensure "Block Notifications Center access in lock screen" is set to "Yes" (Manual)

Profile Applicability:

- Level 2 - Unsupervised Devices

Description:

This restriction prevents access to the Notifications Center on the lock screen. This does not restrict or limit information displayed from notifications, only older notifications that are stored in the notification center. This is usually visible by swiping up on the lock screen.

Rationale:

This will block older notifications from being displayed on the lock screen. The introduction of the notification center is a location where unaddressed notifications often reside.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **Locked Screen Experience** heading
6. Verify that **Block Notifications Center access in lock screen** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **Notifications view on lock screen not allowed** is displayed

Remediation:







From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **Locked Screen Experience** heading
6. Set **Block Notifications Center access in lock screen** to **Yes**

Default Value:

Not configured

CIS Controls:

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

2.6.3 Ensure "Block Today view in lock screen" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Unsupervised Devices

Description:

This restriction prevents access to the Today View and search on the lock screen. This can be seen by swiping left on the lock screen. A Passcode/Face ID must be set for this to apply.

Rationale:

This will block sensitive information from being displayed on the lock screen. Today View allows widgets and reminders to be displayed, as well as the option to list installed applications and other Siri suggestions.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **Locked Screen Experience** heading
6. Verify that **Block Today view in lock screen** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **Today view on lock screen not allowed** is displayed

Remediation:







From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **Locked Screen Experience** heading
6. Set **Block Today view in lock screen** to **Yes**

Default Value:

Not configured

CIS Controls:

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

2.6.4 Ensure "Block Wallet notifications in lock screen" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Unsupervised Devices

Description:

This restriction prevents access to the Apple Wallet while the screen is locked. Passcode/Face ID must be set for this to apply.

Rationale:

This will block the option for the Apple Wallet to be used while the screen is locked.

Impact:

The device will need to be unlocked to access the Wallet.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **Locked Screen Experience** heading
6. Verify that **Block Wallet notifications in lock screen** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **Passbook not allowed** is displayed

Remediation:







From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **Locked Screen Experience** heading
6. Set **Block Wallet notifications in lock screen** to **Yes**

Default Value:

Not configured

CIS Controls:

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

2.7 Password

2.7.1 Ensure "Require password" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Unsupervised Devices

Description:

This restriction enforces a password to be set on the device.

Rationale:

This will block the option for the device to be used without a password.

Impact:

A user will need to set a password to use the device.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **Password** heading
6. Verify that **Require password** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Tap **Passcode**
7. Confirm **Passcode required** is present and its value is **yes**

Remediation:






From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **Password** heading
6. Set **Require password** to **Yes**

Default Value:

Not configured

CIS Controls:

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

2.7.2 Ensure "Block simple passwords" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Unsupervised Devices

Description:

This restriction enforces a block on simple passwords on the device. Passwords such as 1234 and 0000 would be blocked.

Rationale:

This will block the option for a simple password to be used on the device.

Impact:

Those with passwords that do not meet this requirement will be prompted to set a new device password.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **Password** heading
6. Verify that **Block simple passwords** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Tap **Passcode**
7. Confirm **Simple passcodes allowed** is present and its value is **No**

Remediation:






From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **Password** heading
6. Set **Block simple passwords** to **Yes**

Default Value:

Not configured

CIS Controls:

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

2.7.3 Ensure "Required password type" is set to "Alphanumeric" (Manual)

Profile Applicability:

- Level 2 - Unsupervised Devices

Description:

This restriction enforces an alphanumeric password on the device. Numeric-only passcode pins would not be allowed.

Rationale:

Alphanumeric passwords provide a greater security posture by increasing the number of possible combinations, as well as not providing an indicator of password length.

Impact:

Those with passwords that do not meet this requirement will be prompted to set a new device password.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **Password** heading
6. Verify that **Required password type** is present and set to **Alphanumeric**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Tap **Passcode**
7. Confirm **Alphanumeric required** is present and its value is **Yes**

Remediation:






From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **Password** heading
6. Set **Required password type** to **Alphanumeric**

Default Value:

Not configured

CIS Controls:

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

2.7.4 Ensure "Minimum password length" is set to "6" or greater (Manual)

Profile Applicability:

- Level 1 - Unsupervised Devices

Description:

This restriction requires the password length set on the device to be 6 or greater.

Rationale:

Longer passwords provide a greater security posture by increasing the number of possible combinations.

Impact:

Those with passwords that do not meet this requirement will be prompted to set a new device password.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **Password** heading
6. Verify that **Minimum password length** is present and set to **6** or greater

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Tap **Passcode**
7. Confirm **Minimum length** is present and its value is **6** or greater

Remediation:






From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **Password** heading
6. Set **Minimum password length** to **6** or greater

Default Value:

Not configured

CIS Controls:

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

2.7.5 Ensure "Maximum minutes after screen lock before password is required" is set to "Immediately" (Manual)

Profile Applicability:

- Level 1 - Unsupervised Devices

Description:

This restriction disables any grace period where a password is not required to be entered after the screen has locked.

Rationale:

This would make it impossible for the device to be picked up and used after the screen has locked.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **Password** heading
6. Verify that **Maximum minutes after screen lock before password is required** is present and set to **Immediately**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Tap **Passcode**
7. Confirm **Max grace period** is present and its value is **Immediately**

Remediation:







From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **Password** heading
6. Set **Maximum minutes after screen lock before password is required** to **Immediately**

Default Value:

Not configured

CIS Controls:

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

2.7.6 Ensure "Maximum minutes of inactivity until screen locks" is set to "2" or less (Manual)

Profile Applicability:

- Level 1 - Unsupervised Devices

Description:

This restriction sets the maximum time of inactivity before the device will be automatically locked.

Rationale:

This would mitigate the concern of an unattended device being picked up and used, as the window of inactivity has been set.

Impact:

This is not enforced during certain activities, such as watching video content.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **Password** heading
6. Verify that **Maximum minutes of inactivity until screen locks** is present and set to **2** or less

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Tap **Passcode**
7. Confirm **Max inactivity** is present and its value is **2 minutes**

Remediation:







From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **Password** heading
6. Set **Maximum minutes of inactivity until screen locks** to **2** or less

Default Value:

Not configured

CIS Controls:

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

2.7.7 Ensure "Block Touch ID and Face ID unlock" is set to "Yes" (Manual)

Profile Applicability:

- Level 2 - Unsupervised Devices

Description:

This restriction blocks Touch ID and Face ID being used to unlock the device. A standard passcode/password will be the only form of authentication to unlock the device.

If this is not set, passcode/password will still be required after a device power-cycles or the device has been reported as lost.

Rationale:

This would address the concern of a malicious individual using the face/touch identification of the device owner as a means of authentication for the device.

Impact:

A passcode/password will be required to unlock the device.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **Password** heading
6. Verify that **Block Touch ID and Face ID unlock** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **Touch ID unlock not allowed** or **Face ID unlock not allowed** is displayed

Remediation:







From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **Password** heading
6. Set **Block Touch ID and Face ID unlock** to **Yes**

Default Value:

Not configured

CIS Controls:

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

2.8 Wireless

2.8.1 Ensure "Block voice dialing while device is locked" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Unsupervised Devices

Description:

This restriction blocks initiating phone calls from a locked device. Voice dialing is handled separately from Siri.

Rationale:

Allowing calls from a locked device may allow for the impersonation of the device owner, or other malicious actions.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **Wireless** heading
6. Verify that **Block voice dialing while device is locked** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **Voice dialing while locked not allowed** is displayed

Remediation:







From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **Wireless** heading
6. Set **Block voice dialing while device is locked** to **Yes**

Default Value:

Not configured

CIS Controls:

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

3 Recommendations for Supervised (Organization) 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 regard to the state of an iOS or iPadOS device and is generally only applied to institutionally-owned devices. See the Benchmark Guidance section of this benchmark for clarification on supervised and unsupervised states.

3.1 App Store, Doc Viewing, Gaming

3.1.1 Ensure "Block viewing corporate documents in unmanaged apps" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Supervised Devices

Description:

This prevents viewing corporate documents in unmanaged apps.

Rationale:

By default, depending on per app policies, the OS might allow corporate documents to be viewed in any app.

Impact:

Third party keyboards may not function correctly with this restriction set.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **App Store, Doc Viewing, Gaming** heading
6. Verify that **Block viewing corporate documents in unmanaged apps** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **Opening documents from managed to unmanaged apps not allowed** is displayed

Remediation:







From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **App Store, Doc Viewing, Gaming** heading
6. Set **Block viewing corporate documents in unmanaged apps** to **Yes**

Default Value:

Not configured

CIS Controls:

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

3.1.2 Ensure "Treat AirDrop as an unmanaged destination" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Supervised Devices

Description:

This forces AirDrop to be considered an unmanaged drop target.

Rationale:

This stops managed apps data from being sent via Airdrop.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **App Store, Doc Viewing, Gaming** heading
6. Verify that **Treat AirDrop as an unmanaged destination** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **Sharing managed documents using AirDrop not allowed** is displayed

Remediation:







From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **App Store, Doc Viewing, Gaming** heading
6. Set **Treat AirDrop as an unmanaged destination** to **Yes**

Default Value:

Not configured

CIS Controls:

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

3.1.3 Ensure "Allow copy/paste to be affected by managed open-in" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Supervised Devices

Description:

This enforces copy/paste restrictions based on configured Block viewing corporate documents in unmanaged apps and Block viewing non-corporate documents in corporate apps.

Rationale:

This can ensure that copy/paste restrictions set by managed apps are enforced.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **App Store, Doc Viewing, Gaming** heading
6. Verify that **Allow copy/paste to be affected by managed open-in** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **Copy and paste are managed** is displayed

Remediation:







From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **App Store, Doc Viewing, Gaming** heading
6. Set **Allow copy/paste to be affected by managed open-in** to **Yes**

Default Value:

Not configured

CIS Controls:

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

3.1.4 Ensure "Block App Store" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Supervised Devices

Description:

This prevents access to the App Store on supervised devices.

Rationale:

Blocking the App Store will deny users the ability to install apps that have not been explicitly approved by the organization. Allowing users to install apps could introduce malicious applications designed to exfiltrate information intentionally or unintentionally by a user.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **App Store, Doc Viewing, Gaming** heading
6. Verify that **Block App store** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **Installing apps not allowed** is displayed

Remediation:







From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **App Store, Doc Viewing, Gaming** heading
6. Set **Block App store** to **Yes**

Default Value:

Not configured

CIS Controls:

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

3.1.5 Ensure "Block access to network drive in Files app" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Supervised Devices

Description:

This prevents access to networked file shares, such as SMB network drives.

Rationale:

Network drives can be used as an unmanaged storage location for transferring data to and from iOS/iPadOS devices.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **App Store, Doc Viewing, Gaming** heading
6. Verify that **Block access to network drive in Files app** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **Network drives not accessible in Files app** is displayed

Remediation:





From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **App Store, Doc Viewing, Gaming** heading
6. Set **Block access to network drive in Files app** to **Yes**

Default Value:

Not configured

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>1.2 Address Unauthorized Assets</u> Ensure that a process exists to address unauthorized assets on a weekly basis. The enterprise may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.			
v7	<u>13.3 Monitor and Block Unauthorized Network Traffic</u> Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals.			

3.2 Built-in Apps

3.2.1 Ensure "Block Siri while device is locked" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Supervised Devices

Description:

This prevents access to Siri when the device is locked.

Rationale:

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

Impact:

The end user must unlock the device before interacting with Siri.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **Built-in apps** heading
6. Verify that **Block Siri while device is locked** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **Siri while locked not allowed** is displayed

Remediation:







From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **Built-in apps** heading
6. Set **Block Siri while device is locked** to **Yes**

Default Value:

Not configured

CIS Controls:

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

3.2.2 Ensure "Require Safari fraud warnings" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Supervised Devices

Description:

This enforces the feature to display fraud warnings within the Safari web browser.

Rationale:

Fraudulent websites masquerade as legitimate instances of financial, business, or other sensitive 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.

For increased security, the Safari web browser should be used to enforce fraud warnings.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **Built-in apps** heading
6. Verify that **Require Safari fraud warnings** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **Safari fraud warning enforced** is displayed

Remediation:





From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **Built-in apps** heading
6. Set **Require Safari fraud warnings** to **Yes**

Default Value:

Not configured

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.4 <u>Restrict Unnecessary or Unauthorized Browser and Email Client Extensions</u> Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.			
v7	7.2 <u>Disable Unnecessary or Unauthorized Browser or Email Client Plugins</u> Uninstall or disable any unauthorized browser or email client plugins or add-on applications.			

