Table of contents

<table>
<thead>
<tr>
<th>Introduction</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audience</td>
<td>4</td>
</tr>
<tr>
<td>Purpose</td>
<td>4</td>
</tr>
<tr>
<td>Evaluation status</td>
<td>5</td>
</tr>
</tbody>
</table>

**General advice**                                                                                     | 6 |
| iOS encryption                                                               | 6 |
| Supervised devices                                                           | 7 |

**Advice to authorising officers**                                                                          | 8 |
| iOS 12 and the Essential Eight                                               | 8 |

**iOS 12 platform feature summary and risk considerations**                                                   | 10 |
| Supervised Mode (Applicability: Organisation-owned device)               | 10 |
| Supervised Mode (Applicability: Bring Your Own Device)                  | 10 |
| Device passcode                                                           | 10 |
| Biometric device unlock                                                   | 11 |
| Non-native applications                                                   | 11 |
| Mobile Device Management                                                  | 12 |
| Bring Your Own Device                                                     | 12 |
| Managed Open-In                                                           | 12 |
| Virtual Private Network                                                   | 13 |
| Email applications                                                        | 13 |
| Backups                                                                    | 14 |
| Office for iOS                                                            | 14 |
| iOS Calendar                                                              | 14 |
Introduction

This guide has been provided by the Australian Cyber Security Centre (ACSC).
ASD provides guidance and other assistance to Australian federal and state organisations on matters relating to the security and integrity of information that is processed, stored or communicated by electronic or similar means.
The ACSC is located within ASD and leads the Australian Government’s efforts to improve cyber security. Its role is to help make Australia the safest place to connect online.
The ACSC has developed this guide to assist Australian government and industry partners to understand the risks of deploying iOS 12.1.2 and the requirements for iOS 12.1.2 to handle Australian government data. This document does not replace the specific technical controls outlined in ACSC hardening guides relevant to this product, however where a technical conflict arises the most current document shall take priority.

Audience

This guide is for users and administrators of devices running iOS 12.1.2. These devices include iPod Touch, iPhone and iPad. Note that although tvOS, watchOS, and macOS have many similarities, they have not been subject to evaluation under Common Criteria or ASD.
To use this guide, readers should be familiar with basic networking concepts, be an experienced mobile device system administrator, and be or have access to an experienced network administrator.
Parts of this guide will make reference to product features that will require the engagement of other software, networking equipment, firewall or Mobile Device Management (MDM) vendors. While every effort has been made to ensure content involving any third party vendor products is correct at time of writing, organisations should always check with these vendors when planning their system implementation.
Note: Mention of third party products is not a specific endorsement of that vendor over another, and they are mentioned for illustrative purposes only.
Some security configuration instructions within this guide are complex, and if implemented incorrectly could reduce the security of the device, the network or the organisation’s overall security posture. These instructions should only be interpreted by experienced systems administrators and should be used in conjunction with thorough testing.

Purpose

This guide provides information for Australian government organisations on the security of Apple iOS 12.1.2 devices and their security risks that should be considered before being introduced into an organisation’s mobile fleet. The content can be widely applied by commercial organisation and enterprises.
This guide provides information and an outline of risks for Australian government organisations to consider before implementing Apple iOS devices in their fleet. This guide also contains instructions and techniques for Australian government organisations to configure the security of the Australian Apple iPod Touch, iPhone and iPad running 12.1.2. Throughout this guide, these specific devices and combinations of software are referred to as the ‘iOS platform’.
The advice in this guide has been written for the use of the iOS 12 platform within Australia. Organisations and individuals seeking to use iOS 12 platform devices overseas should also refer to Travelling Overseas with Mobile Devices at https://www.cyber.gov.au/acsc/view-all-content/publications/travelling-overseas-electronic-devices.
Implementing the settings advised in this guide can significantly reduce system functionality and user experience. Authorising officers are encouraged to consider the balance of user requirements and security, as not all advice may be appropriate for every user or environment.
Organisations should seek approval from their authorising officer to allow for the formal acceptance of the risks involved. Refer to the applying a risk-based approach to cyber security section of the Australian Government Information Security Manual (ISM) for more information.

