Australian Government
Australian Cyber Security Centre

ACSC
AUSTRALIAN CYBER SECURITY CENTRE

iOS Hardening Configuration Guide

For iPod Touch, iPhone and iPad devices running iOS 8.3 or higher.

acsc.gov.au

PARTNERING FOR A CYBER SECURE AUSTRALIA

iOS Hardening Configuration Guide

About this Guide

This guide provides instructions and techniques for Australian government agencies to harden the security of iOS 8 devices.

Implementing the techniques and settings found in this document can affect system functionality, and may not be appropriate for every user or environment.

In these cases, agencies should seek approval for non-compliance from their accreditation authority to allow for the formal acceptance of the risks involved. Refer to System Accreditation and Product Selection chapters of the *Australian Government Information Security Manual* (ISM) for more information.

Evaluation status

At the time of publication, the latest version of Apple iOS on iPhone, iPad, and iPod Touch has commenced but not completed an ASD recognised evaluation.

https://www.niap-ccevs.org/CCEVS_Products/in_eval.cfm

Apple iOS 8 was launched on 17th September 2014. As per Apple's usual practice, the previously released version, iOS 7 is no longer available for download.

For agencies with existing or planned iOS deployments, ASD advises the following:

a) **Upgrade to iOS 8.3 or later.** Even though iOS 8 has not completed an evaluation, this version does provide security enhancements and addresses a number of software vulnerabilities. This is consistent with ASD's advice to install the latest versions of software and patch operating system vulnerabilities as communicated in the Australian Government Information Security Manual and Strategies to Mitigate Targeted Cyber Intrusions.

b) **Implement the interim advice contained in this guide.** In particular, agencies should take note of advice relating to new features and changed functionality introduced by Apple in iOS 8. This advice is the result of in-house technical testing by ASD, experiences shared by other agencies, and in consultation with the vendor.

Agencies should be made aware that since April 2014, the Australian Signals Directorate (ASD) has endorsed the Mobile Device Fundamentals Protection Profile (MDF PP) as a key component in all new mobile device evaluations. The MDF PP, as defined by the United States' National Information Assurance Partnership (NIAP), outlines the security requirements for a mobile device for use in an enterprise. The process for evaluation is described in detail on ASD's website:

http://www.asd.gov.au/publications/dsdbroadcast/20140410-evaluation-pathway-for-mobile-devices.htm

As in any case where significant updates of a previously evaluated product are issued by a vendor, agencies should investigate the changes as part of their risk management process. Agencies must refer to the Product Security section of the Australian Government Information Security Manual to ensure compliance when planning to use an unevaluated product.

Apple provides detail of the content of security updates. This information may help agencies quantify the risk posed by not updating.

https://support.apple.com/en-au/HT1222

iOS and the Australian Government Information Security Manual

This guide reflects policy specified in the ISM. Currently, not all ISM requirements can be implemented on iOS 8 devices. In these cases, risk mitigation measures are provided in the Risk Management Guide at Chapter 11.

Chapter 6 provides recommended passcode settings for iOS devices. This advice has been developed based on an assessment of security risks related specifically to iOS 8, and takes precedence over the non-platform specific advice in the ISM.

About the Australian Signals Directorate

As the Commonwealth authority on the security of information, the Australian Signals Directorate provides guidance and other assistance to Australian federal and state agencies on matters relating to the security and integrity of information.

For more information, go to http://www.asd.gov.au/about/.

Audience

This guide is for users and administrators of iOS 8 or later devices. These devices include the iPod Touch, iPhone and iPad.

To use this guide, readers should be:

- familiar with basic networking concepts
- an experienced systems administrator

Parts of this guide refer to features that require the engagement of the technical resources of agency telecommunications carriers, firewall vendors, or Mobile Device Management (MDM) vendors. While every effort has been made to ensure content involving these third party products is correct at the time of writing, agencies should always check with these vendors when planning an implementation.

Mention of third party products is not a specific endorsement of that vendor over another; they are mentioned as illustrative examples only.

Some instructions in this guide are complex, and if implemented incorrectly could reduce the security of the device, the network and the agency's security posture. These instructions should only be used by experienced administrators, and should be used in conjunction with thorough testing.

For further clarification or assistance, Australian government IT Security Advisors can consult the Australian Signals Directorate by emailing asd.assist@defence.gov.au or calling the ASD Cyber Hotline on 1300 CYBER1 (1300 292 371).

What's Changed

iOS 8 has brought with it many important new features and improvements. Apple has opened the platform further to app developers with "app extensions" while simultaneously reenforcing platform security. Enterprise administrators are given more control with new configuration profile payloads and restrictions. While users are given a number of new features, many will challenge administrators of business only iOS fleets.

Continuity

Continuity is the name given to a group of new features which enable a user to transition an activity from one device to another. This includes:

- Allowing a user to move from one device to another, and have their internet browsing state preserved.
- Allowing a user to take advantage of their iPhone's cellular network from another associated device for phone calls, messaging and network connectivity.

Refer to Security Features and Capabilities for updated advice on the risks and benefits associated with Continuity.

App Extensions

Third party apps with app extensions can now make available content and functions to other apps in iOS. For example:

- An app may install a custom keyboard that replaces the default iOS keyboard
- Custom Actions allows a third party app to provide a service such as document translation to content in another app.

Refer to Security Features and Capabilities for updated advice on the risks and benefits associated with App Extensions.

New Configuration Profile Controls

New management and supervisory controls have been made available to iOS enterprise fleet administrators. Refer to Recommended Device Profile Settings for our updated advice.

Improved VPN guidance

iOS 8 contains several under-the-hood changes to VPN behaviour. Refer to the VPN section for detail.

Feedback

Advice has been updated throughout the guide based upon the experiences of Australian Government agencies and from industry.

If you have feedback email: asd.assist@defence.gov.au

Chapter 1

Introduction to Mobile Device Security

Understand the key technologies that can be used to secure iOS mobile devices.

Introduction to Mobile Device Security

This chapter provides the planning steps and architecture considerations necessary to set up a secure environment for mobile devices. Much of the content in this chapter is platform agnostic, but some detail is written to address specific features available in iOS. Not all of the options discussed will be applicable to all environments. Agencies need to take into account their own environment and consider their acceptable level of residual risk.

Assumptions

This chapter makes some basic assumptions regarding the pervasive threat environment:

- at some point, there will be no network connection present
- all radiated communication from the device has the potential to be monitored
- all conventional location, voice and SMS/MMS communications are on an insecure channel
- certain infrastructure supporting mobile devices can be trusted
- carrier infrastructure cannot always be trusted as secure in all countries
- at some point, devices will be lost or stolen
- lost or stolen devices will be in a locked state
- third party apps will leak sensitive data.

Offline Device Security

When a device is offline, protection of data on the device is determined by how the device implements data protection locally. There can be no referral to a server for policy or any remote wipe command if there is no network present.

When offline, the security of the device is determined by:

- policy enforced by iOS from Exchange ActiveSync (EAS) or Configuration Profiles
- policy enforced by third party mobility management apps
- the security settings set locally on the device (such as passcode policy and USB pairing restriction)
- the device's cryptographic capabilities
- the correct use of file protection classes and Keychain by apps
- the strength of the device passcode.

Device Security on the Network

The general principle that applies for all data when the device is on a network is that wherever possible, all network traffic should be encrypted, noting that all classified network traffic must be encrypted as per the Cryptography chapter of the ISM. This is not merely achieved by turning on a Virtual Private Network (VPN) for all traffic. Typically this involves using a mixture of:

- TLS to encrypt connections to specific hosts such as mail servers or management servers that need to be highly reachable
- TLS for any traffic containing sensitive data
- a VPN for more general intranet access
- WPA2 with EAP-TLS as a minimum for Wi-Fi security
- 802.1X authentication on Wi-Fi networks combined with Network Access Controls to compartmentalise Wi-Fi access to defined security domains
- data at rest encryption on mobile devices and transport security.

Some third party mobility management vendors may provide an operating system integrity check. Though a useful compliance feature, it cannot be relied upon. Details are available in the Jailbroken Employee Owned Devices section.

Apple Push Notification Service

Many apps and services associated with iOS devices take advantage of the Apple Push Notification Service (APNS). APNS allows apps to “phone home” to their servers, and be sent small notifications, such as updating the badge on an icon, playing an alert tone, or displaying a short text message.

Apple’s documentation on APNS refers to servers that communicate with apps as “Providers”.

Example of providers include push email notification, Mobile Device Management (MDM) servers and iOS client-server applications that are able to execute in the background (such as VOIP apps, streaming audio apps, or location tracking apps). Providers send a request to the device to “phone home”, and the app or agent on the device establishes communication with and responds to the provider. For example, MDM servers send an APNS request to the Apple MDM agent on the device. The Apple MDM agent then “phones home”, establishing a TLS tunnel directly to the MDM server, and exchanging XML queries and responses inside this tunnel.