3.3 Cloud and Storage

3.3.1 Ensure "Force encrypted backup" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Supervised Devices

Description:

This requires device backups to be stored in an encrypted state.

Rationale:

Data that are stored securely on an iOS or iPadOS 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.

Impact:

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

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **Cloud and Storage** heading
6. Verify that **Force encrypted backup** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **Encrypted backups enforced** is displayed

Remediation:







From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **Cloud and Storage** heading
6. Set **Force encrypted backup** to **Yes**

Default Value:

Not configured

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	11.3 <u>Protect Recovery Data</u> Protect recovery data with equivalent controls to the original data. Reference encryption or data separation, based on requirements.			
v7	10.4 <u>Ensure Protection of Backups</u> 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.			

3.3.2 Ensure "Block managed apps from storing data in iCloud" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Supervised Devices

Description:

This prevents managed apps from storing and syncing data to the user's iCloud account.

Rationale:

This recommendation addresses intentional or unintentional data leakage. It prevents a user from installing an application that is managed by the organization on a personal device and allowing iCloud to sync the managed application's data to the personal, non-managed application.

Impact:

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

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **Cloud and Storage** heading
6. Verify that **Block managed apps from storing data in iCloud** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **Managed apps cloud sync not allowed** is displayed

Remediation:






From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **Cloud and Storage** heading
6. Set **Block managed apps from storing data in iCloud** to **Yes**

Default Value:

Not configured

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.3 Address Unauthorized Software Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.			
v7	13.4 Only Allow Access to Authorized Cloud Storage or Email Providers Only allow access to authorized cloud storage or email providers.			

3.3.3 Ensure "Block backup of enterprise books" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Supervised Devices

Description:

This prevents backing up of enterprise books.

Rationale:

This recommendation addresses intentional or unintentional data leakage. It prevents a user from backing up enterprise books (documents handled by the Books application).

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **Cloud and Storage** heading
6. Verify that **Block backup of enterprise books** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **Backing up enterprise books not allowed** is displayed

Remediation:






From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **Cloud and Storage** heading
6. Set **Block backup of enterprise books** to **Yes**

Default Value:

Not configured

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.3 Address Unauthorized Software Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.			
v7	13.4 <u>Only Allow Access to Authorized Cloud Storage or Email Providers</u> Only allow access to authorized cloud storage or email providers.			

3.3.4 Ensure "Block notes and highlights sync for enterprise books" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Supervised Devices

Description:

This prevents syncing notes and highlights in enterprise books.

Rationale:

Notes and highlights of text created within enterprise books may contain sensitive information that should not be backed up.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **Cloud and Storage** heading
6. Verify that **Block notes and highlights sync for enterprise books** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **Synchronizing enterprise books notes and highlights not allowed** is displayed

Remediation:






From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **Cloud and Storage** heading
6. Set **Block notes and highlights sync for enterprise books** to **Yes**

Default Value:

Not configured

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.3 Address Unauthorized Software Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.			
v7	13.4 Only Allow Access to Authorized Cloud Storage or Email Providers Only allow access to authorized cloud storage or email providers.			

3.3.5 Ensure "Block iCloud Photos sync" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Supervised Devices

Description:

This prevents photo stream syncing to iCloud.

Rationale:

This stops the ability to share pictures and screenshots to cloud storage that can be accessed outside your organization's network or devices.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **Cloud and Storage** heading
6. Verify that **Block iCloud Photos sync** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **Photo Stream not allowed** is displayed

Remediation:






From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **Cloud and Storage** heading
6. Set **Block iCloud Photos sync** to **Yes**

Default Value:

Not configured

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.3 Address Unauthorized Software Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.			
v7	13.4 <u>Only Allow Access to Authorized Cloud Storage or Email Providers</u> Only allow access to authorized cloud storage or email providers.			

3.3.6 Ensure "Block iCloud Photo Library" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Supervised Devices

Description:

This prevents photo Library syncing to iCloud.

Rationale:

This stops the ability to share pictures and screenshots to cloud storage that can be accessed outside your organization's network or devices.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **Cloud and Storage** heading
6. Verify that **Block iCloud Photo Library** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **iCloud Photos not allowed** is displayed

Remediation:






From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **Cloud and Storage** heading
6. Set **Block iCloud Photo Library** to **Yes**

Default Value:

Not configured

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.3 Address Unauthorized Software Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.			
v7	13.4 <u>Only Allow Access to Authorized Cloud Storage or Email Providers</u> Only allow access to authorized cloud storage or email providers.			

3.3.7 Ensure "Block My Photo Stream" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Supervised Devices

Description:

This disables iCloud Photo Sharing.

Rationale:

This stops the ability to share pictures and screenshots to cloud storage that can be accessed outside your organization's network or devices.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **Cloud and Storage** heading
6. Verify that **Block My Photo Stream** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **Shared Streams not allowed** is displayed

Remediation:






From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **Cloud and Storage** heading
6. Set **Block My Photo Stream** to **Yes**

Default Value:

Not configured

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.3 Address Unauthorized Software Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.			
v7	13.4 Only Allow Access to Authorized Cloud Storage or Email Providers Only allow access to authorized cloud storage or email providers.			

3.3.8 Ensure "Block Handoff" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Supervised Devices

Description:

This prevents Apple's Handoff data-sharing mechanism, allowing users to carry on tasks on another iOS/iPadOS or macOS device.

Rationale:

Impact:

Handoff does not enforce managed application boundaries. This allows managed application data to be moved to the unmanaged application space on another device, which may allow for intentional or unintentional data leakage

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **Cloud and Storage** heading
6. Verify that **Block Handoff** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **Handoff not allowed** is displayed

Remediation:







From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **Cloud and Storage** heading
6. Set **Block Handoff** to **Yes**

Default Value:

Not configured

CIS Controls:

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

3.3.9 Ensure "Block iCloud backup" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Supervised Devices

Description:

This prevents the function of iCloud on the device being backed up to iCloud.

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 potentially allows for intentional or unintentional data leakage.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **Cloud and Storage** heading
6. Verify that **Block iCloud backup** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **iCloud backup not allowed** is displayed

Remediation:






From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **Cloud and Storage** heading
6. Set **Block iCloud backup** to **Yes**

Default Value:

Not configured

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.3 Address Unauthorized Software Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.			
v7	13.4 <u>Only Allow Access to Authorized Cloud Storage or Email Providers</u> Only allow access to authorized cloud storage or email providers.			

3.3.10 Ensure "Block iCloud document and data sync" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Supervised Devices

Description:

This prevents syncing of documents and data to iCloud.

Rationale:

Managed devices are often connected to personal iCloud accounts. This is expected and normal. The data from managed devices, however, should not co-mingle with the end-user's personal data. This creates a potential avenue for intentional or unintentional data leakage.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **Cloud and Storage** heading
6. Verify that **Block iCloud document and data sync** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **Documents in the Cloud not allowed** is displayed

Remediation:






From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **Cloud and Storage** heading
6. Set **Block iCloud document and data sync** to **Yes**

Default Value:

Not configured

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.3 Address Unauthorized Software Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.			
v7	13.4 Only Allow Access to Authorized Cloud Storage or Email Providers Only allow access to authorized cloud storage or email providers.			

3.3.11 Ensure "Block iCloud Keychain sync" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Supervised Devices

Description:

This prevents syncing of credentials with the iCloud Keychain. Keychain allows passwords associated with an Apple ID to be saved and available for use to the authenticated user for the Apple account.

Rationale:

Enterprise credentials may be stored within Keychain, resulting in these credentials being stored within a user's Apple ID.

Managed devices are often connected to personal iCloud accounts. This is expected and normal. The credentials from managed devices, however, should not co-mingle with the end-user's personal data. This creates a potential avenue for intentional or unintentional data leakage.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **Cloud and Storage** heading
6. Verify that **Block iCloud Keychain sync** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **iCloud Keychain not allowed** is displayed

Remediation:













From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **Cloud and Storage** heading
6. Set **Block iCloud Keychain sync** to **Yes**

Default Value:

Not configured

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v8	15.3 Classify Service Providers Classify service providers. Classification consideration may include one or more characteristics, such as data sensitivity, data volume, availability requirements, applicable regulations, inherent risk, and mitigated risk. Update and review classifications annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.			
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

3.4 Connected Devices

3.4.1 Ensure "Force Apple Watch wrist detection" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Supervised Devices

Description:

This restriction forces wrist detection to be enabled to paired Apple Watches. When enforced, the Apple Watch won't display notifications when it's not being worn. The Apple Watch will also lock itself when it has been removed from a user's wrist.

Rationale:

Wrist detection prevents a removed Apple Watch from providing access to information not otherwise available. It will also automatically lock if the watch was removed.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **Connected devices** heading
6. Verify that **Force Apple Watch wrist detection** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **Wrist detection enforced on Apple Watch** is displayed

Remediation:







From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **Connected devices** heading
6. Set **Force Apple Watch wrist detection** to **Yes**

Default Value:

Not configured

CIS Controls:

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

3.4.2 Ensure "Require AirPlay outgoing requests pairing password" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Supervised Devices

Description:

This restriction enforces the requirement of a pairing password when using AirPlay to stream content to a new Apple device.

Rationale:

This will mitigate the risk of accidental casting of content to an incorrect screen. It will also reduce the effectiveness of a spoofing style attack.

Impact:

Users will have to authenticate to new Airplay devices via a password before first use.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **Connected devices** heading
6. Verify that **Require AirPlay outgoing requests pairing password** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **AirPlay outgoing requests pairing password enforced** is displayed

Remediation:







From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **Connected devices** heading
6. Set **Require AirPlay outgoing requests pairing password** to **Yes**

Default Value:

Not configured

CIS Controls:

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

3.4.3 Ensure "Block Apple Watch auto unlock" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Supervised Devices

Description:

This will restrict users from being able to automatically unlock their Apple Watch when they unlock their iOS/iPadOS device.

Rationale:

If an Apple Watch is connected to the user's iOS/iPadOS device, but is not on their person, this could result in the user unintentionally unlocking their Apple Watch, allowing access to sensitive information on the device.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **Connected devices** heading
6. Verify that **Block Apple Watch auto unlock** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **Phone auto unlock not allowed** is displayed

Remediation:







From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **Connected devices** heading
6. Set **Block Apple Watch auto unlock** to **Yes**

Default Value:

Not configured

CIS Controls:

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

3.4.4 Ensure "Block iBeacon discovery of AirPrint printers" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Supervised Devices

Description:

This blocks the iBeacon function that allows users to discover nearby AirPrint Printers.

Rationale:

This will aim to prevent malicious network traffic phishing attacks using AirPrint beacons.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **Connected devices** heading
6. Verify that **Block iBeacon discovery of AirPrint printers** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **AirPrint iBeacon discovery not allowed** is displayed

Remediation:







From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **Connected devices** heading
6. Set **Block iBeacon discovery of AirPrint printers** to **Yes**

Default Value:

Not configured

CIS Controls:

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

3.4.5 Ensure "Block access to USB drive in Files app" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Supervised Devices

Description:

This will prevent the Files app from accessing USB media to view and/or transfer files.

Rationale:

The Files app provides a local file system and interface to USB media for iOS and iPadOS devices. In environments with sensitive data and strict data loss prevention policies, disabling the use of USB media with such devices may reduce the risk of intentional or unintentional data leakage.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **Connected devices** heading
6. Verify that **Block access to USB drive in Files app** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **USB drives not accessible in Files app** is displayed

Remediation:






From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **Connected devices** heading
6. Set **Block access to USB drive in Files app** to **Yes**

Default Value:

Not configured

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	1.2 Address Unauthorized Assets Ensure that a process exists to address unauthorized assets on a weekly basis. The enterprise may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.			
v7	13.7 Manage USB Devices If USB storage devices are required, enterprise software should be used that can configure systems to allow the use of specific devices. An inventory of such devices should be maintained.			

3.5 General

3.5.1 Ensure "Block sending diagnostic and usage data to Apple" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Supervised Devices

Description:

Apple provides a mechanism to send diagnostic and analytics data back to them in order help improve the platform. This information sent to Apple may contain internal organizational information that should not be disclosed to third parties.