Evaluation status

Since April 2014, ASD has endorsed the Mobile Device Fundamentals Protection Profile (MDFPP) with specified optional mitigations as a key component in all mobile device evaluations. The MDFPP, as defined by the United States National Information Assurance Partnership (NIAP), outlines the security requirements for a mobile device for use in an enterprise.

Earlier versions of iOS have completed evaluation against MDFPP, and completed ASD Cryptographic Evaluations.

This guide is based on the findings of ASD and provides policy advice that must be enforced for OFFICIAL: Sensitive and PROTECTED deployments of the evaluated device. Guidance in this document will also assist organisations to comply with existing policies when deploying iOS platform devices at lower classifications.

Under the Common Criteria evaluation program, the handsets have undergone evaluation against the Protection Profile for MDFPP version 3.1. More information may be obtained from the Common Criteria portal at https://www.commoncriteriaportal.org/.

Apple has obtained a broad range of certifications for their devices. These are listed at https://support.apple.com/en-au/HT202739.
General advice

Apple typically releases a beta of new major iOS versions in June, and the release becomes generally available in September. New iOS devices can only run new versions of iOS, but there is scope for the upgrade of supervised devices to be explicitly controlled.

For organisations with existing or planned iOS deployments, ACSC advises:

- Actively test beta versions of iOS under AppleSeed for IT and Developer Preview Programs.
- Upgrade to the latest iOS version. This is consistent with ASD’s advice to install the latest versions of software and patch operating system vulnerabilities as communicated in the ISM and the Strategies to Mitigate Cyber Security Incidents.
- Implement any interim guidance contained in ACSC documents such as this guide. In particular, organisations should take note of advice relating to new features and changed functionality introduced by Apple in new versions. This advice is the result of in-house technical testing by ASD, experiences shared by other organisations, and in consultation with the vendor.

Apple provides the detail of new content of security updates concurrently with the release of new iOS versions that address vulnerabilities at https://support.apple.com/en-au/HT201222. This information may help organisations quantify the risk posed by not updating.

iOS encryption


In summary, when configured in accordance with ACSC guidance, the following classes of Data Protection are available:

- Class A: When the device is locked, data afforded Class A Data Protection is suitably encrypted and inaccessible. (Note: There is a 10 second window at Device lock before the ephemeral key is discarded).
- Class B: When the device is locked and the file is closed, data afforded Class B Data Protection is suitably encrypted and inaccessible.
- Class C: When the device is turned off, or powered on and a user has not yet authenticated to the device, data afforded Class C Data Protection is encrypted and inaccessible.
- Class D: Whilst the data afforded Class D Data Protection is still encrypted (as is all data on device), the nature of the encryption and key handling means that the data is not considered inaccessible.

ACSC recommends that all Australian government data handled by the device utilise Class A Data Protection. In general, basic iOS functionality that would be utilised by organisations for government use such as email, attachment viewing and file storage all utilise Class A Data Protection by default. Organisations should note that when using the iOS calendar, attachments are afforded Class A Data Protection, but calendar data and metadata (such as the title of the event and any notes or details) are afforded Class C protection. As such, authorising officers should make an informed decision as to the use of the iOS calendar for OFFICIAL: Sensitive information, and should not include PROTECTED information in any iOS calendar event other than within calendar attachments.

Emails that are stored on the device are afforded Class A Data Protection, except in the case where an email is downloading or being received whilst the device is in a locked state. In this situation, the email and attachment are afforded Class B Data Protection, which means the data is encrypted with an ephemeral key that is not generated from user credentials. Once the device is unlocked and a suitable user credential derived key is generated, the email and attachments are then re-encrypted to Class A Data Protection.
**Supervised devices**

ACSC guidance advises that all devices handling sensitive and security classified Australian government data (OFFICIAL: Sensitive and above) be supervised, including for Bring Your Own Device (BYOD). Supervision is managed through Apple Business Manager and further configured via MDM, as outlined later in this guide. Supervision of devices handling Australian government data is necessary to ensure that the correct policies and configurations are applied throughout the lifecycle of a device. Organisations will need to register with Apple to create Business Manager Accounts and Apple ID’s. High risk implementations of iOS devices, and cases where registering with Apple is either not desirable or technically feasible, may seek ACSC advice for alternatives.