It will be necessary to set appropriate firewall rules to enable APNS. Refer to Firewall Rules in Chapter 12 for information on ports and services.

Data Roaming

Data roaming generally refers to a process by which your cellular device is able to receive data on mobile networks that your telecommunications operator doesn’t own.

There are two main risks associated with data roaming:

- When roaming internationally, there are both implied and actual lower levels of trust with the level of eavesdropping and traffic analysis occurring on the foreign network. As soon as traffic goes international, it is no longer subject to the privacy and consumer protection requirements that apply to purely domestic communications in the host country. It is incorrect to assume that the rights protecting individual’s privacy are uniform internationally.

- If data roaming is switched off for cost management, then the device is “off the grid” for management and monitoring consoles such as EAS, MDM, or iCloud’s “Find My iPhone”.

iOS devices may be configured to disable voice and data roaming via MDM, but it is possible for users to re-enable roaming on their devices.

Apps

As outlined in ASD’s *Strategies to Mitigate Targeted Cyber Intrusions*, ASD recommends that only applications that are required should be installed. There are a number of ways to procure and load applications onto an iOS device.

App Store

The App Store is hosted and curated by Apple, and is focused on mass-market distribution of paid and free applications. Apps are loaded to a device:

- Over-The-Air (OTA) from the App Store itself
- OTA via a Mobile Device Management (MDM) solution
- via USB on a paired host running Apple Configurator
- via USB/network on a paired host computer running iTunes.

Apple maintains discretionary control of curating App Store content, and can remove applications for a variety of reasons. ASD recommends that corporately provisioned apps are tested and approved by the agency prior to use.

Although App Store applications come from a curated environment, and the runtime environment the apps execute in is a relatively hardened one, Apple’s app review process is focused on end user privacy, and does not implement ISM policy. Agencies should assess the risks associated with allowing unrestricted user-initiated installation of apps, building on Apples’ review process. Some additional risks that need to be considered are:

- the inappropriate use of data protection
  - Most App Store apps default to Class C, PROTECTED data must be stored in Class A or Class B.
- the inappropriate use of transport security
  - Ensure that apps use iOS native TLS APIs and mitigate against man-in-the-middle attacks using certificate pinning where possible.
- the inappropriate access of contact list, photos, location information, and synchronisation of data with cloud services
- the registration of Uniform Type Identifiers (UTIs) and URL handlers.

Agencies can manage these risks through discussions with the app developer or through conducting professional penetration testing. Refer to Managing Apps and Data in Chapter 5 for information on questions to ask app developers.

Note: App Store apps may be automatically updated over the air using Wi-Fi.

In-House apps

Through the use of an ad-hoc provisioning profile, up to 100 instances of a signed application binary can be installed via iTunes or Apple Configurator.

Ad-hoc applications are locked to a specific set of devices by the provisioning profile. These are most commonly used for beta testing of applications, or where very restricted distribution of a small number of instances of a bespoke application is appropriate.

Agencies with a Dun and Bradstreet Data Universal Numbering System (DUNS) number can apply to become Enterprise developers. This allows the creation and distribution of custom applications and provisioning profiles within an agency for its own use, where the distribution is limited to employees and contractors (i.e; not to the general public).

Enterprise In-House apps can be installed using:

- Apple Configurator (USB only)
- OTA via web site
- OTA via MDM server
- iTunes (USB and Wi-Fi).

In all the above cases, an MDM console allows monitoring of versions of apps installed on a device. This allows a management decision as to when updates are required.

Volume Purchase Program (VPP)

The VPP allows businesses to buy app store apps in bulk using a corporate purchasing card. Agencies with a VPP account may also use the Business to Business (B2B) portal to request custom versions of App Store apps directly from app developers. Agencies may request custom apps that utilise a stronger use of data protection or transport security APIs, or request that functionality (such as cloud synchronisation) is disabled.

Historically, apps purchased through VPP were redeemed by a user to a particular Apple ID permanently. Recent changes to VPP now allow apps to be both assigned to and revoked from users.

For more information on VPP go to http://www.apple.com/au/business/vpp/

Managed apps

App Store and Enterprise In-house Applications installations can be triggered via an MDM server; these apps are called “Managed apps”. Managed apps can be uninstalled by the MDM server along with any associated data or can be set to uninstall when the MDM profile is removed.

Web apps

The iOS web browser Mobile Safari has extensive support for HTML5, CSS3 and JavaScript features for web apps. This is often a useful mechanism to deploy informational applications quickly from a central intranet point; however Mobile Safari on iOS is still subject to the same threats as other browsers.

iTunes

iTunes is no longer a requirement for device management. If agencies decide to use iTunes as part of their device management workflow it can be locked down for use on agency Standard Operating Environments (SOE) via registry keys or XML property lists as detailed here:

http://help.apple.com/iosdeployment-itunes/mac/1.2/

Apple IDs

One of the organisational risks that some users express concern about is a perceived need to associate a credit card with every Apple ID. This is actually a misconception, and no association with a credit card is required. The following approaches are recommended at the policy and procedural level.

For a Bring Your Own Device (BYOD) model, there is generally implied trust that users can continue to install apps on their own device. Therefore, users may register their existing Apple ID as part of the process of submitting to the agency Acceptable Use Policy (AUP). If users then purchase approved apps, using their own credit card, they can be reimbursed. This provides one method to control expenditure of agency funds. An MDM console can be used to monitor what applications have been installed.

For an agency owned device model, where users are not allowed to install their own apps, per device Apple IDs are created that are not linked to a credit card. The process for doing this is described here:

http://support.apple.com/kb/HT2534

Individual app redemption codes, or store credit can then be gifted to those accounts and installed on the devices from an agency owned computer using iTunes. Note that the end user requires the Apple ID password in order to enable application updates.

Apple IDs can be optionally used to create free iCloud accounts to facilitate user initiated device location and remote wipe.

Siri

Siri provides voice to text services by transmitting voice data to remote services for processing. Any dictation performed using Siri must be considered Unclassified. By default Siri can be used from a locked screen to perform actions such as opening emails and reading calendar entries. This behaviour can be disabled via Configuration Profile restriction while still allowing Siri when unlocked.

Lock Screen Services

By default locked iOS devices still provide some limited services for user convenience. These lock screen services may be administratively disabled, although in doing so there is a security versus usability trade off.

Control Centre

The Control Centre panel is accessed at the lock screen with an upward swipe from the bottom of the screen, and contains the following:

- airplane mode, Wi-Fi, Bluetooth, Do-Not-Disturb mode, rotation lock and flashlight on/off switches
- screen brightness
- volume and media playback controls
- AirDrop discoverability control and AirPlay output selection
- access to Stopwatch, Calculator and Camera apps.

Although the new control centre has many useful user convenience functions, there are risks in enabling it from the lock screen. Control Centre can be disabled at the lock screen via Configuration Profile restriction.

Notification Centre

Notification Centre and Today View are accessed from the lock screen with a downward swipe from the top of the screen. iOS displays APNS notifications at the lock screen such as messages (iMessage) or invitations/requests (GameCentre).

Although such content must be Unclassified, revealing notifications at the lock screen is not recommended. Notification Centre from lock screen can be disabled via Configuration Profile restriction.

Today View

Today View gives a summary of information about a user's day. Normally this will include the day's weather, traffic and calendar entry.

Today view can be disabled via Configuration Profile restriction.

Planning your mobility deployment

Every Australian government agency should have a BYOD policy, even if that policy is "No employee owned devices are to be allowed on the agency network". A*SD's Risk Management of Enterprise Mobility including Bring Your Own Device (BYOD)* provides advice regarding the risks and benefits of a number of possible mobility approaches. It comprehensively covers:

- the potential benefits of enterprise mobility
- how to choose an appropriate mobility approach, including:
    - corporately owned devices allowing limited personal use
    - employee owned "Choose your own device" (CYOD)
    - developing mobility policy
    - risk management controls.

This document is a thorough guide to planning a mobile deployment and is available at:

http://www.asd.gov.au/publications/csocprotect/enterprise_mobility_bring_your_own_device_byod_paper.htm

CHAPTER 2

Security Features and Capabilities

Trust This Computer?

Your settings and data will be accessible from this computer when connected.

Mobile device security features, and the enabling technologies for implementing those features under iOS.

Security Features and Capabilities

This chapter covers mobile device security features, and the enabling technologies for implementing those features under iOS and related infrastructure.

Security features in iOS

iOS provides a number of features that include:

- management of credentials and passwords with Keychain
- encryption of data at rest and in transit (using AACA and AACP)
- digital signatures, certificates and trust services
- randomisation services
- code signed applications.

Enterprise In-House Applications developed for an agency should generally take advantage of these services, rather than re-inventing the same capabilities.

Configuration Profiles

Configuration Profiles are XML formatted plist files that contain device settings, security policies and restrictions. An administrator may use a Configuration Profile to:

- set passcode policy on a device
- set restrictions (such as disabling use of Siri)
- configure wireless networks
- configure VPN
- configure email
- install X.509 certificates
- set a Mobile Device Management (MDM) server.