Rationale:

Organizations should have knowledge of what is shared with vendors and other third parties, and should also be in full control of what is disclosed.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **General** heading
6. Verify that **Block sending diagnostic and usage data to Apple** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **Diagnostic submission not allowed** is displayed

Remediation:





From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **General** heading
6. Set **Block sending diagnostic and usage data to Apple** to **Yes**

Default Value:

Not configured

CIS Controls:

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

3.5.2 Ensure "Block screenshots and screen recording" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Supervised Devices

Description:

This recommendation limits screen recording and the ability to screenshot from the device.

Rationale:

Sensitive information displayed on the device may be captured by screenshot or screen recording into an unmanaged storage location intentionally or unintentionally by a user.

Impact:

Screenshots and screen recordings will be disabled entirely.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **General** heading
6. Verify that **Block screenshots and screen recording** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **Screen capture not allowed** is displayed

Remediation:







From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **General** heading
6. Set **Block screenshots and screen recording** to **Yes**

Default Value:

Not configured

CIS Controls:

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

3.5.3 Ensure "Block untrusted TLS certificates" is set to "Yes" (Manual)

Profile Applicability:

- Level 2 - Supervised Devices

Description:

This recommendation blocks untrusted Transport Layer Security (TLS) certificates.

Rationale:

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

Impact:

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

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **General** heading
6. Verify that **Block untrusted TLS certificates** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **Establishing untrusted TLS connections not allowed** is displayed

Remediation:







From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **General** heading
6. Set **Block untrusted TLS certificates** to **Yes**

Default Value:

Not configured

CIS Controls:

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

3.5.4 Ensure "Force limited ad tracking" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Supervised Devices

Description:

This recommendation disables the ad identifier that is used to link advertisement information to a device.

Rationale:

Having this enabled allows ad companies to better track and harvest information from a device.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **General** heading
6. Verify that **Force limited ad tracking** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **Requests to track from apps not allowed** is displayed

Remediation:





From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **General** heading
6. Set **Force limited ad tracking** to **Yes**

Default Value:

Not configured

CIS Controls:

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

3.5.5 Ensure "Block trusting new enterprise app authors" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Supervised Devices

Description:

This recommendation disables application installation by end users from outside the Apple App Store or Mobile Device Management (MDM) deployment.

Rationale:

Allowing application installation by end users from outside of the Apple App Store or Mobile Device Management (MDM) may permit a user to intentionally or unintentionally install a malicious application.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **General** heading
6. Verify that **Block trusting new enterprise app authors** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **Trusting enterprise apps not allowed** is displayed

Remediation:







From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **General** heading
6. Set **Block trusting new enterprise app authors** to **Yes**

Default Value:

Not configured

CIS Controls:

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

3.5.6 Ensure "Limit Apple personalized advertising" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Supervised Devices

Description:

Apple provides a framework that allows advertisers to target Apple users with advertisements relevant to them and their interests by means of a unique identifier. For such personalized advertisements to be delivered, however, detailed information is collected, correlated, and made available to advertisers. This information is valuable to both advertisers and attackers and has been used with other metadata to reveal users' identities.

Rationale:

Disabling the use of a unique identifier helps hinder the tracking of users, which in turn supports protection of user data.

Impact:

Users will see generic advertising rather than targeted advertising. Apple has warned that this will reduce the number of relevant ads.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **General** heading
6. Verify that **Limit Apple personalized advertising** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **Apple personalized advertising not allowed** is displayed

Remediation:





From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **General** heading
6. Set **Limit Apple personalized advertising** to **Yes**

Default Value:

Not configured

CIS Controls:

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

3.5.7 Ensure "Block users from erasing all content and settings on device" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Supervised Devices

Description:

This restriction prevents the "erase all content and settings" option on devices.

Rationale:

An organization-owned device should not allow an end user to destroy data and/or repurpose the device.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **General** heading
6. Verify that **Block users from erasing all content and settings on device** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **Erase content and settings not allowed** is displayed

Remediation:







From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **General** heading
6. Set **Block users from erasing all content and settings on device** to **Yes**

Default Value:

Not configured

CIS Controls:

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

3.5.8 Ensure "Block modification of device name" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Supervised Devices

Description:

This restriction prevents a user from having the ability to change the name of the device. The device name is visible and can be changed from this location: Settings > General > About

Rationale:

Giving users the ability to change their device name at any point may hinder the functionality of device identification and asset tracking.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **General** heading
6. Verify that **Block modification of device name** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **Device name modification not allowed** is displayed

Remediation:






From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **General** heading
6. Set **Block modification of device name** to **Yes**

Default Value:

Not configured

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	1.1 <u>Establish and Maintain Detailed Enterprise Asset Inventory</u> Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, enterprise asset owner, department for each asset, and whether the asset has been approved to connect to the network. For mobile end-user devices, MDM type tools can support this process, where appropriate. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise. Review and update the inventory of all enterprise assets bi-annually, or more frequently.			
v7	9.1 <u>Associate Active Ports, Services and Protocols to Asset Inventory</u> Associate active ports, services and protocols to the hardware assets in the asset inventory.			

3.5.9 Ensure "Block configuration profile changes" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Supervised Devices

Description:

This restriction prevents a user from intentionally or unintentionally installing additional configuration profiles.

Rationale:

This adds an additional security control, so third-party and potentially malicious configuration profiles can not be installed.

Impact:

Some services, such as WiFi access points that have been configured requiring a user to install a configuration profile, may be prevented from working by blocking their configuration profiles.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **General** heading
6. Verify that **Block configuration profile changes** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **Installing configuration profiles not allowed** is displayed

Remediation:







From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **General** heading
6. Set **Block configuration profile changes** to **Yes**

Default Value:

Not configured

CIS Controls:

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

3.5.10 Ensure "Allow activation lock" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Supervised Devices

Description:

This restriction enables Activation Lock on devices. This feature is commonly seen when a device is marked as lost in the Apple Find My app.

Rationale:

The Activation Lock feature increases the security of the device, and restricts functionality if the device has been marked as lost or stolen.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **General** heading
6. Verify that **Allow activation lock** is present and set to **Yes**

This restriction can not be audited from the device.

Remediation:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **General** heading
6. Set **Allow activation lock** to **Yes**

Default Value:

Not configured

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.13 <u>Deploy a Data Loss Prevention Solution</u> Implement an automated tool, such as a host-based Data Loss Prevention (DLP) tool to identify all sensitive data stored, processed, or transmitted through enterprise assets, including those located onsite or at a remote service provider, and update the enterprise's sensitive data inventory.			●
v7	14.5 <u>Utilize an Active Discovery Tool to Identify Sensitive Data</u> Utilize an active discovery tool to identify all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located onsite or at a remote service provider and update the organization's sensitive information inventory.			●

3.5.11 Ensure "Force automatic date and time" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Supervised Devices

Description:

This restriction forces automatic date and time to be used on the device. The time zone updates only when the device can determine its location, such as when a device has a cellular connection or a Wi-Fi connection with location services enabled.

Rationale:

Correct date and time settings are required for authentication protocols, file creation, modification dates, and log entries. Having this information accurate is important in incident response and forensic investigations.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **General** heading
6. Verify that **Force automatic date and time** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **Automatic date & time enforced** is displayed

Remediation:





From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **General** heading
6. Set **Force automatic date and time** to **Yes**

Default Value:

Not configured

CIS Controls:

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

3.5.12 Ensure "Block VPN creation" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Supervised Devices

Description:

This restriction prevents a user from intentionally or unintentionally creating VPN configuration.

Rationale:

A VPN configuration can route traffic via unsecure systems if this has not been configured safely.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **General** heading
6. Verify that **Block VPN creation** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **VPN creation not allowed** is displayed

Remediation:





From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **General** heading
6. Set **Block VPN creation** to **Yes**

Default Value:

Not configured

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v7	14.4 <u>Encrypt All Sensitive Information in Transit</u> Encrypt all sensitive information in transit.			

3.6 Locked Screen Experience

3.6.1 Ensure "Block Control Center access in lock screen" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Supervised Devices

Description:

This restriction prevents access to the Control Center on the lock screen. Passcode/Face ID must be set for this to apply.

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. Further information such as media recently played, alarm information, and latest calculator history can also be seen.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **Locked Screen Experience** heading
6. Verify that **Block Control Center access in lock screen** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **Control Center on lock screen not allowed** is displayed

Remediation:







From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **Locked Screen Experience** heading
6. Set **Block Control Center access in lock screen** to **Yes**

Default Value:

Not configured

CIS Controls:

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

3.6.2 Ensure "Block Notifications Center access in lock screen" is set to "Yes" (Manual)

Profile Applicability:

- Level 2 - Supervised Devices

Description:

This restriction prevents access to the Notifications Center on the lock screen. This does not restrict or limit information displayed from notifications, only older notifications that are stored in the notification center. This is usually visible by swiping up on the lock screen.

Rationale:

This will block older notifications from being displayed on the lock screen. The introduction of the notification center is a location where unaddressed notifications often reside.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **Locked Screen Experience** heading
6. Verify that **Block Notifications Center access in lock screen** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **Notifications view on lock screen not allowed** is displayed

Remediation:







From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **Locked Screen Experience** heading
6. Set **Block Notifications Center access in lock screen** to **Yes**

Default Value:

Not configured

CIS Controls:

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

3.6.3 Ensure "Block Today view in lock screen" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Supervised Devices

Description:

This restriction prevents access to the Today View and search on the lock screen. This can be seen by swiping left on the lock screen. A Passcode/Face ID must be set for this to apply.

Rationale:

This will block sensitive information from being displayed on the lock screen. Today View allows widgets and reminders to be displayed, as well as the option to list installed applications and other Siri suggestions.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **Locked Screen Experience** heading
6. Verify that **Block Today view in lock screen** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **Today view on lock screen not allowed** is displayed

Remediation:







From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **Locked Screen Experience** heading
6. Set **Block Today view in lock screen** to **Yes**

Default Value:

Not configured

CIS Controls:

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

3.6.4 Ensure "Block Wallet notifications in lock screen" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Supervised Devices

Description:

This restriction prevents access to the Apple Wallet while the screen is locked. Passcode/Face ID must be set for this to apply.

Rationale:

This will block the option for the Apple Wallet to be used while the screen is locked.

Impact:

The device will need to be unlocked to access the Wallet.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **Locked Screen Experience** heading
6. Verify that **Block Wallet notifications in lock screen** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **Passbook not allowed** is displayed

Remediation:







From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **Locked Screen Experience** heading
6. Set **Block Wallet notifications in lock screen** to **Yes**

Default Value:

Not configured

CIS Controls:

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

3.7 Password

3.7.1 Ensure "Require password" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Supervised Devices

Description:

This restriction enforces a password to be set on the device.

Rationale:

This will block the option for the device to be used without a password.

Impact:

A user will need to set a password to use the device.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **Password** heading
6. Verify that **Require password** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Tap **Passcode**
7. Confirm **Passcode required** is present and its value is **yes**

Remediation:






From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **Password** heading
6. Set **Require password** to **Yes**

Default Value:

Not configured

CIS Controls:

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

3.7.2 Ensure "Block simple passwords" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Supervised Devices

Description:

This restriction enforces a block on simple passwords on the device. Passwords such as 1234 and 0000 would be blocked.

Rationale:

This will block the option for a simple password to be used on the device.

Impact:

Those with passwords that do not meet this requirement will be prompted to set a new device password.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **Password** heading
6. Verify that **Block simple passwords** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Tap **Passcode**
7. Confirm **Simple passcodes allowed** is present and its value is **No**

Remediation:






From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **Password** heading
6. Set **Block simple passwords** to **Yes**

Default Value:

Not configured

CIS Controls:

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

3.7.3 Ensure "Required password type" is set to "Alphanumeric" (Manual)

Profile Applicability:

- Level 2 - Supervised Devices

Description:

This restriction enforces an alphanumeric password on the device. Numeric-only passcode pins would not be allowed.

Rationale:

Alphanumeric passwords provide a greater security posture by increasing the number of possible combinations, as well as not providing an indicator of password length.

Impact:

Those with passwords that do not meet this requirement will be prompted to set a new device password.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **Password** heading
6. Verify that **Required password type** is present and set to **Alphanumeric**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Tap **Passcode**
7. Confirm **Alphanumeric required** is present and its value is **Yes**

Remediation:






From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **Password** heading
6. Set **Required password type** to **Alphanumeric**

Default Value:

Not configured

CIS Controls:

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

3.7.4 Ensure "Minimum password length" is set to "6" or greater (Manual)

Profile Applicability:

- Level 1 - Supervised Devices

Description:

This restriction requires the password length set on the device to be 6 or greater.