The need for supervision of BYOD is a serious consideration for individuals wishing to work from their own device, as it hands control of the device over to the organisation. As such detailed consideration as to the need for BYOD should be discussed between the user and authorising officer.
Advice to authorising officers

The ACSC has developed the *Strategies to Mitigate Cyber Security Incidents* to help organisations and their authorising officers mitigate cyber security incidents caused by various cyber threats. The most effective set of these mitigation strategies is known as the Essential Eight. While the strategies were developed for workstations and servers, much of the functionality described exists on modern smartphones. Consequently, the risks are just as important to consider on mobile devices. In order to assist authorising officers with understanding security implications, iOS 12, when configured as advised by this guide, has been assessed against the three maturity levels defined for each mitigation strategy:

- Maturity Level One denotes that the security control is partly aligned with the intent of the mitigation strategy.
- Maturity Level Two denotes that the security control is mostly aligned with the intent of the mitigation strategy.
- Maturity Level Three denotes that the security control is fully aligned with the intent of the mitigation strategy.


**iOS 12 and the Essential Eight**

**Application control**

- Finding: Maturity Level Three - Fully aligned with the intent of the mitigation strategy.
- When configured in accordance with ACSC guidance, iOS 12 implements application control that is enforced via cryptographic signatures. iOS application control provides sufficient granularity such that an administrator may approve specific versions of an application.

**Patch applications**

- Finding: Maturity Level Three - Fully aligned with the intent of the mitigation strategy.
- Patches to applications are made available to the device as soon as they are released. When configured in accordance with ACSC guidance, system administrators are able to remotely apply patches to organisation-owned devices.

**Configure Microsoft Office macros settings**

- Finding: Maturity Level Three - Fully aligned with the intent of the mitigation strategy.
- iOS does not support high risk features, such as Microsoft Office macros and Object Linking and Embedding packages.

**User application hardening**

- Finding: Maturity Level Three - Fully aligned with the intent of the mitigation strategy.
- When configured in accordance with ACSC guidance, at risk applications such as web browsers are secured by not supporting Java and utilising content blocker solutions.

**Restrict administration privileges**

- Finding: Maturity Level Three - Fully aligned with the intent of the mitigation strategy.
- iOS 12 restricts administrator permissions by default for both the user and applications.
Patch operating systems

- Finding: Maturity Level Three - Fully aligned with the intent of the mitigation strategy.
- iOS operating system patches are made available directly to the device as soon as they are released. When configured in accordance with ACSC guidance, system administrators are able to remotely apply patches to organisation-owned devices.

Multi-factor authentication

- Finding: Maturity Level Three - Fully aligned with the intent of the mitigation strategy.
- When configured in accordance with ACSC guidance, devices and user identities are authenticated through multiple authentication factors.

Daily backups

- Finding: Maturity Level One - Partly aligned with the intent of the mitigation strategy.
- iOS supports remote backups of some content to solutions approved by either the organisation or the Australian government. Further decisions can be made beyond ACSC guidance to further improve the maturity level of daily backup solutions.
iOS 12 platform feature summary and risk considerations

**Supervised Mode (Applicability: Organisation-owned device)**

<table>
<thead>
<tr>
<th>OFFICIAL: Sensitive</th>
<th>PROTECTED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Required</td>
<td>Required</td>
</tr>
</tbody>
</table>

**Risks**

Without this, devices may not always comply with an organisation’s controls and misplaced devices are unable to be secured remotely.

All organisation-owned devices are required to be supervised. Supervision of devices enables an organisation to enforce broader device policy, monitor the status of the device, manage Activation Lock and enable Lost Mode. iOS devices that handle Australian government data or interact with an organisation’s systems are required to utilise Supervised Mode via Apple Business Manager and an MDM.