These are only a few examples of possible configuration options. For more information please see the iOS Configuration Profile Reference:

https://developer.apple.com/library/ios/featuredarticles/iPhoneConfigurationProfileRef/

Note: Configuration Profiles are not encrypted.

Credentials that are stored in Configuration Profiles are available to anyone who has access to the files. Passwords may be in clear text or encoded in base 64, which offers no protection.

Some of the credentials that could be in a Configuration Profile include:

- Wi-Fi passwords
- VPN Shared secrets
- Email usernames/passwords
- ActiveSync usernames/passwords
- LDAP usernames/passwords
- CalDAV usernames/passwords
- CardDav usernames/password
- Subscribed Calendars usernames/passwords
- SCEP pre-shared secrets.

Note: Take care to ensure that Configuration Profile files are stored appropriately and not improperly accessed.

Provisioning Profiles

Provisioning profiles allow custom applications to be run on iOS devices. They are often used in the following ways:

- to allow developers to test applications on their devices
- to allow organisations to distribute applications directly to their employees.

To obtain an enterprise distribution provisioning profile, an agency must join the Apple Developer Enterprise Program. More information about the iOS Developer Enterprise Program can be found at:

http://developer.apple.com/programs/ios/enterprise/

Note: If the enterprise program login is compromised an adversary could install malicious applications on users' iOS devices.

Find My iPhone and Activation Lock

Find my iPhone (FmiP) is an iCloud service which allows users to locate and remote wipe their Apple devices. On devices which have not been configured as supervised, FmiP enables a feature called "Activation Lock". This feature ties the Apple ID used for FmiP to device activation. Following a device wipe or OS installation, a user must enter their Apple ID credentials. This is intended to reduce the resale value of stolen devices, as the device cannot be used without knowledge of the original user's Apple ID.

Activation Lock has the potential to deny an organisation access to its own devices. If Activation Lock is enabled on an agency owned iOS device with a user's personal Apple ID, the user must disable FmiP prior to returning the device for service. If the device were returned with Activation Lock enabled, the agency would not be able to re-activate after re-installing iOS, and may not remove FmiP even if the device passcode was known.

By default, supervised devices have Activation Lock disabled, however agencies may choose to re-enable this through the use of Configuration Profiles. Please refer to the Activation Lock section of the Deploying iOS Devices chapter for further information.

The link below contains information on how personal users may take advantage of the service.

http://www.apple.com/au/icloud/find-my-iphone.html

Sandboxing

Sandboxing ensures that applications that run on iOS devices are restricted in terms of the resources that they can access. This is enforced by the kernel.

For detailed information on the iOS/OS X sandbox see Dion Blazakis's paper The Apple Sandbox or Vincenzo Iozzo's presentation A Sandbox Odyssey.

Managed Apps and Extensions

When devices are enroled in to MDM, apps and app extensions obey "Managed Open-In" restrictions. This feature allows administrators to configure devices in a way that prevents documents being exported from "managed" to "unmanaged" (user) applications. It can also be used to prevent unmanaged app extensions being accessible from managed apps. These native features have reduced the need for the use of managed container applications, however there may be cases where an agency may seek a third party solution.

In cases where the agency requires greater protection of their contact and calendar information a third party solution may be required.

A number of managed container solutions can be used to provide:

- finer grained control and policy enforcement for data transmission between apps which support the 3rd party SDK
- "app wrapping" to enhance existing security or add restrictions to previously developed in-house apps
- a suite of apps which have been designed to enforce a secure workflow.

There are a number of non security related trade-offs which should also be considered before the use of 3rd party container solutions:

- 3rd party container solutions often have a lower level of integration with both apps present in iOS and common App Store apps
- many 3rd party container solutions rely upon software encryption which is slower than those which rely upon the hardware accelerated native data protection offered by iOS
- container solutions which rely upon software encryption may require an additional passcode separate to the device passcode, often with an increased complexity requirement.

When used, care must be taken to prevent a situation where the agency provided container solution is so prohibitive that users attempt to start working their way around the system.

Information regarding evaluated container solutions is available on the EPL:

http://www.asd.gov.au/infosec/epl/

Content Filtering

Access to intranet sites and some mail, contact or calendar data can be achieved via reverse proxies and content filters. There are multiple solutions in this space.

EAS filtering products can be used to ensure email sent to EAS devices have appropriate protective markings for the classification the device is approved to by an agency. This approach allows mobile devices to only receive email content at a classification appropriate to the device, as well as having policy and controls applied to the email content.

In this scenario, the agency's Wide Area Network (WAN) security domain is not extended out to the mobile device, and there is no need to lower the classification of the agency WAN. Such solutions can be used to redact specific content patterns from emails sent via EAS, for example, to scrub credit card numbers from all emails synced to mobile devices. This class of tools can also facilitate correct protective marking of email coming from mobile devices without direct on-device support for Australian government marking standards. For further information see the ISM section on Content Filtering.

Enterprise Single Sign On (SSO)

Enterprise SSO helps to reduce the number of times a user is required to enter credentials, particularly when switching between apps. SSO is built on top of kerberos, which is the industry standard authentication scheme already present in many corporate networks.

To take advantage of SSO, agencies must create and then deploy an Enterprise SSO Configuration Profile payload. This payload contains:

- username (PrincipalName)
- kerberos realm name
- a list of URL prefixes where kerberos authentication should be applied
- a list of app identifiers which will be granted access to kerberos.

Some apps support SSO without modification, others may have to be updated to take advantage of Apple's higher level networking APIs.

For detail please refer to the Apple WWDC 2013 presentation: Extending Your apps for Enterprise and Education Use (Apple Developer login required):

http://devstreaming.apple.com/videos/wwdc/2013/301xcx2xzxf8qjdcu3y2k1itm/301/301.pdf

Per App VPN

In deployments which permit limited personal use, Per App VPN can be used to divide work and personal network traffic. Typically, this would be configured so that corporate network traffic from managed apps traverses a VPN back to the corporate intranet, while unmanaged personal apps connect to the internet directly or through a proxy. This VPN enhancement is intended to increase the privacy of the user by not transmitting their personal network traffic through corporate infrastructure while at the same time protecting the corporate network from traffic generated by unmanaged apps.

Secure Browser

Where Per App VPN is used, a “Secure Browser” may be mapped to use the configured Per App VPN for corporate network traffic exclusively. There are several advantages to using a separate secure browser:

- a secure browser may be chosen that protects cached data and credentials in a higher data protection class than Safari
- depending upon MDM solution, a secure browser may have corporate data wiped when a device is lost/stolen, out of compliance, or upon other configurable triggers.
- when the secure browser is mapped to the corporate intranet Per App VPN, users may be permitted to use Safari for ordinary internet access. This reduces the risk of sensitive data transmission from corporate intranet to internet. In this case, Safari may still be configured with a web proxy to protect against web based threats and for acceptable use policy enforcement.

Global Proxy

Supervised devices may be configured with a “Global Proxy” setting. This allows administrators to configure supervised devices to use a specified HTTP(S) proxy on all network interfaces.

Continuity

Continuity is the name given to a group of iOS and Mac OS X features which enhance device to device collaboration. For more information on this feature visit Apple’s website:

https://www.apple.com/au/ios/whats-new/continuity/

Continuity offers some productivity benefits for organisations, while at the same time creating some new concerns such as:

- A corporate iOS device may handoff a sensitive or classified document being worked on to a user’s personal Mac with the same Apple ID. *Handoff may be administratively disabled by configuration profile restriction.*
- For phone calls and messages, the level of protection given to data on an untrusted Wi-Fi network. *Refer to Apple’s* iOS Security Guide *for details.*

App Extensions

Beginning with iOS 8, 3rd party iOS App developers may create functionality which may be utilised by other apps on the device. App Extensions cannot be disabled through configuration profile restriction. For details regarding features, please refer to Apple’s documentation:

https://developer.apple.com/app-extensions/

Some organisational concerns may include:

- User installs custom keyboard extension which transmits keystrokes to a 3rd party.

- User uploads sensitive or classified data to a 3rd party document provider.
- User shares sensitive or classified data using a custom share extension.

When an app with an extension is installed, both the app and the extension may be considered “Managed” or “Unmanaged” depending upon how the App was installed. Additionally, App Extensions respect Managed Document configuration profile restrictions.

If the following settings are disabled by configuration profile:

Allow documents from managed apps in unmanaged apps

Extensions installed with MDM deployed managed apps can’t be activated by user installed App Store apps. For example, a corporate installed document provider extension can’t be used by a user’s personal app store app.