Rationale:

Longer passwords provide a greater security posture by increasing the number of possible combinations.

Impact:

Those with passwords that do not meet this requirement will be prompted to set a new device password.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **Password** heading
6. Verify that **Minimum password length** is present and set to **6** or greater

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Tap **Passcode**
7. Confirm **Minimum length** is present and its value is **6** or greater

Remediation:






From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **Password** heading
6. Set **Minimum password length** to **6** or greater

Default Value:

Not configured

CIS Controls:

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

3.7.5 Ensure "Maximum minutes after screen lock before password is required" is set to "Immediately" (Manual)

Profile Applicability:

- Level 1 - Supervised Devices

Description:

This restriction disables any grace period where a password is not required to be entered after the screen has locked.

Rationale:

This would make it impossible for the device to be picked up and used after the screen has locked.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **Password** heading
6. Verify that **Maximum minutes after screen lock before password is required** is present and set to **Immediately**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Tap **Passcode**
7. Confirm **Max grace period** is present and its value is **Immediately**

Remediation:







From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **Password** heading
6. Set **Maximum minutes after screen lock before password is required** to **Immediately**

Default Value:

Not configured

CIS Controls:

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

3.7.6 Ensure "Maximum minutes of inactivity until screen locks" is set to "2" or less (Manual)

Profile Applicability:

- Level 1 - Supervised Devices

Description:

This restriction sets the maximum time of inactivity before the device will be automatically locked.

Rationale:

This would mitigate the concern of a unattended device being picked up and used, as the window of inactivity has been set.

Impact:

This is not enforced during certain activities, such as watching video content.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **Password** heading
6. Verify that **Maximum minutes of inactivity until screen locks** is present and set to **2** or less

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Tap **Passcode**
7. Confirm **Max inactivity** is present and its value is **2 minutes**

Remediation:







From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **Password** heading
6. Set **Maximum minutes of inactivity until screen locks** to **2** or less

Default Value:

Not configured

CIS Controls:

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

3.7.7 Ensure "Block Touch ID and Face ID unlock" is set to "Yes" (Manual)

Profile Applicability:

- Level 2 - Supervised Devices

Description:

This restriction blocks Touch ID and Face ID being used to unlock the device. A standard passcode/password will be the only form of authentication to unlock the device.

If this is not set, passcode/password will still be required after a device power-cycle or the device has been reported as lost.

Rationale:

This would address the concern of a malicious individual using the face/touch identification of the device owner as a means of authentication to the device.

Impact:

A passcode/password will be required to unlock the device.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **Password** heading
6. Verify that **Block Touch ID and Face ID unlock** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **Touch ID unlock not allowed** or **Face ID unlock not allowed** is displayed

Remediation:







From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **Password** heading
6. Set **Block Touch ID and Face ID unlock** to **Yes**

Default Value:

Not configured

CIS Controls:

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

3.7.8 Ensure "Block password proximity requests" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Supervised Devices

Description:

This restriction prevents proximity-based password sharing for nearby devices.

Rationale:

Access to systems and applications should be provisioned by role, with credentials only being transferred through supported credential management systems. Additionally, credential sharing requests may be exploited through social engineering.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **Password** heading
6. Verify that **Block password proximity requests** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **Proximity password requests not allowed** is displayed

Remediation:




From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **Password** heading
6. Set **Block password proximity requests** to **Yes**

Default Value:

Not configured

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	13.5 <u>Manage Access Control for Remote Assets</u> Manage access control for assets remotely connecting to enterprise resources. Determine amount of access to enterprise resources based on: up-to-date anti-malware software installed, configuration compliance with the enterprise's secure configuration process, and ensuring the operating system and applications are up-to-date.			
v7	12.12 <u>Manage All Devices Remotely Logging into Internal Network</u> Scan all enterprise devices remotely logging into the organization's network prior to accessing the network to ensure that each of the organization's security policies has been enforced in the same manner as local network devices.			

3.7.9 Ensure "Block password sharing" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Supervised Devices

Description:

This restriction prevents sharing credentials between devices, such as via AirDrop.

Rationale:

Access to systems and applications should be provisioned by role, with credentials only being transferred through supported credential management systems. Additionally, credential sharing requests may be exploited through social engineering.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **Password** heading
6. Verify that **Block password sharing** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **Password Sharing is not allowed** is displayed

Remediation:










From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **Password** heading
6. Set **Block password sharing** to **Yes**

Default Value:

Not configured

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	13.5 <u>Manage Access Control for Remote Assets</u> Manage access control for assets remotely connecting to enterprise resources. Determine amount of access to enterprise resources based on: up-to-date anti-malware software installed, configuration compliance with the enterprise's secure configuration process, and ensuring the operating system and applications are up-to-date.			
v8	14.3 <u>Train Workforce Members on Authentication Best Practices</u> Train workforce members on authentication best practices. Example topics include MFA, password composition, and credential management.			
v7	12.12 <u>Manage All Devices Remotely Logging into Internal Network</u> Scan all enterprise devices remotely logging into the organization's network prior to accessing the network to ensure that each of the organization's security policies has been enforced in the same manner as local network devices.			
v7	17.5 <u>Train Workforce on Secure Authentication</u> Train workforce members on the importance of enabling and utilizing secure authentication.			

3.7.10 Ensure "Require Touch ID or Face ID authentication for AutoFill of password or credit card information" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Supervised Devices

Description:

This restriction forces an authentication prompt before each AutoFill operation.

Rationale:

A device may be accessed by an unauthorized user while unlocked. This recommendation provides defense-in-depth by forcing re-authentication before credentials will be populated by AutoFill.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **Password** heading
6. Verify that **Require Touch ID or Face ID authentication for AutoFill of password or credit card information** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **Authentication before Auto Filling passwords enforced** is displayed

Remediation:







From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **Password** heading
6. Set **Require Touch ID or Face ID authentication for AutoFill of password or credit card information** to **Yes**

Default Value:

Not configured

CIS Controls:

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

3.8 Wireless

3.8.1 Ensure "Block voice dialing while device is locked" is set to "Yes" (Manual)

Profile Applicability:

- Level 1 - Supervised Devices

Description:

This restriction blocks initiating phone calls from a locked device. Voice dialing is handled separately from Siri.

Rationale:

Allowing calls from a locked device may allow for the impersonation of the device owner, or other malicious actions.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **Wireless** heading
6. Verify that **Block voice dialing while device is locked** is present and set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Tap **Restrictions**
6. Confirm **Voice dialing while locked not allowed** is displayed

Remediation:







From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **Wireless** heading
6. Set **Block voice dialing while device is locked** to **Yes**

Default Value:

Not configured

CIS Controls:

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

3.9 Lock Screen Message

3.9.1 Ensure a "Lock Screen Message" has been set (Manual)

Profile Applicability:

- Level 1 - Supervised Devices

Description:

This recommendation applies to configuring a lock screen message.

Rationale:

A lock screen message will allow an honest bystander 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 (for example, the help desk of an organization).

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the device features profile which applies to the iOS/iPadOS device
4. Under **Configuration settings**
5. Select the **Lock Screen Message** heading
6. Verify that **"If Lost, Return to..." Message** is present and has an appropriate message associated with it

Or, from the device:

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

Remediation:







From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Configuration profiles**
3. Select the profile which applies to the iOS/iPadOS device
4. Click edit, next to **Configuration settings**
5. Select the **Lock Screen Message** heading
6. Set **"If Lost, Return to..." Message** with an appropriate message

Default Value:

Not configured

CIS Controls:

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

3.10 Additional Recommendations

3.10.1 Ensure the ability to remove the management profile does not exist (Manual)

Profile Applicability:

- Level 1 - Supervised Devices

Description:

This recommendation denies the ability remove an installed configuration profile.

Rationale:

Removal of the configuration profile (and all of it's configured security restrictions) should be at the discretion of the organization, not the end user, in order to prevent greatly weakening the device's security and exposing its data.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **iOS/iPadOS**
3. Select **iOS/iPadOS enrollment**
4. Select **Enrollment program tokens**
5. Select the enrollment token which applies to the iOS/iPadOS device
6. Select **Profiles**
7. Select the profile which applies to the iOS/iPadOS device
8. Select **Properties**
9. Ensure **Locked enrollment** is set to **Yes**

Or, from the device:

1. Tap **Settings**
2. Tap **General**
3. Tap **VPN & Device Management**
4. Tap **<Profile Name>**
5. Confirm the **Remove Management** button is not displayed

Remediation:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **iOS/iPadOS**
3. Select **iOS/iPadOS enrollment**
4. Select **Enrollment program tokens**
5. Select the enrollment token which applies to the iOS/iPadOS device
6. Select **Profiles**
7. Select the profile which applies to the iOS/iPadOS device
8. Select **Properties**
9. Next to the **Management Settings** heading press **Edit**
10. Set **Locked enrollment** to **Yes**







Default Value:

Not configured

References:

1. <https://learn.microsoft.com/en-us/mem/intune/enrollment/device-enrollment-program-enroll-ios#create-an-apple-enrollment-profile>

CIS Controls:

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

3.10.2 Ensure the ability to sync with computers has been blocked (Manual)

Profile Applicability:

- Level 1 - Supervised Devices

Description:

This recommendation prevents the transfer of data to and from the device.

Rationale:

This recommendation addresses intentional or unintentional data leakage. It prevents a user from using a computer to transfer information to or from.

Impact:

This could potentially impact the use of recovery or forensic tools on locked or unlocked devices.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **iOS/iPadOS**
3. Select **iOS/iPadOS enrollment**
4. Select **Enrollment program tokens**
5. Select the enrollment token which applies to the iOS/iPadOS device
6. Select **Profiles**
7. Select the profile which applies to the iOS/iPadOS device
8. Select **Properties**
9. Ensure **Sync with computers** is set to **Deny All**

This restriction can not be audited from the device.

Remediation:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **iOS/iPadOS**
3. Select **iOS/iPadOS enrollment**
4. Select **Enrollment program tokens**
5. Select the enrollment token which applies to the iOS/iPadOS device
6. Select **Profiles**
7. Select the profile which applies to the iOS/iPadOS device
8. Select **Properties**
9. Next to the **Management Settings** heading press **Edit**
10. Set **Sync with computers** to **Deny All**






Default Value:

Not configured

References:

1. <https://learn.microsoft.com/en-us/mem/intune/enrollment/device-enrollment-program-enroll-ios#create-an-apple-enrollment-profile>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	1.2 Address Unauthorized Assets Ensure that a process exists to address unauthorized assets on a weekly basis. The enterprise may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.			
v7	13.7 Manage USB Devices If USB storage devices are required, enterprise software should be used that can configure systems to allow the use of specific devices. An inventory of such devices should be maintained.			

4 Recommendations for Compliance Policies

This section provides both level 1 and level 2 Compliance Policy recommendations for devices registered within Intune, regardless of whether they are in an supervised or unsupervised state.

4.1 Ensure "Jailbroken devices" is set to "Block" (Manual)

Profile Applicability:

- Level 1 - Supervised Devices

Description:

This recommendation ensures that jailbroken devices have been blocked by the organization via the compliance policy.

Rationale:

A jailbroken device may execute arbitrary code, compromise configuration profile requirements, or open the device to exploits that are otherwise not possible.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Compliance policies**
3. Select the compliance policy which applies to the iOS/iPadOS device
4. Select Properties
5. Under the **Compliance settings** section
6. Under the **Device Health** heading
7. Verify that **Jailbroken devices** is present and set to **Block**

Remediation:







From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Compliance policies**
3. Select the compliance policy which applies to the iOS/iPadOS device
4. Select Properties
5. Select **Edit** in the **Compliance settings** section
6. Under the **Device Health** heading
7. Set **Jailbroken devices** to **Block**

Default Value:

Not configured

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>2.2 Ensure Authorized Software is Currently Supported</u> Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.			
v7	<u>2.2 Ensure Software is Supported by Vendor</u> Ensure that only software applications or operating systems currently supported by the software's vendor are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system.			

4.2 Ensure "Minimum OS version" or "Minimum OS build version" has been defined (Manual)

Profile Applicability:

- Level 1 - Supervised Devices

Description:

This recommendation ensures that outdated devices that do not adhere to the defined minimum OS version or minimum OS build version are blocked by the organization via the compliance policy.