The use of Supervised Mode prevents users from being able to sync or backup their device contents to their home computer and ensures that users cannot easily sidestep restrictions without erasing the device. Additionally, iOS forensic recovery utilities may not be able to recover data from the device without a jailbreak.

Supervised Mode increases the difficulty of a number of attacks that rely upon the USB host pairing protocol.

Supervised Mode allows an MDM to manage Activation Lock.

**Supervised Mode (Applicability: Bring Your Own Device)**

<table>
<thead>
<tr>
<th>OFFICIAL: Sensitive</th>
<th>PROTECTED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organisation decision</td>
<td>Required</td>
</tr>
</tbody>
</table>

**Risks**

Without this, devices may not always comply with an organisation’s controls and misplaced devices are unable to be secured remotely.

Organisations have a reduced ability to enforce security, audit and monitoring of non-supervised BYOD.

An organisation’s BYOD deployment model will impact upon the outstanding risk.

An organisation may decide whether BYOD are to be supervised. Supervision of devices enables an organisation to enforce broader device policy, monitor the status of the device, manage Activation Lock and enable Lost Mode. iOS BYOD that handle Australian government data or interact with the organisation’s systems should utilise Supervised Mode via Apple Business Manager and an MDM.

**Device passcode**

<table>
<thead>
<tr>
<th>OFFICIAL: Sensitive</th>
<th>PROTECTED</th>
</tr>
</thead>
</table>
Risks

Device passcodes that do not meet the requirements outlined in ACSC guidance significantly reduce the security posture of the device’s data at rest encryption defences and in scenarios where a device is lost or stolen.

Sufficiently long and complex device passcodes ensure that devices are appropriately protected whilst locked, by ensuring that passcodes are both difficult to guess and that enough entropy is generated by the user credentials to derive adequate ephemeral keys.

Biometric device unlock

<table>
<thead>
<tr>
<th>OFFICIAL: Sensitive</th>
<th>PROTECTED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organisation decision</td>
<td>Not allowed</td>
</tr>
</tbody>
</table>

Risks

When supported by a sufficiently strong device passcode, there is no technical risk difference between using TouchID and FaceID. Deployments of iOS devices using biometrics should consider the practicality and privacy of users, and tailor advice surrounding these features to best suit the deployment scenario.

Authorising officers should seek ACSC guidance to articulate these considerations where a tangible practical demand for biometrics is identified.

The biometric mechanisms of iOS have not undergone an ASD Cryptographic Evaluation, and the security claims of the feature are difficult to assess.

The use of iOS TouchID and FaceID to protect Australian government data may be considered for OFFICIAL: Sensitive deployments, however must not be used when the device handles PROTECTED data.

Non-native applications

<table>
<thead>
<tr>
<th>OFFICIAL: Sensitive</th>
<th>PROTECTED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organisation decision</td>
<td>Organisation decision</td>
</tr>
</tbody>
</table>

Risks

Applications that do not handle Australian government data appropriately or afford a suitable level of encryption are at risk of disclosing or mishandling of Australian government data.

Non-native applications are applications that are purchased for use on the iOS platform, or developed by an organisation for specific use on the iOS platform. Such applications are sourced from the App Store (either public App Store or Custom Apps), or internal to an organisation using Apple Developer Enterprise Program.

Organisations considering the implementation of applications should carefully review the data at rest and data in transit mechanisms offered by the developer to ensure that appropriate encryption mechanisms are being implemented. Data at rest solutions must make use of Class A Data Protection for PROTECTED deployments.
Mobile Device Management

<table>
<thead>
<tr>
<th>OFFICIAL: Sensitive</th>
<th>PROTECTED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organisation decision</td>
<td>Required</td>
</tr>
</tbody>
</table>

**Risks**

Without this, devices may not always comply with an organisation’s controls and misplaced devices are unable to be secured remotely.