Allow documents from unmanaged apps in managed apps

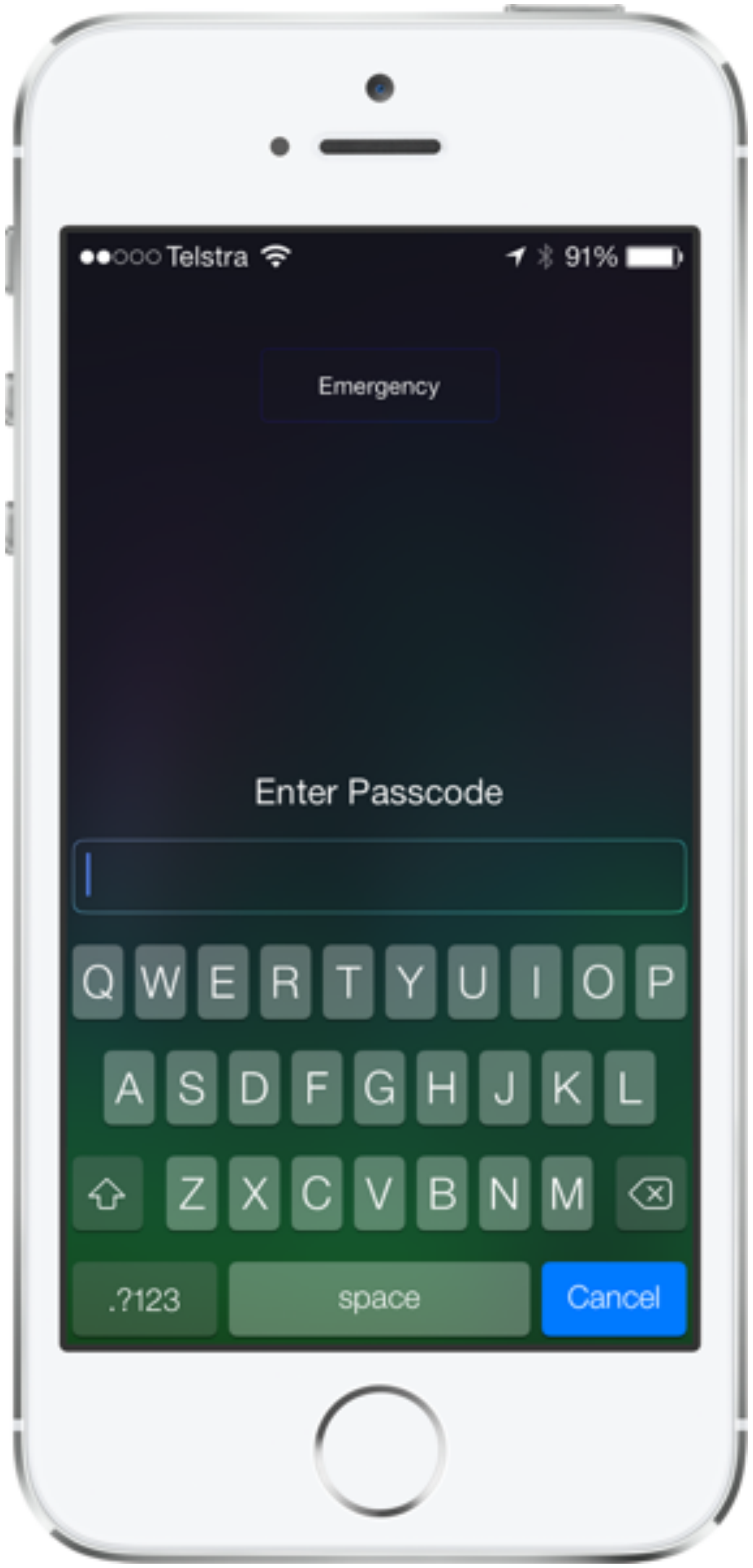
Extensions installed by user App Store apps can’t be activated by MDM installed managed apps. For example, a user installed custom keyboard can’t be used by corporate apps.

Capability	Enablers	Comment
Remote Wipe	MDM, EAS, Apple Push Notification Service (APNS), Find My iPhone	Remote wipe can be initiated by a user through Find my iPhone or by an administrator through MDM. Third party MDM software may offer a separate “Enterprise Wipe” which is intended to erase data in a secure container or selected apps.
Proxy	VPN, Global Proxy	A proxy can be set on a VPN session.
Firewall	VPN to firewalled corporate network	iOS does not implement a local firewall. This is significantly mitigated by the hardened runtime environment.
Force Device Settings	Apple Configurator and MDM	Apple Configurator and MDM may be used to generate, sign and deploy Configuration Profiles to iOS devices.
Multi-factor Authentication	TLS CA infrastructure, DNS, RSA or CryptoCard (VPN Only), Smartcard (Requires third party software and hardware)	Depending on the agency’s security posture, device certificates or soft tokens may be considered as a second factor of authentication. At the time of writing, Touch ID can not be used for multi-factor authentication.
OTA Configuration Profile (pull)	TLS CA infrastructure, DNS, Web Service, Directory Service	Sign profiles using enterprise CA infrastructure.
Mobile Device Management	Enterprise Developer Agreement, 3rd Party MDM appliance, CA infrastructure, DNS, Directory Services, APNS	MDM should be tied into CA and Directory Services.
Remote Application Deployment	Enterprise Developer Agreement, Web Server, 3rd Party MDM appliance (optional), APNS (optional)	Enterprise and App Store apps can be remotely deployed. Mac OS X Server Caching Server may help reduce corporate network internet consumption.
Home screen	Apple Configurator / MDM	Set Home screen to “If found return to PO BOX XXXX”.

Table 2.1: Capability enablers

CHAPTER 3

Encryption in iOS



Keeping data safe when the device is out of your control.

Encryption in iOS

This chapter is provided to help agencies understand the underlying encryption architecture employed in iOS 8 to assist make an informed assessment of the risks to Australian government information.

Data Protection

Apple has explained that one of the goals of iOS is to 'keep data safe even when the device is compromised'. However, as will be explained in this chapter, the onus remains largely on app developers as to how much or how little data protection is applied.

For this reason, it is important that an agency wishing to use a particular application understands the security features of iOS 8 in order to make a more informed decision as to whether the application meets the security needs of the agency.

It is important to note that if devices are not configured to use the Managed Open-In feature, users can still move attachments to apps that use lower data protection classes. This can happen if installed apps have registered document types or URL handlers.

Secrets and Data

Within iOS 8, information stored by apps can be broadly categorised as either a secret or as data. The term secret can be understood to mean information by which one may get access to data; this can include system credentials, keys and passwords. Data on the other hand, refers to user/application data such as text, pictures and documents.

Accordingly there are two data stores where a developer should choose to store information: the Keychain and the File System. Developers are encouraged to store secrets within the Keychain and place more general application data within the File System.

Information stored within either of these stores can be customised to different levels of security, accessibility and portability. Note that it is entirely up to the developer to determine the level of protection applied. This choice is made by the app developer through API calls and the choice of availability as detailed in Table 3.1.

For included iOS apps, the default file system protection class utilised is "...CompleteUntilFirstUserAuthentication", and most iOS Keychain items utilise "…AfterFirstUnlock".

Note: Agencies developing or making use of applications handling sensitive data should take care to investigate how data is handled within their application. They must ensure the appropriate data stores and availability flags (outlined in Table 3.1) are used to achieve the secure handling of Australian government information.

Classes of Protection

An application developer has the option of setting the following availability flags with any File System Element or Keychain entry they create.

Availability	File system element	Keychain entry
When unlocked	...Complete	...WhenUnlocked
While locked	...CompleteUnlessOpen	N/A
After first unlock	...CompleteUntilFirstUserAuthentication	...AfterFirstUnlock
Always	...None	...Always

Table 3.1: File system class accessibility

From Table 3.1, it is possible to abstract these settings into four standard classes of containers with the following behaviour:

Class A: Files and credentials within this class can only be read or written when the device is unlocked.

Class B: Through the use of public key cryptography, files within this class can be written after the device is initially unlocked, and can be read only when unlocked.

Class C: Files and credentials within this class can be read or written only after the device is initially unlocked. App Store apps use this class by default. Powering off or rebooting the device will render data in this protection class inaccessible.

Class D: The lowest protection class, files and credentials within this class can be read or written to in all conditions.

iOS Encryption Architecture

Figure 2.1 illustrates an example where four files exist, each assigned a different class:

- File 1 is of type Class A: accessible only when unlocked
- File 2 is of type Class B: can be written to after first unlock, but can only be read when unlocked
- File 3 is of type Class C: accessible after first unlock
- File 4 is of type Class D: accessible always.

Note that while files were used for the purposes of this example, with the exception of Class B, Keychain entries could just as easily be used in their place.

Similar to the File System, an application's credentials stored within the Keychain are encrypted using the appropriate Class Key found within the System Keybag (refer to the Keybag Section of this chapter for more information).

However, as illustrated in Table 3.1, the protection offered by Class B is only available to File System Elements.

In Figure 2.1, irrespective of class, each file is encrypted with both a unique File Key and a File System Key.