Rationale:

An up-to-date operating system helps provides the best possible protection against cyber threats.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Compliance policies**
3. Select the compliance policy which applies to the iOS/iPadOS device
4. Select Properties
5. Under the **Compliance settings** section
6. Under the **Device Properties** heading
7. Verify that **Minimum OS version** or **Minimum OS build version** is present and set to a value that is representative of a recent iOS/iPadOS version or build number.

Remediation:













From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Compliance policies**
3. Select the compliance policy which applies to the iOS/iPadOS device
4. Select Properties
5. Select **Edit** in the **Compliance settings** section
6. Under the **Device Properties** heading
7. Set **Minimum OS version** or **Minimum OS build version** to a value that is representative of a recent iOS/iPadOS version or build number.

Default Value:

Not configured

CIS Controls:

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

4.3 Ensure "Mark device noncompliant" is set to "Immediately" (Manual)

Profile Applicability:

- Level 1 - Supervised Devices

Description:

This recommendation ensures that devices which aren't compliant with the applied compliance policy are marked as not compliant immediately. Although this is the default, there is an option for this to be set between immediately and 365 days.

Rationale:

As soon as a device is found to be non-compliant, it should be flagged immediately so that attention can be raised to this device via manual or scheduled automatic actioning.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Compliance policies**
3. Select the compliance policy which applies to the iOS/iPadOS device
4. Select Properties
5. Under the **Actions for noncompliance** heading
6. Verify that **Mark device noncompliant** is present and set to **Immediately**

Remediation:







From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Compliance policies**
3. Select the compliance policy which applies to the iOS/iPadOS device
4. Select Properties
5. Select **Edit** in the **Actions for noncompliance** section
6. Set **Mark device noncompliant** to **0** which will resolve to immediately

Default Value:

Immediately

CIS Controls:

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

4.4 Ensure "Send email to end user" is set to "3 days" or less (Manual)

Profile Applicability:

- Level 2 - Supervised Devices

Description:

This recommendation ensures that devices that have been marked as "not compliant" will have an email sent to the assigned primary user of the device. An additional recipient (e.g. SOC or Intune administrator) should also be set.

A message template must be created and selected.

Rationale:

Action on non-compliant devices should be taken as soon as feasibly possible to reduce the impact of a device that is not compliant with the organization's compliance policy.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Compliance policies**
3. Select the compliance policy which applies to the iOS/iPadOS device
4. Select Properties
5. Under the **Actions for noncompliance** heading
6. Verify that **Send email to end user** is present and set to **3 days** or less

Remediation:







From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Compliance policies**
3. Select the compliance policy which applies to the iOS/iPadOS device
4. Select Properties
5. Select **Edit** in the **Actions for noncompliance** section
6. Set **Send email to end user** to **3** (or less) which will resolve to 3 days

Default Value:

Not configured

CIS Controls:

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

4.5 Ensure all devices are marked as "compliant" (Manual)

Profile Applicability:

- Level 1 - Supervised Devices

Description:

This recommendation ensures that devices that are not compliant to the compliance policy are addressed by either being removed from the organization or ensuring they meet the defined compliance policy.

Rationale:

Devices that aren't marked as compliant give an indicator as to which devices need attention from endpoint administrators.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Compliance policies**
3. Select the compliance policy which applies to the iOS/iPadOS device
4. Select Device status
5. Verify that the compliance status of all devices are set to "Compliant"

Remediation:







From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Compliance policies**
3. Select the compliance policy which applies to the iOS/iPadOS device
4. Select Device status
5. Address "Not Compliant" devices by either removing them or ensuring they meet the defined compliance policy

Default Value:

Not configured

CIS Controls:

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

4.6 Ensure "Mark devices with no compliance policy assigned as" is set to "Not compliant" (Manual)

Profile Applicability:

- Level 1 - Supervised Devices

Description:

This recommendation ensures that devices that do not have a compliance policy assigned to them are marked as not compliant.

Rationale:

This recommendation helps to ensure that devices that don't have a configuration policy applied are marked as "Not Compliant" so they are able to be addressed by Intune administrators.

Impact:

This applies to all compliance policies within the directory, regardless of device type.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Compliance policies**
3. Select **Compliance policy settings**
4. Verify that **Mark devices with no compliance policy assigned as** is set to **Not compliant**

Remediation:







From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Compliance policies**
3. Select **Compliance policy settings**
4. Set **Mark devices with no compliance policy assigned as** to **Not compliant**

Default Value:

Compliant

CIS Controls:

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

4.7 Ensure "Compliance status validity period (days)" is set to "7" or less (Manual)

Profile Applicability:

- Level 1 - Supervised Devices

Description:

This recommendation ensures that if devices do not check-in (report compliance status) within the defined validity period, they are marked as not compliant.

Rationale:

This recommendation helps to ensure devices that have not reported compliance status in 7 days are treated as not compliant. If the default of 30 days is used, this period of time could mean devices may not follow compliance for up to 30 days before being marked as not compliant.

Impact:

This applies to all compliance policies within the directory, regardless of device type.

Audit:

From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Compliance policies**
3. Select **Compliance policy settings**
4. Verify that **Compliance status validity period (days)** is set to **7** or less

Remediation:







From the Microsoft Intune admin center:

1. Select **Devices**
2. Select **Compliance policies**
3. Select **Compliance policy settings**
4. Set **Compliance status validity period (days)** to **7** or less

Default Value:

30

CIS Controls:

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

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	Benchmark Guidance		
2	Recommendations for Unsupervised (BYOD) Devices		
2.1	App Store, Doc Viewing, Gaming		
2.1.1	Ensure "Block viewing corporate documents in unmanaged apps" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.2	Ensure "Treat AirDrop as an unmanaged destination" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.3	Ensure "Allow copy/paste to be affected by managed open-in" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.2	Built-in Apps		
2.2.1	Ensure "Block Siri while device is locked" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.2	Ensure "Require Safari fraud warnings" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.3	Cloud and Storage		
2.3.1	Ensure "Force encrypted backup" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2	Ensure "Block managed apps from storing data in iCloud" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3	Ensure "Block backup of enterprise books" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.4	Ensure "Block notes and highlights sync for enterprise books" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.5	Ensure "Block iCloud Photos sync" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.3.6	Ensure "Block iCloud Photo Library" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.7	Ensure "Block My Photo Stream" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.8	Ensure "Block Handoff" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.4	Connected Devices		
2.4.1	Ensure "Force Apple Watch wrist detection" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.2	Ensure "Require AirPlay outgoing requests pairing password" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.3	Ensure "Block Apple Watch auto unlock" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.5	General		
2.5.1	Ensure "Block sending diagnostic and usage data to Apple" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.5.2	Ensure "Block screenshots and screen recording" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.5.3	Ensure "Block untrusted TLS certificates" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.5.4	Ensure "Force limited ad tracking" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.5.5	Ensure "Block trusting new enterprise app authors" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.5.6	Ensure "Limit Apple personalized advertising" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.6	Locked Screen Experience		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.6.1	Ensure "Block Control Center access in lock screen" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.6.2	Ensure "Block Notifications Center access in lock screen" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.6.3	Ensure "Block Today view in lock screen" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.6.4	Ensure "Block Wallet notifications in lock screen" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.7	Password		
2.7.1	Ensure "Require password" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.7.2	Ensure "Block simple passwords" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.7.3	Ensure "Required password type" is set to "Alphanumeric" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.7.4	Ensure "Minimum password length" is set to "6" or greater (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.7.5	Ensure "Maximum minutes after screen lock before password is required" is set to "Immediately" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.7.6	Ensure "Maximum minutes of inactivity until screen locks" is set to "2" or less (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.7.7	Ensure "Block Touch ID and Face ID unlock" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.8	Wireless		
2.8.1	Ensure "Block voice dialing while device is locked" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3	Recommendations for Supervised (Organization) Devices		
3.1	App Store, Doc Viewing, Gaming		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
3.1.1	Ensure "Block viewing corporate documents in unmanaged apps" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.1.2	Ensure "Treat AirDrop as an unmanaged destination" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.1.3	Ensure "Allow copy/paste to be affected by managed open-in" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.1.4	Ensure "Block App Store" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.1.5	Ensure "Block access to network drive in Files app" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.2	Built-in Apps		
3.2.1	Ensure "Block Siri while device is locked" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.2.2	Ensure "Require Safari fraud warnings" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.3	Cloud and Storage		
3.3.1	Ensure "Force encrypted backup" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.2	Ensure "Block managed apps from storing data in iCloud" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.3	Ensure "Block backup of enterprise books" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.4	Ensure "Block notes and highlights sync for enterprise books" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.5	Ensure "Block iCloud Photos sync" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.6	Ensure "Block iCloud Photo Library" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
3.3.7	Ensure "Block My Photo Stream" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.8	Ensure "Block Handoff" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.9	Ensure "Block iCloud backup" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.10	Ensure "Block iCloud document and data sync" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.11	Ensure "Block iCloud Keychain sync" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.4	Connected Devices		
3.4.1	Ensure "Force Apple Watch wrist detection" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2	Ensure "Require AirPlay outgoing requests pairing password" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3	Ensure "Block Apple Watch auto unlock" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4	Ensure "Block iBeacon discovery of AirPrint printers" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.4.5	Ensure "Block access to USB drive in Files app" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.5	General		
3.5.1	Ensure "Block sending diagnostic and usage data to Apple" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.5.2	Ensure "Block screenshots and screen recording" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.5.3	Ensure "Block untrusted TLS certificates" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
3.5.4	Ensure "Force limited ad tracking" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.5.5	Ensure "Block trusting new enterprise app authors" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.5.6	Ensure "Limit Apple personalized advertising" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.5.7	Ensure "Block users from erasing all content and settings on device" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.5.8	Ensure "Block modification of device name" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.5.9	Ensure "Block configuration profile changes" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.5.10	Ensure "Allow activation lock" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.5.11	Ensure "Force automatic date and time" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.5.12	Ensure "Block VPN creation" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.6	Locked Screen Experience		
3.6.1	Ensure "Block Control Center access in lock screen" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.2	Ensure "Block Notifications Center access in lock screen" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.3	Ensure "Block Today view in lock screen" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.4	Ensure "Block Wallet notifications in lock screen" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.7	Password		
3.7.1	Ensure "Require password" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
3.7.2	Ensure "Block simple passwords" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.7.3	Ensure "Required password type" is set to "Alphanumeric" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.7.4	Ensure "Minimum password length" is set to "6" or greater (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.7.5	Ensure "Maximum minutes after screen lock before password is required" is set to "Immediately" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.7.6	Ensure "Maximum minutes of inactivity until screen locks" is set to "2" or less (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.7.7	Ensure "Block Touch ID and Face ID unlock" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.7.8	Ensure "Block password proximity requests" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.7.9	Ensure "Block password sharing" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.7.10	Ensure "Require Touch ID or Face ID authentication for AutoFill of password or credit card information" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.8	Wireless		
3.8.1	Ensure "Block voice dialing while device is locked" is set to "Yes" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.9	Lock Screen Message		
3.9.1	Ensure a "Lock Screen Message" has been set (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.10	Additional Recommendations		
3.10.1	Ensure the ability to remove the management profile does not exist (Manual)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
3.10.2	Ensure the ability to sync with computers has been blocked (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
4	Recommendations for Compliance Policies		
4.1	Ensure "Jailbroken devices" is set to "Block" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
4.2	Ensure "Minimum OS version" or "Minimum OS build version" has been defined (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
4.3	Ensure "Mark device noncompliant" is set to "Immediately" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
4.4	Ensure "Send email to end user" is set to "3 days" or less (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
4.5	Ensure all devices are marked as "compliant" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
4.6	Ensure "Mark devices with no compliance policy assigned as" is set to "Not compliant" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
4.7	Ensure "Compliance status validity period (days)" is set to "7" or less (Manual)	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v7 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.1.1	Ensure "Block viewing corporate documents in unmanaged apps" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.1.2	Ensure "Treat AirDrop as an unmanaged destination" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.1.3	Ensure "Allow copy/paste to be affected by managed open-in" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.2.1	Ensure "Block Siri while device is locked" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1	Ensure "Force encrypted backup" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.3.8	Ensure "Block Handoff" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1	Ensure "Force Apple Watch wrist detection" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.4.2	Ensure "Require AirPlay outgoing requests pairing password" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.4.3	Ensure "Block Apple Watch auto unlock" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.5.2	Ensure "Block screenshots and screen recording" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.5.3	Ensure "Block untrusted TLS certificates" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.5.5	Ensure "Block trusting new enterprise app authors" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.6.1	Ensure "Block Control Center access in lock screen" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.6.2	Ensure "Block Notifications Center access in lock screen" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.6.3	Ensure "Block Today view in lock screen" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.6.4	Ensure "Block Wallet notifications in lock screen" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.7.5	Ensure "Maximum minutes after screen lock before password is required" is set to "Immediately"	<input type="checkbox"/>	<input type="checkbox"/>
2.7.6	Ensure "Maximum minutes of inactivity until screen locks" is set to "2" or less	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.7.7	Ensure "Block Touch ID and Face ID unlock" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.8.1	Ensure "Block voice dialing while device is locked" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.1.1	Ensure "Block viewing corporate documents in unmanaged apps" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.1.2	Ensure "Treat AirDrop as an unmanaged destination" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.1.3	Ensure "Allow copy/paste to be affected by managed open-in" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.1.4	Ensure "Block App Store" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.2.1	Ensure "Block Siri while device is locked" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.3.1	Ensure "Force encrypted backup" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.3.8	Ensure "Block Handoff" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.3.11	Ensure "Block iCloud Keychain sync" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.4.1	Ensure "Force Apple Watch wrist detection" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2	Ensure "Require AirPlay outgoing requests pairing password" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3	Ensure "Block Apple Watch auto unlock" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4	Ensure "Block iBeacon discovery of AirPrint printers" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.5.2	Ensure "Block screenshots and screen recording" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.5.3	Ensure "Block untrusted TLS certificates" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.5.5	Ensure "Block trusting new enterprise app authors" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.5.7	Ensure "Block users from erasing all content and settings on device" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.5.9	Ensure "Block configuration profile changes" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.6.1	Ensure "Block Control Center access in lock screen" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.6.2	Ensure "Block Notifications Center access in lock screen" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
3.6.3	Ensure "Block Today view in lock screen" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.6.4	Ensure "Block Wallet notifications in lock screen" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.7.5	Ensure "Maximum minutes after screen lock before password is required" is set to "Immediately"	<input type="checkbox"/>	<input type="checkbox"/>
3.7.6	Ensure "Maximum minutes of inactivity until screen locks" is set to "2" or less	<input type="checkbox"/>	<input type="checkbox"/>
3.7.7	Ensure "Block Touch ID and Face ID unlock" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.7.9	Ensure "Block password sharing" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.7.10	Ensure "Require Touch ID or Face ID authentication for AutoFill of password or credit card information" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.8.1	Ensure "Block voice dialing while device is locked" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.9.1	Ensure a "Lock Screen Message" has been set	<input type="checkbox"/>	<input type="checkbox"/>
3.10.1	Ensure the ability to remove the management profile does not exist	<input type="checkbox"/>	<input type="checkbox"/>
4.1	Ensure "Jailbroken devices" is set to "Block"	<input type="checkbox"/>	<input type="checkbox"/>
4.2	Ensure "Minimum OS version" or "Minimum OS build version" has been defined	<input type="checkbox"/>	<input type="checkbox"/>
4.3	Ensure "Mark device noncompliant" is set to "Immediately"	<input type="checkbox"/>	<input type="checkbox"/>
4.4	Ensure "Send email to end user" is set to "3 days" or less	<input type="checkbox"/>	<input type="checkbox"/>
4.5	Ensure all devices are marked as "compliant"	<input type="checkbox"/>	<input type="checkbox"/>
4.6	Ensure "Mark devices with no compliance policy assigned as" is set to "Not compliant"	<input type="checkbox"/>	<input type="checkbox"/>