The iOS platform allows organisations to automatically manage their devices enrolment in MDM through the Apple Business Manager platform. MDM solutions allow for configuration management, deeper inspection and auditing of devices, as well as a content such as Apps and documents. In certain limited circumstances it may be appropriate to use Apple Configurator as an alternative to, or in conjunction with, MDM.

Organisations implementing MDM solutions are encouraged to use evaluated products under the NIAP’s MDFPP.

Organisations operating in higher risk situations are encouraged to engage the ACSC when developing and implementing MDM solutions.

Using an MDM allows an organisation to vet and deploy applications without user action or using iTunes.

Bring Your Own Device

<table>
<thead>
<tr>
<th>OFFICIAL: Sensitive</th>
<th>PROTECTED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organisation decision</td>
<td>Not recommended</td>
</tr>
</tbody>
</table>

**Risks**

BYOD have a higher risk of introducing malware into an organisation’s networks, and are at risk of being infected with malicious applications or software prior to configuration for handling of Australian government data. As such, organisations should understand the risks around allowing personal devices onto an organisation’s networks, and ensure they follow ACSC guidance.

As long as a device is enrolled in an MDM and appropriately configured, devices handling OFFICIAL: Sensitive data can be BYOD.


Managed Open-In

<table>
<thead>
<tr>
<th>OFFICIAL: Sensitive</th>
<th>PROTECTED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Required</td>
<td>Required</td>
</tr>
</tbody>
</table>
Risks

Devices not correctly configured risk allowing unvetted applications onto the device. These may not meet data at rest and data in transit requirements for Australian government data.

Managed Open-In is built in to iOS and configured by MDM. Managed Open-In allows organisations to decide which applications or accounts configured on a device that can access Australian government data. Even if a device is configured in a ‘work only’ mode with no personal enablement, Managed Open-in can be used to ensure PROTECTED data is only held in and moved between applications that have appropriate data at rest and data in transit behaviours implemented.

Virtual Private Network

<table>
<thead>
<tr>
<th>OFFICIAL: Sensitive</th>
<th>PROTECTED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Required</td>
<td>Required</td>
</tr>
</tbody>
</table>

Risks

Not using a Virtual Private Network (VPN) risks exposing data in transit to increased visibility of both data and metadata by any entities on the networks the data moves through.

Not using a VPN may increase the organisation’s attack surface, as alternatives may require servers to be exposed to the internet.

All data communications for devices handling Australian government data must be through a VPN. Typically BYOD and Corporately Owned, Personally Enabled (COPE) configurations will use Per-App VPN, but some deployments will have a risk profile where they need to use a whole device Always on VPN configuration. The built in IPSec IKEv2 VPN client can be configured via profile for either type. This can be changed dynamically to suit the deployment requirements.

Email applications

<table>
<thead>
<tr>
<th>OFFICIAL: Sensitive</th>
<th>PROTECTED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organisation decision</td>
<td>Organisation decision</td>
</tr>
</tbody>
</table>

Risks

Organisations may resort to over-classified emails if emails aren’t able to be marked by the originator on a mobile device. Additional server processing may be required at the server to handle lesser email client functionality at the mobile device.

If an email client does not provide classification and security markings of emails, organisations should consider configuring email servers to handle marking of emails that are not appropriately manually marked. In some cases installing a Managed Keyboard to simplify marking of emails will be convenient.

The native email client is approved for PROTECTED data, when configured to ACSC guidance. See the iOS Encryption section for more details.
Backups

<table>
<thead>
<tr>
<th>OFFICIAL: Sensitive</th>
<th>PROTECTED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organisation decision</td>
<td>Organisation decision</td>
</tr>
</tbody>
</table>

Risks

Without regular backups, Australian Government data may be irrecoverable should only a local copy of the data exist and become inaccessible.

With unapproved backup solutions, Australian Government data may be extracted and then stored on or transit systems which are not suitable for the sensitivity of the data.