The File System Key is used to encrypt all data within the device. As it is stored openly its use does not add to the cryptographic security of data, but is instead used to facilitate a remote wipe. Refer to the Remote Wipe section of this chapter for more information regarding this function.

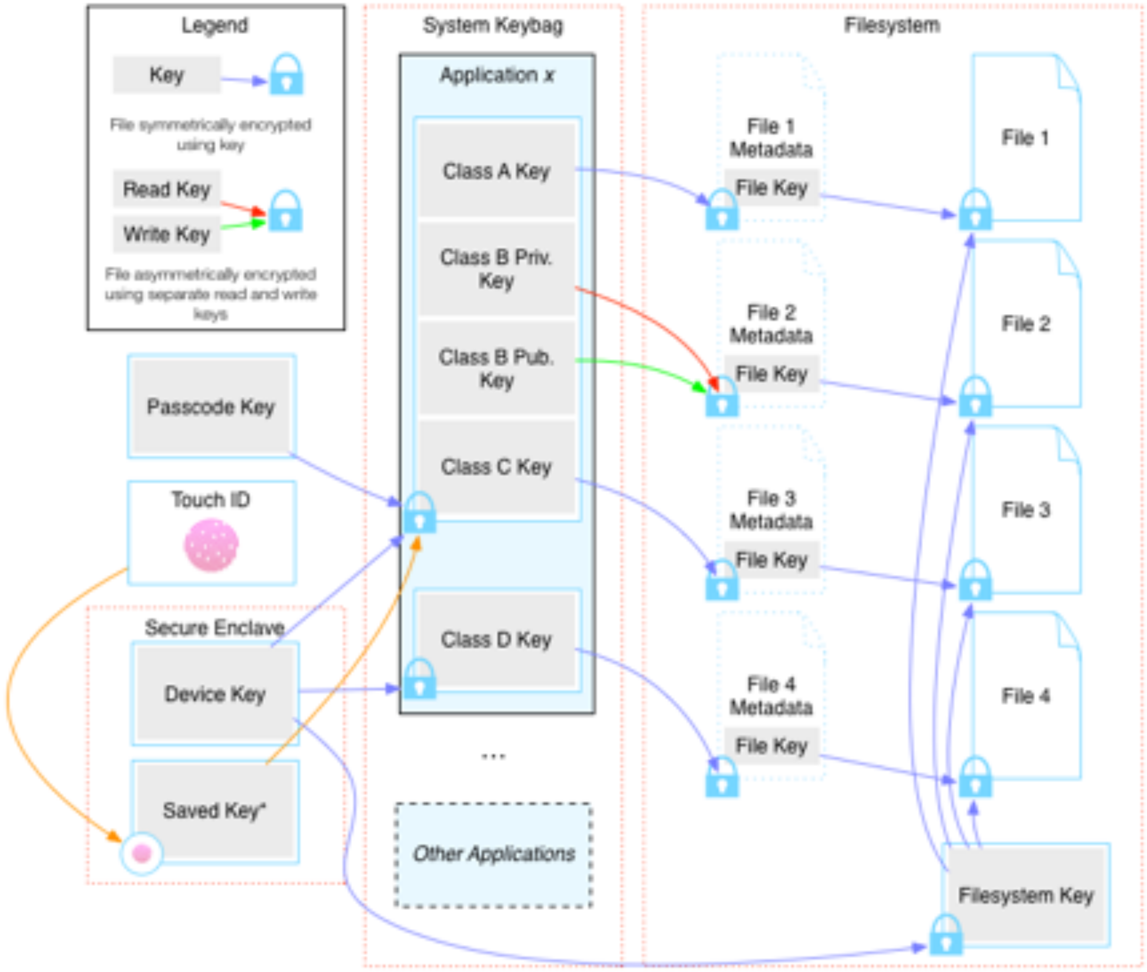


Figure 3.1: iOS File System Architecture

The File Key is stored within the file's metadata, which is itself encrypted by the file's corresponding Class Key. The System Keybag stores all Class Keys within the device. Refer to the Keybag section of this chapter for more information on different types of Keybags used throughout the system.

Upon turning on the device, the Class A, Class B (public and private) and Class C keys are initially inaccessible as they rely on the Passcode Key to be unencrypted.

When the device is first unlocked by the user, through the use of their passcode, these keys are unencrypted, stored for use and the derived Passcode Key promptly forgotten.

The Device Key is stored within, and never divulged from, the Hardware Security Module (HSM). This acts to encrypt and decrypt files at will using the Device Key. Refer to the Hardware Security Module section of this chapter for more information on this component.

The Class D Key is encrypted using the Device Key. As this decryption process is always available, irrespective of the state of the device, files protected by this Class Key are accessible always.

Finally, when the device re-enters a locked state, the Class A Key and Class B Private Key are forgotten, protecting that data, leaving the Class C Key and Class B Public Key accessible.

Remote Wipe

Remote Wipe is the ability for a network connected iOS device to have the data within the device made inaccessible (enacted by received system command). This is achieved in iOS by erasing the File System Key, which is used by the device to encrypt all user data (as shown in Figure 2.1). For this reason, once this key is removed, no user data on the device is retrievable.

Hardware Security Module (HSM)

Internal to the device, the HSM is the only means by which iOS can make use of the Device Key. This Device Key is unique to the device and is not exportable using any non-invasive technique.

For this reason (as files encrypted with the Device Key can only be decrypted on the device), the iOS architecture makes itself resistant to off-line attacks. The most significant being a brute-force to exhaust and thus discover the user's Passcode Key. All such brute force attempts rely upon the HSM, are performed on device, and are rate limited.

Note: While the HSM has been evaluated under FIPS-140-2 and an ACE, the secure enclave present in the A7 processor is yet to be evaluated.

Keybags

There are three types of Keybags used in iOS: System, Backup and Escrow.

All Keybags are responsible for storing the systems Class Keys, which are in turn used to gain access to individual files or Keychain entries (as shown in Figure 2.1).

The System Keybag, shown in Figure 2.1, is used internally within the device to facilitate the user's access to the File System and Keychain.

The Backup Keybag is designed to facilitate backups in a secure manner. This is done by transferring the encrypted contents of the File System, and Keychain to a remote system along with the Backup Keybag.

The user then has the option to password protect this Keybag; this decision has implications concerning the portability of the Keybag. If the user specifies a password, the Backup Keybag is then encrypted with this password.

Given the password, this data can then be restored to an iOS device (Note: if a developer has specified data 'ThisDeviceOnly', such data will not be made portable). If, however, the user does not set a password, then the Backup Keybag is protected using the Device Key which never leaves the device. Consequently, the Backup Keybag can only be restored to the original device.

The Escrow Keybag is designed to enable a paired device (normally a computer) to gain full access to the device's file system when the device is in a locked state. In this context pairing refers to connecting the iOS device in an unlocked state (or within 10 seconds of being in an unlocked state) to the other device in question.

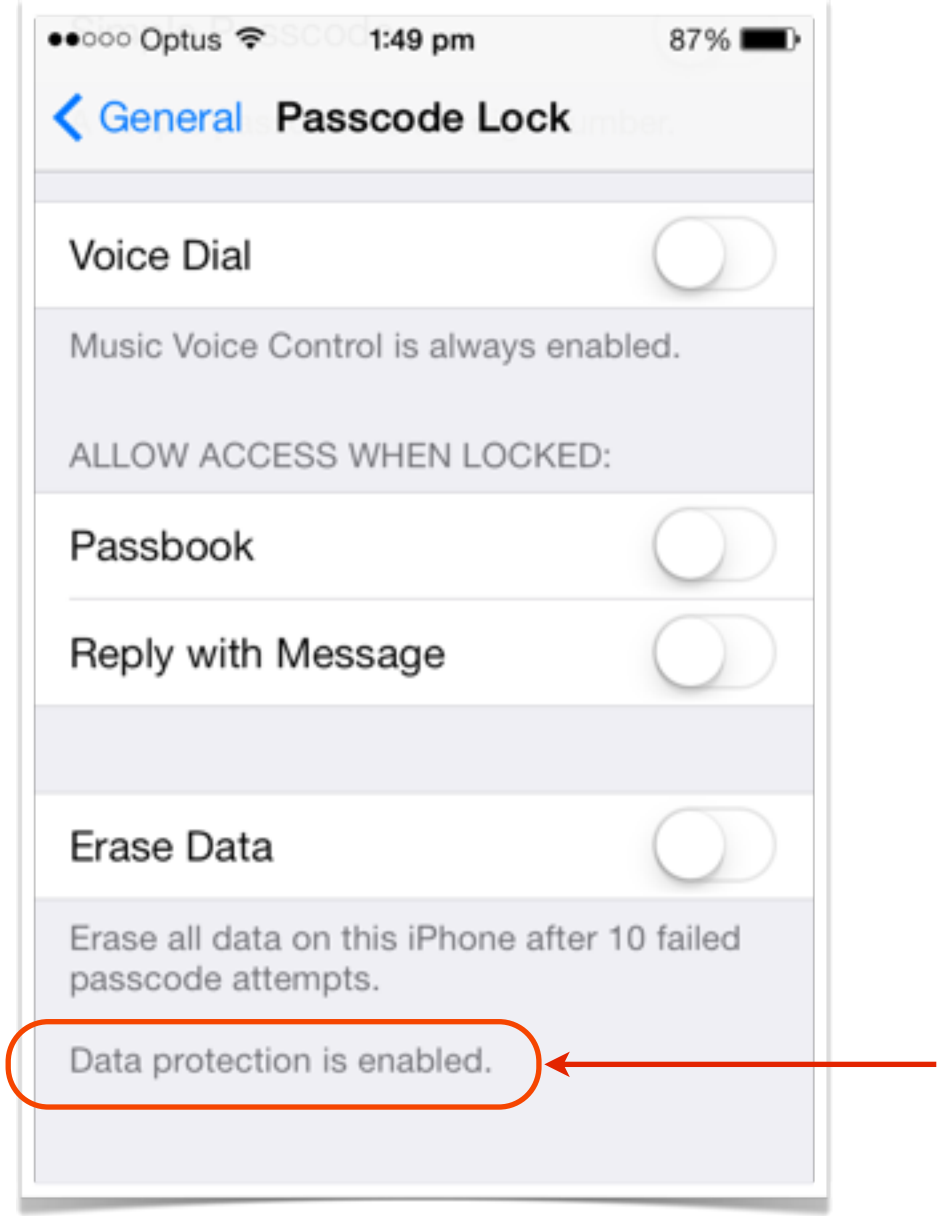
An exchange then occurs, where the paired device receives a copy of the iOS device's Escrow Keybag. This Keybag is encrypted using the iOS device's Device Key, thus restricting access when disconnected from the iOS device.