4.7	Ensure "Compliance status validity period (days)" is set to "7" or less	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v7 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.1.1	Ensure "Block viewing corporate documents in unmanaged apps" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.1.2	Ensure "Treat AirDrop as an unmanaged destination" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.1.3	Ensure "Allow copy/paste to be affected by managed open-in" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.2.1	Ensure "Block Siri while device is locked" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.2.2	Ensure "Require Safari fraud warnings" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1	Ensure "Force encrypted backup" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2	Ensure "Block managed apps from storing data in iCloud" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3	Ensure "Block backup of enterprise books" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.3.4	Ensure "Block notes and highlights sync for enterprise books" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.3.5	Ensure "Block iCloud Photos sync" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.3.6	Ensure "Block iCloud Photo Library" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.3.7	Ensure "Block My Photo Stream" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.3.8	Ensure "Block Handoff" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1	Ensure "Force Apple Watch wrist detection" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.4.2	Ensure "Require AirPlay outgoing requests pairing password" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.4.3	Ensure "Block Apple Watch auto unlock" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.5.1	Ensure "Block sending diagnostic and usage data to Apple" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.5.2	Ensure "Block screenshots and screen recording" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.5.3	Ensure "Block untrusted TLS certificates" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.5.4	Ensure "Force limited ad tracking" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.5.5	Ensure "Block trusting new enterprise app authors" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.5.6	Ensure "Limit Apple personalized advertising" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.6.1	Ensure "Block Control Center access in lock screen" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.6.2	Ensure "Block Notifications Center access in lock screen" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.6.3	Ensure "Block Today view in lock screen" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.6.4	Ensure "Block Wallet notifications in lock screen" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.7.1	Ensure "Require password" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.7.2	Ensure "Block simple passwords" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.7.3	Ensure "Required password type" is set to "Alphanumeric"	<input type="checkbox"/>	<input type="checkbox"/>
2.7.4	Ensure "Minimum password length" is set to "6" or greater	<input type="checkbox"/>	<input type="checkbox"/>
2.7.5	Ensure "Maximum minutes after screen lock before password is required" is set to "Immediately"	<input type="checkbox"/>	<input type="checkbox"/>
2.7.6	Ensure "Maximum minutes of inactivity until screen locks" is set to "2" or less	<input type="checkbox"/>	<input type="checkbox"/>
2.7.7	Ensure "Block Touch ID and Face ID unlock" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.8.1	Ensure "Block voice dialing while device is locked" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.1.1	Ensure "Block viewing corporate documents in unmanaged apps" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.1.2	Ensure "Treat AirDrop as an unmanaged destination" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.1.3	Ensure "Allow copy/paste to be affected by managed open-in" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.1.4	Ensure "Block App Store" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.2.1	Ensure "Block Siri while device is locked" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.2.2	Ensure "Require Safari fraud warnings" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.3.1	Ensure "Force encrypted backup" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
3.3.2	Ensure "Block managed apps from storing data in iCloud" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.3.3	Ensure "Block backup of enterprise books" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.3.4	Ensure "Block notes and highlights sync for enterprise books" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.3.5	Ensure "Block iCloud Photos sync" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.3.6	Ensure "Block iCloud Photo Library" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.3.7	Ensure "Block My Photo Stream" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.3.8	Ensure "Block Handoff" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.3.9	Ensure "Block iCloud backup" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.3.10	Ensure "Block iCloud document and data sync" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.3.11	Ensure "Block iCloud Keychain sync" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.4.1	Ensure "Force Apple Watch wrist detection" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2	Ensure "Require AirPlay outgoing requests pairing password" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3	Ensure "Block Apple Watch auto unlock" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4	Ensure "Block iBeacon discovery of AirPrint printers" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.4.5	Ensure "Block access to USB drive in Files app" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.5.1	Ensure "Block sending diagnostic and usage data to Apple" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.5.2	Ensure "Block screenshots and screen recording" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.5.3	Ensure "Block untrusted TLS certificates" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.5.4	Ensure "Force limited ad tracking" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.5.5	Ensure "Block trusting new enterprise app authors" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.5.6	Ensure "Limit Apple personalized advertising" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.5.7	Ensure "Block users from erasing all content and settings on device" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
3.5.8	Ensure "Block modification of device name" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.5.9	Ensure "Block configuration profile changes" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.5.11	Ensure "Force automatic date and time" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.5.12	Ensure "Block VPN creation" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.6.1	Ensure "Block Control Center access in lock screen" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.6.2	Ensure "Block Notifications Center access in lock screen" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.6.3	Ensure "Block Today view in lock screen" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.6.4	Ensure "Block Wallet notifications in lock screen" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.7.1	Ensure "Require password" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.7.2	Ensure "Block simple passwords" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.7.3	Ensure "Required password type" is set to "Alphanumeric"	<input type="checkbox"/>	<input type="checkbox"/>
3.7.4	Ensure "Minimum password length" is set to "6" or greater	<input type="checkbox"/>	<input type="checkbox"/>
3.7.5	Ensure "Maximum minutes after screen lock before password is required" is set to "Immediately"	<input type="checkbox"/>	<input type="checkbox"/>
3.7.6	Ensure "Maximum minutes of inactivity until screen locks" is set to "2" or less	<input type="checkbox"/>	<input type="checkbox"/>
3.7.7	Ensure "Block Touch ID and Face ID unlock" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.7.9	Ensure "Block password sharing" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.7.10	Ensure "Require Touch ID or Face ID authentication for AutoFill of password or credit card information" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.8.1	Ensure "Block voice dialing while device is locked" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.9.1	Ensure a "Lock Screen Message" has been set	<input type="checkbox"/>	<input type="checkbox"/>
3.10.1	Ensure the ability to remove the management profile does not exist	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
3.10.2	Ensure the ability to sync with computers has been blocked	<input type="checkbox"/>	<input type="checkbox"/>
4.1	Ensure "Jailbroken devices" is set to "Block"	<input type="checkbox"/>	<input type="checkbox"/>
4.2	Ensure "Minimum OS version" or "Minimum OS build version" has been defined	<input type="checkbox"/>	<input type="checkbox"/>
4.3	Ensure "Mark device noncompliant" is set to "Immediately"	<input type="checkbox"/>	<input type="checkbox"/>
4.4	Ensure "Send email to end user" is set to "3 days" or less	<input type="checkbox"/>	<input type="checkbox"/>
4.5	Ensure all devices are marked as "compliant"	<input type="checkbox"/>	<input type="checkbox"/>
4.6	Ensure "Mark devices with no compliance policy assigned as" is set to "Not compliant"	<input type="checkbox"/>	<input type="checkbox"/>
4.7	Ensure "Compliance status validity period (days)" is set to "7" or less	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v7 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.1.1	Ensure "Block viewing corporate documents in unmanaged apps" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.1.2	Ensure "Treat AirDrop as an unmanaged destination" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.1.3	Ensure "Allow copy/paste to be affected by managed open-in" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.2.1	Ensure "Block Siri while device is locked" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.2.2	Ensure "Require Safari fraud warnings" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1	Ensure "Force encrypted backup" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2	Ensure "Block managed apps from storing data in iCloud" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3	Ensure "Block backup of enterprise books" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.3.4	Ensure "Block notes and highlights sync for enterprise books" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.3.5	Ensure "Block iCloud Photos sync" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.3.6	Ensure "Block iCloud Photo Library" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.3.7	Ensure "Block My Photo Stream" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.3.8	Ensure "Block Handoff" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1	Ensure "Force Apple Watch wrist detection" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.4.2	Ensure "Require AirPlay outgoing requests pairing password" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.4.3	Ensure "Block Apple Watch auto unlock" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.5.1	Ensure "Block sending diagnostic and usage data to Apple" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.5.2	Ensure "Block screenshots and screen recording" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.5.3	Ensure "Block untrusted TLS certificates" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.5.4	Ensure "Force limited ad tracking" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.5.5	Ensure "Block trusting new enterprise app authors" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.5.6	Ensure "Limit Apple personalized advertising" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.6.1	Ensure "Block Control Center access in lock screen" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.6.2	Ensure "Block Notifications Center access in lock screen" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.6.3	Ensure "Block Today view in lock screen" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.6.4	Ensure "Block Wallet notifications in lock screen" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.7.1	Ensure "Require password" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.7.2	Ensure "Block simple passwords" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.7.3	Ensure "Required password type" is set to "Alphanumeric"	<input type="checkbox"/>	<input type="checkbox"/>
2.7.4	Ensure "Minimum password length" is set to "6" or greater	<input type="checkbox"/>	<input type="checkbox"/>
2.7.5	Ensure "Maximum minutes after screen lock before password is required" is set to "Immediately"	<input type="checkbox"/>	<input type="checkbox"/>
2.7.6	Ensure "Maximum minutes of inactivity until screen locks" is set to "2" or less	<input type="checkbox"/>	<input type="checkbox"/>
2.7.7	Ensure "Block Touch ID and Face ID unlock" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.8.1	Ensure "Block voice dialing while device is locked" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.1.1	Ensure "Block viewing corporate documents in unmanaged apps" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.1.2	Ensure "Treat AirDrop as an unmanaged destination" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.1.3	Ensure "Allow copy/paste to be affected by managed open-in" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.1.4	Ensure "Block App Store" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.1.5	Ensure "Block access to network drive in Files app" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.2.1	Ensure "Block Siri while device is locked" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
3.2.2	Ensure "Require Safari fraud warnings" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.3.1	Ensure "Force encrypted backup" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.3.2	Ensure "Block managed apps from storing data in iCloud" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.3.3	Ensure "Block backup of enterprise books" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.3.4	Ensure "Block notes and highlights sync for enterprise books" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.3.5	Ensure "Block iCloud Photos sync" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.3.6	Ensure "Block iCloud Photo Library" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.3.7	Ensure "Block My Photo Stream" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.3.8	Ensure "Block Handoff" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.3.9	Ensure "Block iCloud backup" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.3.10	Ensure "Block iCloud document and data sync" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.3.11	Ensure "Block iCloud Keychain sync" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.4.1	Ensure "Force Apple Watch wrist detection" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2	Ensure "Require AirPlay outgoing requests pairing password" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3	Ensure "Block Apple Watch auto unlock" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4	Ensure "Block iBeacon discovery of AirPrint printers" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.4.5	Ensure "Block access to USB drive in Files app" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.5.1	Ensure "Block sending diagnostic and usage data to Apple" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.5.2	Ensure "Block screenshots and screen recording" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.5.3	Ensure "Block untrusted TLS certificates" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.5.4	Ensure "Force limited ad tracking" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.5.5	Ensure "Block trusting new enterprise app authors" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.5.6	Ensure "Limit Apple personalized advertising" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
3.5.7	Ensure "Block users from erasing all content and settings on device" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.5.8	Ensure "Block modification of device name" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.5.9	Ensure "Block configuration profile changes" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.5.10	Ensure "Allow activation lock" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.5.11	Ensure "Force automatic date and time" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.5.12	Ensure "Block VPN creation" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.6.1	Ensure "Block Control Center access in lock screen" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.6.2	Ensure "Block Notifications Center access in lock screen" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.6.3	Ensure "Block Today view in lock screen" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.6.4	Ensure "Block Wallet notifications in lock screen" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.7.1	Ensure "Require password" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.7.2	Ensure "Block simple passwords" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.7.3	Ensure "Required password type" is set to "Alphanumeric"	<input type="checkbox"/>	<input type="checkbox"/>
3.7.4	Ensure "Minimum password length" is set to "6" or greater	<input type="checkbox"/>	<input type="checkbox"/>
3.7.5	Ensure "Maximum minutes after screen lock before password is required" is set to "Immediately"	<input type="checkbox"/>	<input type="checkbox"/>
3.7.6	Ensure "Maximum minutes of inactivity until screen locks" is set to "2" or less	<input type="checkbox"/>	<input type="checkbox"/>
3.7.7	Ensure "Block Touch ID and Face ID unlock" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.7.8	Ensure "Block password proximity requests" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.7.9	Ensure "Block password sharing" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.7.10	Ensure "Require Touch ID or Face ID authentication for AutoFill of password or credit card information" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
3.8.1	Ensure "Block voice dialing while device is locked" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.9.1	Ensure a "Lock Screen Message" has been set	<input type="checkbox"/>	<input type="checkbox"/>
3.10.1	Ensure the ability to remove the management profile does not exist	<input type="checkbox"/>	<input type="checkbox"/>
3.10.2	Ensure the ability to sync with computers has been blocked	<input type="checkbox"/>	<input type="checkbox"/>
4.1	Ensure "Jailbroken devices" is set to "Block"	<input type="checkbox"/>	<input type="checkbox"/>
4.2	Ensure "Minimum OS version" or "Minimum OS build version" has been defined	<input type="checkbox"/>	<input type="checkbox"/>
4.3	Ensure "Mark device noncompliant" is set to "Immediately"	<input type="checkbox"/>	<input type="checkbox"/>
4.4	Ensure "Send email to end user" is set to "3 days" or less	<input type="checkbox"/>	<input type="checkbox"/>
4.5	Ensure all devices are marked as "compliant"	<input type="checkbox"/>	<input type="checkbox"/>
4.6	Ensure "Mark devices with no compliance policy assigned as" is set to "Not compliant"	<input type="checkbox"/>	<input type="checkbox"/>
4.7	Ensure "Compliance status validity period (days)" is set to "7" or less	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v7 Unmapped Recommendations