The configuration of devices is set by MDM, and is restored whenever a device is enrolled. Whether backups are necessary depends on the nature of applications in use on a device – for example, email or chat applications are almost always synchronised server storage, and thus do not need a backup from the device. If data of organisational value is being created on device, careful application selection or development can negate the need for institutional data to need be backed-up explicitly from a device, because it is synchronised to servers implicitly (such as using a Content Management System that has a client with a File Sharing Extension). Note that in BYOD or COPE configurations, backup of personal content is generally desirable for users but covered by consumer solutions such as iCloud backup. Managed Apps and Accounts containing Australian government data can be excluded from the backups of personal content, using appropriate configuration from an MDM.

Office for iOS

<table>
<thead>
<tr>
<th>OFFICIAL: Sensitive</th>
<th>PROTECTED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organisation decision</td>
<td>Organisation decision</td>
</tr>
</tbody>
</table>

Risks

Organisations looking to implement Office for iOS are encouraged to contact the ACSC to articulate risks and discuss deployment scenarios.

iOS Calendar

<table>
<thead>
<tr>
<th>OFFICIAL: Sensitive</th>
<th>PROTECTED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organisation decision</td>
<td>Organisation decision</td>
</tr>
</tbody>
</table>

Risks

Should there be sensitive and security classified data in calendar data and metadata, these will not be stored with sufficient protection for Australian government data.

iOS Calendar allows synchronising calendar entries across accounts and devices. The iOS Calendar interacts with other applications to detect dates and times and suggest entries to be submitted to the calendar.

When using the iOS calendar, attachments are afforded Class A Data Protection, but calendar data and metadata (such as the title of the event and any notes or details) are afforded Class C protection. As such, authorising officers should
make an informed decision as to the use of the iOS calendar for OFFICIAL: Sensitive information, and should not include PROTECTED information in any iOS calendar event other than within calendar attachments.

iOS Contacts

<table>
<thead>
<tr>
<th>OFFICIAL: Sensitive</th>
<th>PROTECTED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organisation decision</td>
<td>Not recommended</td>
</tr>
</tbody>
</table>

Risks

iOS Contacts does not store details with sufficient protection for Australian government data.

iOS Contacts implements specific controls set by MDM for flow of contact information between Managed and Unmanaged spaces (for example, whether a managed contact can be used to display a person’s name at the lock screen, instead of their phone number for an incoming call).

iOS Contacts data is stored on the device in Class C, and if names and phone numbers are considered PROTECTED by an organisation, then consideration should be given to using a dedicated application to manage such contacts. Please engage ACSC in such situations.

iOS Camera App

<table>
<thead>
<tr>
<th>OFFICIAL: Sensitive</th>
<th>PROTECTED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organisation decision</td>
<td>Not recommended</td>
</tr>
</tbody>
</table>

Risks

Photos taken with the camera application are stored locally and may be transferred automatically to locations that do not have sufficient protection for Australian government data.

In BYOD and COPE devices, or deployments where photographs may be considered PROTECTED, consider using a dedicated purpose built camera app that stores photos in Class A for all photography on official duties.

The built in Camera App uses Class C data protection to store photographs, and depending on configuration by MDM, may be allowed to sync data to iCloud Photo Stream or to users’ personal, unmanaged devices.

iOS Books App

<table>
<thead>
<tr>
<th>OFFICIAL: Sensitive</th>
<th>PROTECTED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organisation decision</td>
<td>Not recommended</td>
</tr>
</tbody>
</table>

Risks

iOS Books App does not store data with sufficient protection for Australian government data.

MDM can push iBook, ePub and PDF documents into the native iBooks App on device. Such documents are considered managed by built in controls and are not included in backups, nor can they be moved to unmanaged destinations or synchronise to iCloud. However, any PROTECTED documents must use a dedicated application that uses Class A data protection.
iBooks App uses Class C data protection, so it is only suitable for documents classified OFFICIAL: Sensitive or below.
Further information


Contact details

If you have any questions regarding this guidance you can contact us via 1300 CYBER1 (1300 292 371) or https://www.cyber.gov.au/acsc/contact.