Setting a Passcode

Setting a passcode is required to enable data protection. In most environments enabling a passcode will form part of agency policy, and this will be enforced either over EAS, or via a Configuration Profile installed on the device. For passcode policies see Suggested Policies in Chapter 6.

Verifying Data Protection is Enabled

There are two main methods of verifying that the file system of a device has been configured to support data protection. An MDM console can query the data protection status and report centrally. The user of a device can also validate if data protection is enabled by navigating to Settings > General > Passcode Lock and scrolling to the bottom of the screen. If data protection is enabled, "Data protection is enabled" will be displayed at the bottom of the screen.



Voice Dial

Music Voice Control is always enabled.

ALLOW ACCESS WHEN LOCKED:

Passbook

Reply with Message

Erase Data

Erase all data on this iPhone after 10 failed passcode attempts.

Data protection is enabled.

Figure 2.2: Data protection enabled

References and Further Reading

For more information on the encryption used in iOS, please refer to the following:

iOS Security October 2014: https://www.apple.com/br/privacy/docs/iOS_Security_Guide_Oct_2014.pdf

"iPhone data protection in depth" by Jean-Baptiste Bedrune and Jean Sigwald from Sogeti

iOS filesystem decryption tools and information from Bedrune and Sigwald: http://code.google.com/p/iphone-dataprotection/

"Apple iOS 4 Security Evaluation" by Dino A. Dai Zovi

Session 709: Protecting Secrets with the Keychain, Apple Developer WWDC 2013 Presentation

Session 208: Securing iOS Applications, Apple Developer WWDC 2011 Presentation

Chapter 4

Deploying iOS Devices

Enrol and sanitise iOS devices using Apple Configurator.

Deploying iOS Devices

iOS has a number of features that are aimed at helping administrators manage iOS devices in large organisations. In most cases, agencies must use a combination of available tools during deployment.

Apple Configurator

Apple Configurator allows administrators to set up and deploy groups of similarly configured iOS devices. Apple Configurator may be suitable for:

- preparing devices for PROTECTED deployments
- preparing devices for MDM enrolment
- activating and naming groups of new devices
- updating iOS on groups of devices
- installing apps and Configuration Profiles on groups of devices
- backing up and restoring devices
- saving and retrieving documents.

It is recommended that administrators use Apple Configurator with an MDM for large deployments of iOS devices.

Supervised Mode

A key feature of Apple Configurator is the ability to place devices into what is called "supervised" mode. Supervised mode modifies standard iOS behaviour in a number of ways. Some of the effects include:

- devices are able to be administered using Configuration Profile restrictions not normally available
- devices are unable to sync music or media from their computer running iTunes to their iOS device
- devices are unable to install apps using iTunes
- devices are unable to backup using iTunes
- increased difficulty in jailbreaking
- in some cases, users not being notified when changes are made to device configuration
- administrative message on lock screen
- Activation Lock disabled for lost or stolen devices
- device data being erased upon initial provisioning.

Though it may not be appropriate to use supervised mode in a BYOD model, there are reasons why supervised mode is desirable for agency owned devices:

- Sensitive data on each device is better protected. Users cannot sync or backup their device contents to their home computer. iOS forensic recovery utilities may not be able to recover data from the device without a jailbreak.

- Users cannot easily sidestep restrictions without erasing the device.
- Supervised mode increases the difficulty of a number of attacks that rely upon the USB host pairing protocol.

Devices not configured as *supervised devices* are referred to as *unsupervised devices*.

Note: PROTECTED devices must use supervised mode.

Supervisory Host Identity Certificate

Normally, an unlocked iOS device is able to pair with any host running iTunes (or supporting the lockdown protocol). When an iOS device is set to supervised mode, it authenticates with a host using the "Supervisory Host Identity Certificate". If the "Allow pairing with non-Configurator hosts" Configuration Profile restriction is disabled, a device will only pair with a host running Apple Configurator with the correct Supervisory Host Identity Certificate. Ordinary pairing with iTunes is not possible with any other hosts. On a Mac host running Apple Configurator, the Supervisory Host Identity Certificate is stored in the login Keychain.

While supervised devices with this restriction are unable to establish new trust relationships with iTunes hosts, a trust relationship will be formed between devices and the Apple Configurator host. A record of this trust relationship is stored in Escrow Keybag files, which on Mac OS X are located at: /var/db/lockdown. It is important to ensure that the Apple Configurator host is regularly backed up, loss of the Supervisory Host Identity Certificate and Escrow Keybag files will mean that supervised devices cannot be administered via the USB interface in the future.

Note: Escrow Keybag files and exported Supervisory Host Identity Certificates should be protected in a similar manner to private keys.

Activating devices with Apple Configurator

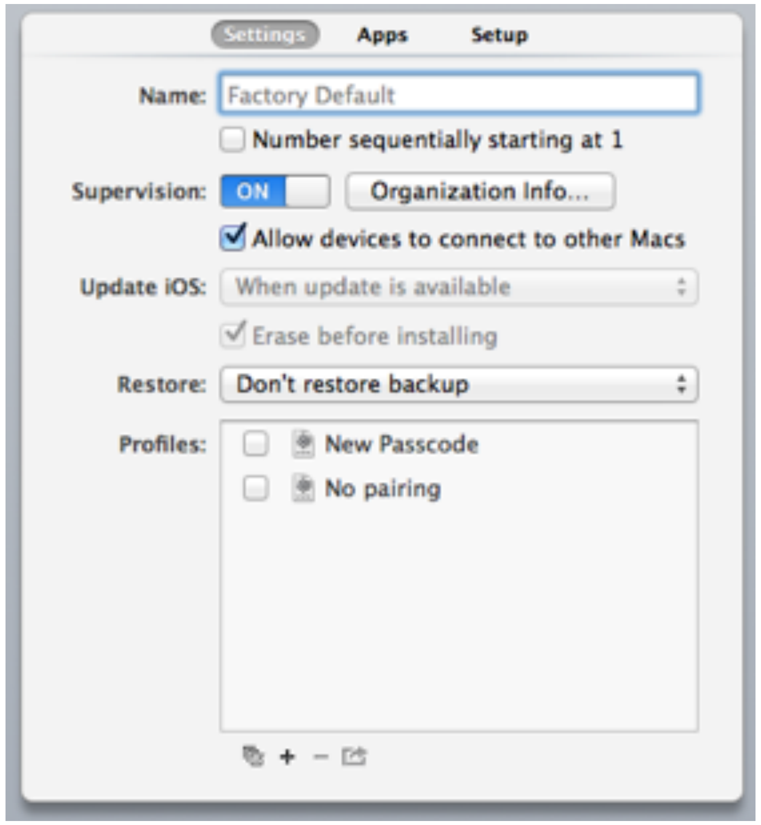
Apple Configurator will attempt to automatically activate all connected devices after operating system installation. It is important for administrators to note that iPhones and iPads require a SIM for activation. If the SIM has a passcode lock, automatic activation will be unsuccessful.