Recommendation		Set Correctly	
		Yes	No
	No unmapped recommendations to CIS Controls v7	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v8 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.1.1	Ensure "Block viewing corporate documents in unmanaged apps" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.1.2	Ensure "Treat AirDrop as an unmanaged destination" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.1.3	Ensure "Allow copy/paste to be affected by managed open-in" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.2.1	Ensure "Block Siri while device is locked" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1	Ensure "Force encrypted backup" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2	Ensure "Block managed apps from storing data in iCloud" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3	Ensure "Block backup of enterprise books" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.3.4	Ensure "Block notes and highlights sync for enterprise books" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.3.5	Ensure "Block iCloud Photos sync" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.3.6	Ensure "Block iCloud Photo Library" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.3.7	Ensure "Block My Photo Stream" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.3.8	Ensure "Block Handoff" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1	Ensure "Force Apple Watch wrist detection" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.4.2	Ensure "Require AirPlay outgoing requests pairing password" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.4.3	Ensure "Block Apple Watch auto unlock" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.5.2	Ensure "Block screenshots and screen recording" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.5.3	Ensure "Block untrusted TLS certificates" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.5.5	Ensure "Block trusting new enterprise app authors" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.6.1	Ensure "Block Control Center access in lock screen" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.6.2	Ensure "Block Notifications Center access in lock screen" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.6.3	Ensure "Block Today view in lock screen" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.6.4	Ensure "Block Wallet notifications in lock screen" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.7.1	Ensure "Require password" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.7.2	Ensure "Block simple passwords" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.7.3	Ensure "Required password type" is set to "Alphanumeric"	<input type="checkbox"/>	<input type="checkbox"/>
2.7.4	Ensure "Minimum password length" is set to "6" or greater	<input type="checkbox"/>	<input type="checkbox"/>
2.7.5	Ensure "Maximum minutes after screen lock before password is required" is set to "Immediately"	<input type="checkbox"/>	<input type="checkbox"/>
2.7.6	Ensure "Maximum minutes of inactivity until screen locks" is set to "2" or less	<input type="checkbox"/>	<input type="checkbox"/>
2.7.7	Ensure "Block Touch ID and Face ID unlock" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.8.1	Ensure "Block voice dialing while device is locked" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.1.1	Ensure "Block viewing corporate documents in unmanaged apps" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.1.2	Ensure "Treat AirDrop as an unmanaged destination" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.1.3	Ensure "Allow copy/paste to be affected by managed open-in" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.1.4	Ensure "Block App Store" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.1.5	Ensure "Block access to network drive in Files app" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.2.1	Ensure "Block Siri while device is locked" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.3.1	Ensure "Force encrypted backup" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.3.2	Ensure "Block managed apps from storing data in iCloud" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.3.3	Ensure "Block backup of enterprise books" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.3.4	Ensure "Block notes and highlights sync for enterprise books" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
3.3.5	Ensure "Block iCloud Photos sync" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.3.6	Ensure "Block iCloud Photo Library" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.3.7	Ensure "Block My Photo Stream" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.3.8	Ensure "Block Handoff" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.3.9	Ensure "Block iCloud backup" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.3.10	Ensure "Block iCloud document and data sync" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.3.11	Ensure "Block iCloud Keychain sync" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.4.1	Ensure "Force Apple Watch wrist detection" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2	Ensure "Require AirPlay outgoing requests pairing password" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3	Ensure "Block Apple Watch auto unlock" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4	Ensure "Block iBeacon discovery of AirPrint printers" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.4.5	Ensure "Block access to USB drive in Files app" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.5.2	Ensure "Block screenshots and screen recording" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.5.3	Ensure "Block untrusted TLS certificates" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.5.5	Ensure "Block trusting new enterprise app authors" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.5.7	Ensure "Block users from erasing all content and settings on device" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.5.8	Ensure "Block modification of device name" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.5.9	Ensure "Block configuration profile changes" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.6.1	Ensure "Block Control Center access in lock screen" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.6.2	Ensure "Block Notifications Center access in lock screen" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.6.3	Ensure "Block Today view in lock screen" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.6.4	Ensure "Block Wallet notifications in lock screen" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
3.7.1	Ensure "Require password" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.7.2	Ensure "Block simple passwords" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.7.3	Ensure "Required password type" is set to "Alphanumeric"	<input type="checkbox"/>	<input type="checkbox"/>
3.7.4	Ensure "Minimum password length" is set to "6" or greater	<input type="checkbox"/>	<input type="checkbox"/>
3.7.5	Ensure "Maximum minutes after screen lock before password is required" is set to "Immediately"	<input type="checkbox"/>	<input type="checkbox"/>
3.7.6	Ensure "Maximum minutes of inactivity until screen locks" is set to "2" or less	<input type="checkbox"/>	<input type="checkbox"/>
3.7.7	Ensure "Block Touch ID and Face ID unlock" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.7.9	Ensure "Block password sharing" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.7.10	Ensure "Require Touch ID or Face ID authentication for AutoFill of password or credit card information" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.8.1	Ensure "Block voice dialing while device is locked" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.9.1	Ensure a "Lock Screen Message" has been set	<input type="checkbox"/>	<input type="checkbox"/>
3.10.1	Ensure the ability to remove the management profile does not exist	<input type="checkbox"/>	<input type="checkbox"/>
3.10.2	Ensure the ability to sync with computers has been blocked	<input type="checkbox"/>	<input type="checkbox"/>
4.1	Ensure "Jailbroken devices" is set to "Block"	<input type="checkbox"/>	<input type="checkbox"/>
4.2	Ensure "Minimum OS version" or "Minimum OS build version" has been defined	<input type="checkbox"/>	<input type="checkbox"/>
4.3	Ensure "Mark device noncompliant" is set to "Immediately"	<input type="checkbox"/>	<input type="checkbox"/>
4.4	Ensure "Send email to end user" is set to "3 days" or less	<input type="checkbox"/>	<input type="checkbox"/>
4.5	Ensure all devices are marked as "compliant"	<input type="checkbox"/>	<input type="checkbox"/>
4.6	Ensure "Mark devices with no compliance policy assigned as" is set to "Not compliant"	<input type="checkbox"/>	<input type="checkbox"/>
4.7	Ensure "Compliance status validity period (days)" is set to "7" or less	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v8 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.1.1	Ensure "Block viewing corporate documents in unmanaged apps" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.1.2	Ensure "Treat AirDrop as an unmanaged destination" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.1.3	Ensure "Allow copy/paste to be affected by managed open-in" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.2.1	Ensure "Block Siri while device is locked" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.2.2	Ensure "Require Safari fraud warnings" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1	Ensure "Force encrypted backup" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2	Ensure "Block managed apps from storing data in iCloud" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3	Ensure "Block backup of enterprise books" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.3.4	Ensure "Block notes and highlights sync for enterprise books" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.3.5	Ensure "Block iCloud Photos sync" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.3.6	Ensure "Block iCloud Photo Library" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.3.7	Ensure "Block My Photo Stream" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.3.8	Ensure "Block Handoff" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1	Ensure "Force Apple Watch wrist detection" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.4.2	Ensure "Require AirPlay outgoing requests pairing password" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.4.3	Ensure "Block Apple Watch auto unlock" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.5.1	Ensure "Block sending diagnostic and usage data to Apple" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.5.2	Ensure "Block screenshots and screen recording" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.5.3	Ensure "Block untrusted TLS certificates" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.5.4	Ensure "Force limited ad tracking" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.5.5	Ensure "Block trusting new enterprise app authors" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.5.6	Ensure "Limit Apple personalized advertising" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.6.1	Ensure "Block Control Center access in lock screen" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.6.2	Ensure "Block Notifications Center access in lock screen" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.6.3	Ensure "Block Today view in lock screen" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.6.4	Ensure "Block Wallet notifications in lock screen" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.7.1	Ensure "Require password" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.7.2	Ensure "Block simple passwords" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.7.3	Ensure "Required password type" is set to "Alphanumeric"	<input type="checkbox"/>	<input type="checkbox"/>
2.7.4	Ensure "Minimum password length" is set to "6" or greater	<input type="checkbox"/>	<input type="checkbox"/>
2.7.5	Ensure "Maximum minutes after screen lock before password is required" is set to "Immediately"	<input type="checkbox"/>	<input type="checkbox"/>
2.7.6	Ensure "Maximum minutes of inactivity until screen locks" is set to "2" or less	<input type="checkbox"/>	<input type="checkbox"/>
2.7.7	Ensure "Block Touch ID and Face ID unlock" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.8.1	Ensure "Block voice dialing while device is locked" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.1.1	Ensure "Block viewing corporate documents in unmanaged apps" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.1.2	Ensure "Treat AirDrop as an unmanaged destination" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.1.3	Ensure "Allow copy/paste to be affected by managed open-in" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.1.4	Ensure "Block App Store" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.1.5	Ensure "Block access to network drive in Files app" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.2.1	Ensure "Block Siri while device is locked" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
3.2.2	Ensure "Require Safari fraud warnings" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.3.1	Ensure "Force encrypted backup" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.3.2	Ensure "Block managed apps from storing data in iCloud" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.3.3	Ensure "Block backup of enterprise books" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.3.4	Ensure "Block notes and highlights sync for enterprise books" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.3.5	Ensure "Block iCloud Photos sync" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.3.6	Ensure "Block iCloud Photo Library" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.3.7	Ensure "Block My Photo Stream" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.3.8	Ensure "Block Handoff" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.3.9	Ensure "Block iCloud backup" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.3.10	Ensure "Block iCloud document and data sync" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.3.11	Ensure "Block iCloud Keychain sync" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.4.1	Ensure "Force Apple Watch wrist detection" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2	Ensure "Require AirPlay outgoing requests pairing password" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3	Ensure "Block Apple Watch auto unlock" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4	Ensure "Block iBeacon discovery of AirPrint printers" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.4.5	Ensure "Block access to USB drive in Files app" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.5.1	Ensure "Block sending diagnostic and usage data to Apple" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.5.2	Ensure "Block screenshots and screen recording" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.5.3	Ensure "Block untrusted TLS certificates" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.5.4	Ensure "Force limited ad tracking" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.5.5	Ensure "Block trusting new enterprise app authors" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.5.6	Ensure "Limit Apple personalized advertising" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
3.5.7	Ensure "Block users from erasing all content and settings on device" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.5.8	Ensure "Block modification of device name" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.5.9	Ensure "Block configuration profile changes" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.5.11	Ensure "Force automatic date and time" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.5.12	Ensure "Block VPN creation" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.6.1	Ensure "Block Control Center access in lock screen" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.6.2	Ensure "Block Notifications Center access in lock screen" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.6.3	Ensure "Block Today view in lock screen" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.6.4	Ensure "Block Wallet notifications in lock screen" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.7.1	Ensure "Require password" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.7.2	Ensure "Block simple passwords" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.7.3	Ensure "Required password type" is set to "Alphanumeric"	<input type="checkbox"/>	<input type="checkbox"/>
3.7.4	Ensure "Minimum password length" is set to "6" or greater	<input type="checkbox"/>	<input type="checkbox"/>
3.7.5	Ensure "Maximum minutes after screen lock before password is required" is set to "Immediately"	<input type="checkbox"/>	<input type="checkbox"/>
3.7.6	Ensure "Maximum minutes of inactivity until screen locks" is set to "2" or less	<input type="checkbox"/>	<input type="checkbox"/>
3.7.7	Ensure "Block Touch ID and Face ID unlock" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.7.8	Ensure "Block password proximity requests" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.7.9	Ensure "Block password sharing" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.7.10	Ensure "Require Touch ID or Face ID authentication for AutoFill of password or credit card information" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.8.1	Ensure "Block voice dialing while device is locked" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
3.9.1	Ensure a "Lock Screen Message" has been set	<input type="checkbox"/>	<input type="checkbox"/>
3.10.1	Ensure the ability to remove the management profile does not exist	<input type="checkbox"/>	<input type="checkbox"/>
3.10.2	Ensure the ability to sync with computers has been blocked	<input type="checkbox"/>	<input type="checkbox"/>
4.1	Ensure "Jailbroken devices" is set to "Block"	<input type="checkbox"/>	<input type="checkbox"/>
4.2	Ensure "Minimum OS version" or "Minimum OS build version" has been defined	<input type="checkbox"/>	<input type="checkbox"/>
4.3	Ensure "Mark device noncompliant" is set to "Immediately"	<input type="checkbox"/>	<input type="checkbox"/>
4.4	Ensure "Send email to end user" is set to "3 days" or less	<input type="checkbox"/>	<input type="checkbox"/>
4.5	Ensure all devices are marked as "compliant"	<input type="checkbox"/>	<input type="checkbox"/>
4.6	Ensure "Mark devices with no compliance policy assigned as" is set to "Not compliant"	<input type="checkbox"/>	<input type="checkbox"/>
4.7	Ensure "Compliance status validity period (days)" is set to "7" or less	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v8 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.1.1	Ensure "Block viewing corporate documents in unmanaged apps" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.1.2	Ensure "Treat AirDrop as an unmanaged destination" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.1.3	Ensure "Allow copy/paste to be affected by managed open-in" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.2.1	Ensure "Block Siri while device is locked" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.2.2	Ensure "Require Safari fraud warnings" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1	Ensure "Force encrypted backup" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2	Ensure "Block managed apps from storing data in iCloud" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3	Ensure "Block backup of enterprise books" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.3.4	Ensure "Block notes and highlights sync for enterprise books" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.3.5	Ensure "Block iCloud Photos sync" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.3.6	Ensure "Block iCloud Photo Library" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.3.7	Ensure "Block My Photo Stream" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.3.8	Ensure "Block Handoff" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1	Ensure "Force Apple Watch wrist detection" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.4.2	Ensure "Require AirPlay outgoing requests pairing password" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.4.3	Ensure "Block Apple Watch auto unlock" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.5.1	Ensure "Block sending diagnostic and usage data to Apple" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.5.2	Ensure "Block screenshots and screen recording" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.5.3	Ensure "Block untrusted TLS certificates" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.5.4	Ensure "Force limited ad tracking" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.5.5	Ensure "Block trusting new enterprise app authors" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.5.6	Ensure "Limit Apple personalized advertising" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.6.1	Ensure "Block Control Center access in lock screen" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.6.2	Ensure "Block Notifications Center access in lock screen" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.6.3	Ensure "Block Today view in lock screen" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.6.4	Ensure "Block Wallet notifications in lock screen" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.7.1	Ensure "Require password" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.7.2	Ensure "Block simple passwords" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.7.3	Ensure "Required password type" is set to "Alphanumeric"	<input type="checkbox"/>	<input type="checkbox"/>
2.7.4	Ensure "Minimum password length" is set to "6" or greater	<input type="checkbox"/>	<input type="checkbox"/>
2.7.5	Ensure "Maximum minutes after screen lock before password is required" is set to "Immediately"	<input type="checkbox"/>	<input type="checkbox"/>
2.7.6	Ensure "Maximum minutes of inactivity until screen locks" is set to "2" or less	<input type="checkbox"/>	<input type="checkbox"/>
2.7.7	Ensure "Block Touch ID and Face ID unlock" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
2.8.1	Ensure "Block voice dialing while device is locked" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.1.1	Ensure "Block viewing corporate documents in unmanaged apps" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.1.2	Ensure "Treat AirDrop as an unmanaged destination" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.1.3	Ensure "Allow copy/paste to be affected by managed open-in" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.1.4	Ensure "Block App Store" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.1.5	Ensure "Block access to network drive in Files app" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.2.1	Ensure "Block Siri while device is locked" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
3.2.2	Ensure "Require Safari fraud warnings" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.3.1	Ensure "Force encrypted backup" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.3.2	Ensure "Block managed apps from storing data in iCloud" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.3.3	Ensure "Block backup of enterprise books" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.3.4	Ensure "Block notes and highlights sync for enterprise books" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.3.5	Ensure "Block iCloud Photos sync" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.3.6	Ensure "Block iCloud Photo Library" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.3.7	Ensure "Block My Photo Stream" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.3.8	Ensure "Block Handoff" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.3.9	Ensure "Block iCloud backup" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.3.10	Ensure "Block iCloud document and data sync" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.3.11	Ensure "Block iCloud Keychain sync" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.4.1	Ensure "Force Apple Watch wrist detection" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2	Ensure "Require AirPlay outgoing requests pairing password" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3	Ensure "Block Apple Watch auto unlock" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4	Ensure "Block iBeacon discovery of AirPrint printers" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.4.5	Ensure "Block access to USB drive in Files app" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.5.1	Ensure "Block sending diagnostic and usage data to Apple" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.5.2	Ensure "Block screenshots and screen recording" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.5.3	Ensure "Block untrusted TLS certificates" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.5.4	Ensure "Force limited ad tracking" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.5.5	Ensure "Block trusting new enterprise app authors" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.5.6	Ensure "Limit Apple personalized advertising" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
3.5.7	Ensure "Block users from erasing all content and settings on device" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.5.8	Ensure "Block modification of device name" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.5.9	Ensure "Block configuration profile changes" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.5.10	Ensure "Allow activation lock" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.5.11	Ensure "Force automatic date and time" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.5.12	Ensure "Block VPN creation" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.6.1	Ensure "Block Control Center access in lock screen" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.6.2	Ensure "Block Notifications Center access in lock screen" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.6.3	Ensure "Block Today view in lock screen" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.6.4	Ensure "Block Wallet notifications in lock screen" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.7.1	Ensure "Require password" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.7.2	Ensure "Block simple passwords" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.7.3	Ensure "Required password type" is set to "Alphanumeric"	<input type="checkbox"/>	<input type="checkbox"/>
3.7.4	Ensure "Minimum password length" is set to "6" or greater	<input type="checkbox"/>	<input type="checkbox"/>
3.7.5	Ensure "Maximum minutes after screen lock before password is required" is set to "Immediately"	<input type="checkbox"/>	<input type="checkbox"/>
3.7.6	Ensure "Maximum minutes of inactivity until screen locks" is set to "2" or less	<input type="checkbox"/>	<input type="checkbox"/>
3.7.7	Ensure "Block Touch ID and Face ID unlock" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.7.8	Ensure "Block password proximity requests" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.7.9	Ensure "Block password sharing" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.7.10	Ensure "Require Touch ID or Face ID authentication for AutoFill of password or credit card information" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
3.8.1	Ensure "Block voice dialing while device is locked" is set to "Yes"	<input type="checkbox"/>	<input type="checkbox"/>
3.9.1	Ensure a "Lock Screen Message" has been set	<input type="checkbox"/>	<input type="checkbox"/>
3.10.1	Ensure the ability to remove the management profile does not exist	<input type="checkbox"/>	<input type="checkbox"/>
3.10.2	Ensure the ability to sync with computers has been blocked	<input type="checkbox"/>	<input type="checkbox"/>
4.1	Ensure "Jailbroken devices" is set to "Block"	<input type="checkbox"/>	<input type="checkbox"/>
4.2	Ensure "Minimum OS version" or "Minimum OS build version" has been defined	<input type="checkbox"/>	<input type="checkbox"/>
4.3	Ensure "Mark device noncompliant" is set to "Immediately"	<input type="checkbox"/>	<input type="checkbox"/>
4.4	Ensure "Send email to end user" is set to "3 days" or less	<input type="checkbox"/>	<input type="checkbox"/>
4.5	Ensure all devices are marked as "compliant"	<input type="checkbox"/>	<input type="checkbox"/>
4.6	Ensure "Mark devices with no compliance policy assigned as" is set to "Not compliant"	<input type="checkbox"/>	<input type="checkbox"/>
4.7	Ensure "Compliance status validity period (days)" is set to "7" or less	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v8 Unmapped Recommendations

Recommendation		Set Correctly	
		Yes	No
	No unmapped recommendations to CIS Controls v8	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: Change History

Date	Version	Changes for this version
Sep 8, 2025	1.0.0	Initial Draft Release
Sep 30, 2025	1.0.0	Initial Release