Installing iOS

A key feature of Apple Configurator is its ability to install iOS on many devices concurrently. Additionally, varied device platforms (iPhone, iPad, iPod) can all be simultaneously connected. Apple Configurator will seamlessly download iOS for all supported device platforms when there is an internet connection available. A theoretical maximum of 64 devices can be connected concurrently for installation.

Installing Configuration Profiles

Apple Configurator may be used both to install Configuration Profiles and to create new Configuration Profiles. These profiles can be installed on devices in bulk when initially preparing devices for deployment. As an example, this may be used to initially roll out a trust profile for an agency MDM server.



Name: Factory Default

☐ Number sequentially starting at 1

Supervision: ON

☑ Allow devices to connect to other Macs

Update iOS: When update is available

☑ Erase before installing

Restore: Don't restore backup

Profiles:
☐ New Passcode
☐ No pairing

Figure 4.1 Installing Configuration Profiles with Apple Configurator

iOS Updates

There are two methods for Apple Configurator deployed devices to receive iOS updates. Devices with an internet connection will prompt users to install Over-The-Air updates. Alternatively, users can return their devices to their administrator to have them updated using Apple Configurator.

References and Further Reading

Refer to the following publication for additional information on Apple Configurator:

http://help.apple.com/configurator/mac/

Device Enrolment Program

Recently made available in Australia, the Device Enrolment Program (DEP) is a deployment feature which allows organisations to pre-configure iOS devices, allowing these devices to be delivered directly to the user.

Devices can be preset to supervised mode and can be preconfigured for an organisation's MDM system. There are numerous benefits for administrators in deploying a fleet using DEP:

- save time deploying by not having to physically connect devices to host running Apple Configurator
- no need to use Apple Configurator to re-provision device after device wiped
- lost/stolen devices may be recovered or rendered useless

ASD's testing of DEP is currently incomplete. Agencies should make a risk determination on the use of this feature which at minimum must consider the possibility of an adversary taking control of the Apple ID used to administer DEP.

Device Sanitisation

Administrators should erase and re-provision devices for the following reasons:

1. to sanitise a returned iOS device for re-issue
2. to sanitise an employee owned iOS device before provisioning
3. to sanitise a deployed employee owned iOS device prior to the employee leaving
4. to break all device-to-host trust relationships and invalidate old Escrow Keybag files.

Activation Lock

Activation Lock is a feature which requires Apple ID user authentication before device activation. Typically Activation Lock is enabled if a user enables iCloud > Find my iPhone in the Settings app on an unsupervised device.

If a user has enabled Activation Lock on an iOS device, that user’s Apple ID will be required to activate the iOS device after (or during) sanitisation.

Breaking The Device-to-host Trust Relationship

When an iOS device pairs with a host, a trust relationship is formed. In many cases an administrator may want to erase an iOS device and break all the established host trust relationships that a device has previously created. The most reliable method to break all established relationships is to restore the iOS device firmware using what is commonly known as “Device Firmware Upgrade” mode (DFU mode).

Note: Restoring a device in this way will also erase all data and settings on the device.

The DFU mode restoration can be performed from a host that has no established trust relationship with the device, and the device passcode is not required.

DFU Mode Restoration

To perform an iOS firmware restoration follow this procedure:

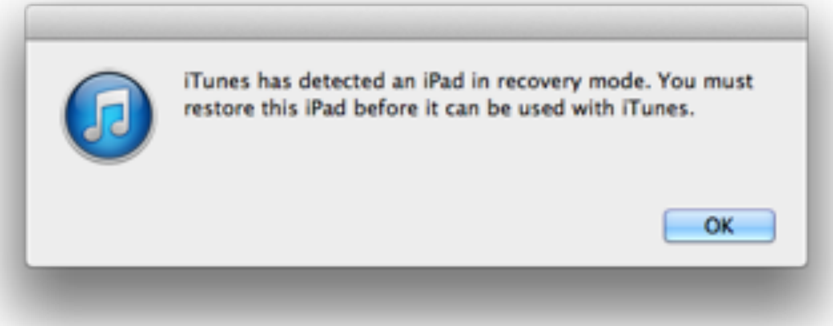
1. Connect the iOS device to the host PC or Mac running iTunes

2. If iTunes is unable to pair with the iOS device, please clear any error dialog boxes

3. Press and hold both the Sleep/Wake and Home buttons on the iOS device for ten seconds

4. Release the Sleep/Wake button, and continue to hold the home button

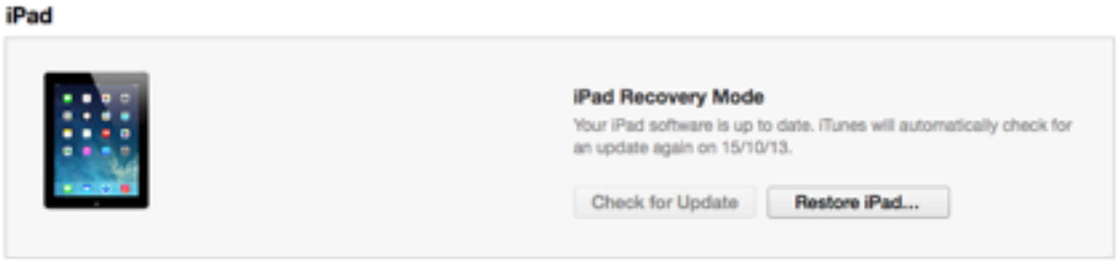
5. Release the home button after iTunes generates the following dialog box:



iTunes has detected an iPad in recovery mode. You must restore this iPad before it can be used with iTunes.

Figure 4.2: iTunes detects device in recovery mode.

6. After clicking OK, click the Restore button.



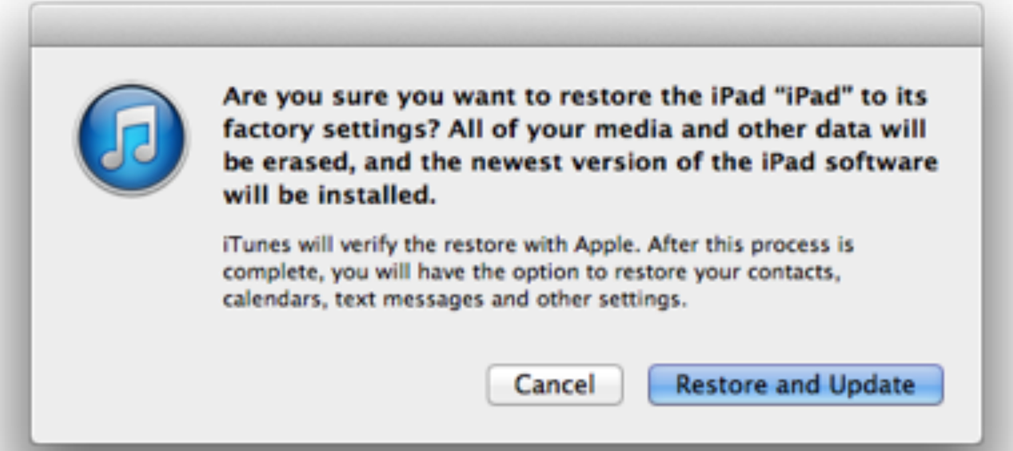
iPad

iPad Recovery Mode

Your iPad software is up to date. iTunes will automatically check for an update again on 15/10/13.

Figure 4.3: Restore iPad.

7. Begin the iOS restoration process by clicking Restore and Update.



Are you sure you want to restore the iPad “iPad” to its factory settings? All of your media and other data will be erased, and the newest version of the iPad software will be installed.

iTunes will verify the restore with Apple. After this process is complete, you will have the option to restore your contacts, calendars, text messages and other settings.

Figure 4.4: Restore and Update.

Sanitising an iOS Device For Re-issue

If an agency owned device is returned for re-issue to another employee, it should be erased by performing a DFU mode restoration. One reason that this is important is so that the previous iOS device owner cannot take advantage of any old device-host trust relationships to retrieve data from the device.

By performing the DFU mode restoration the old trust relationships are broken.

Before an iOS device is re-provisioned for enterprise use, it is recommended to perform a DFU mode restoration. This will ensure that the device is in a known state.

Sanitising Employee Owned iOS Devices

Employee owned iOS devices are making their way into government agencies, creating a new set of challenges for administrators. Some of the challenges being faced include:

- jailbroken devices running untrusted code
- jailbroken devices being able to bypass all security protection (including 3rd party managed containers)
- unpatched iOS devices that are vulnerable to exploitation
- devices previously configured with conflicting settings and/or Configuration Profiles.

Older Versions of iOS

Each revision of iOS includes many security related fixes. If left unpatched, iOS devices could be exploited remotely, risking both employees' personal information and the security of the corporate network.

The agency acceptable use policy should require users to install iOS updates as they become available.

Jailbroken Employee Owned Devices

Jailbroken devices allow users to install applications on their iOS devices from outside of Apple's App Store. Though there are many useful legal purposes for jailbreaking a device, jailbreaking carries with it a number of negative side effects that impact the security of the corporate network and the confidentiality of data stored on a device:

- Jailbreaking usually disables application code signing checks. These iOS code signing checks help to prevent malware executing on a device. Removing this makes exploitation easier.
- Jailbreaking may disable or break important security features such as Address Space Layout Randomisation (ASLR) and application sandboxing. ASLR increases the difficulty of successful exploitation of vulnerability. Malware on a jailbroken device would not be constrained by the application sandbox.
- Jailbroken devices often have serious unpatched operating system vulnerabilities and are more vulnerable to exploitation.
- Publicly available jailbreaks may contain malware.
- Jailbroken devices should be assumed to be untrusted.

Jailbroken devices are also often able to enrol into market leading MDM systems without detection. Indeed, there are applications that have been written with the purpose of evading MDM agent jailbreak detection. When this occurs, administrators can not have confidence that Configuration

Profile restrictions and settings are enforced by the operating system.

Information about a commonly used jailbreak detection bypass utility is available at:

http://theiphonewiki.com/wiki/XCon

Administrators should not allow employee owned jailbroken iOS devices to be provisioned on the corporate network.

For all the above reasons it is important to ensure that devices are sanitised prior to deployment.

Sanitisation Prior To Deployment

When considering how to sanitise employee owned iOS devices for enterprise deployment, it is important to take into account the data that employees already have on their devices. Employees may have expectations about how they will be able to use their devices and the effect of enterprise deployment on their device. As an example, an employee might expect their iPhone's contact list to be preserved after deployment. If the device is erased using DFU mode this will not be the case.

If an employee's personal data is to be preserved, the following procedure may be performed prior to enterprise deployment:

1. Take a backup of the device
2. Perform DFU mode restore
3. Restore a backup to the device
4. Delete backup from the host
5. Provision and deploy the device as per MDM instructions.

This will clear the existing host trust relationships on the device, but will preserve the employee's data. When following this procedure agencies must consider their legal responsibilities to protect the privacy of their users' data.

If there is no need to preserve an employee's personal data on a device, agencies should simply perform a DFU mode restore.

Sanitisation For Departing Employees

When an employee departs an agency or no longer requires iOS device connection to the agency network, it is important to remove existing host trust relationships from the employee's iOS device. On return, agency owned devices should be sanitised by performing a DFU mode restore as described previously. Employees should be made aware that agency owned devices will be sanitised upon return.

In a BYOD model, the following procedure is suggested for departing employees:

1. Remove MDM profile from the iOS device, which will:
    - remove the corporate mail account installed by the MDM
    - remove any apps which have been installed by the MDM which will also remove any associated data
2. Take a backup of the device
3. Perform DFU mode restore

4. Restore backup to the device

5. Erase backup files from the host

6. If the user's Apple ID is associated with a corporate SIM/ phone number, it is also necessary to de-register iMessage (https://selfsolve.apple.com/deregister-imessage).

This procedure will also remove any trust relationships established between the iOS device and any trusted host computers. If the employee does not return their iOS device prior to departing, it may be necessary to use the MDM remote wipe function. Employees should be made aware of this fact in an agency acceptable use policy.

Removing Trust Relationships

It is possible to remove only the host pairing relationships from a device without performing a complete device erase. This can be accomplished by a device user performing the following procedure:

1. Open the Settings app

2. Select "General" and then "Reset"

3. Select either:

   A. "Reset Location & Privacy" which will also restore all privacy settings to factory default, or

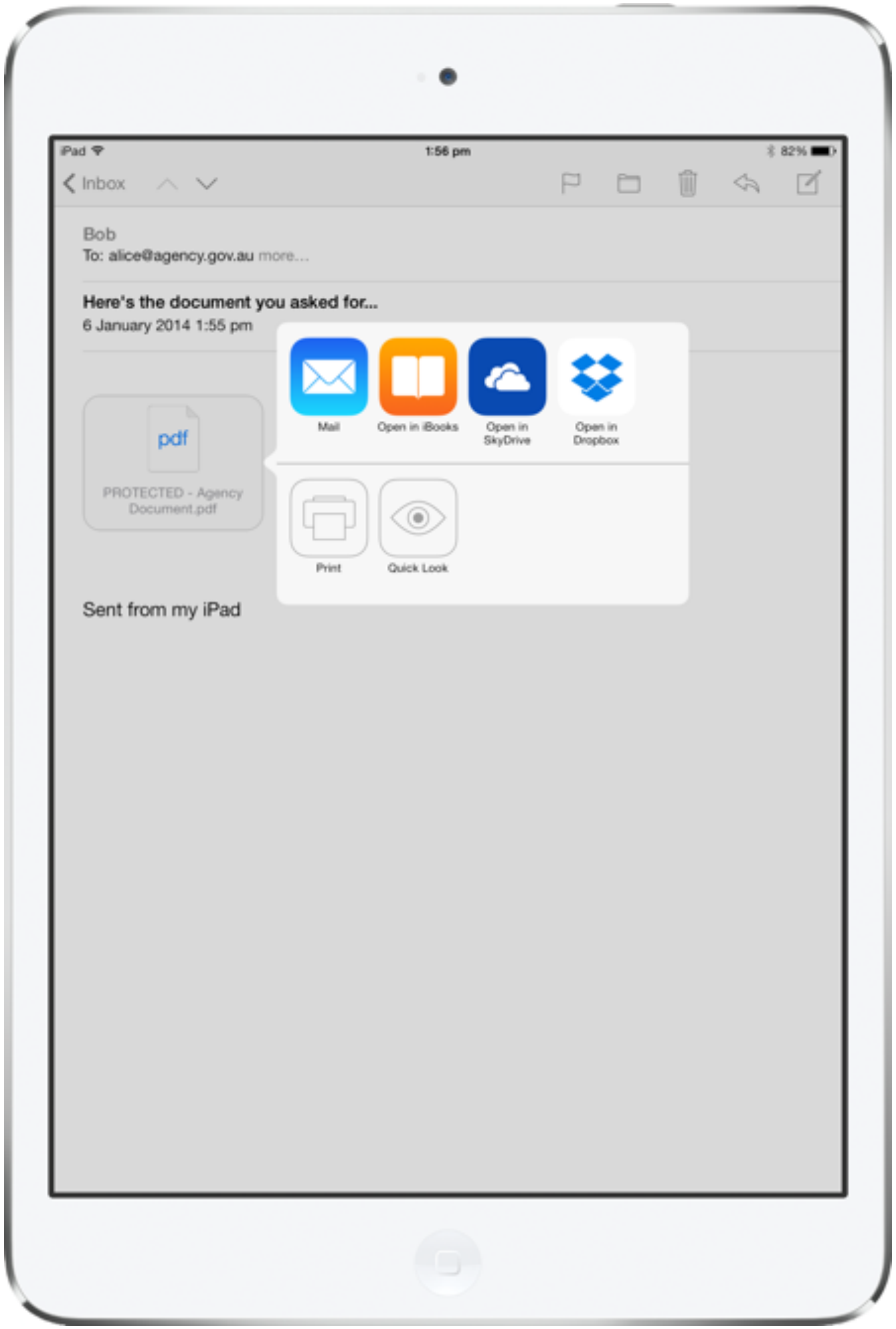
   B. "Reset Network Settings" which will also remove Wi-Fi networks and passwords, Bluetooth pairing records, VPN settings and APN settings.

For more information on this process refer to:

https://support.apple.com/kb/HT5868

CHAPTER 5

Managing Apps and Data



Bob

To: alice@agency.gov.au more…

Here's the document you asked for...

6 January 2014 1:55 pm

PROTECTED - Agency Document.pdf

Sent from my iPad

Understand and mitigate the risks posed by installing third party apps.

Managing apps and Data

Installing iOS apps can expand the attack surface of an iOS device and increase the probability of a leak of sensitive data. This chapter aims to explain the risks and provide mitigations.

Security Scenarios

Devices running iOS share many of the same security weaknesses of PCs while at the same time presenting some new challenges. Presented below are a few common scenarios that may lead to a leak of sensitive data.

Lost or stolen device

Due to the portable nature of iOS devices, there is always a chance that a deployed agency device will one day be lost or stolen.

In many situations remote wipe may not be the most desirable option, in some situations it will be impossible. In these situations, adequate data at rest protection is vital. When an iOS device is configured following the recommendations given in this guide, data at rest protection depends upon how third party app developers have implemented iOS data protection for files and if they have made correct use of the Keychain for credentials.

If we make the following assumptions about a hypothetical example:

- an iOS device is able to be jailbroken
- has data protection enabled with alphanumeric passcode
- has not been put in to supervised mode
- has 3rd party apps installed
- has been lost or stolen.

If a third party app developer used Class D (*NSFileProtectionNone)* data protection class, files within this app's sandbox could be recovered using free or commercial data recovery tools. As an example, if an instant messaging client did not utilise data protection appropriately, chat logs and received files may be recoverable. If the developer stored credentials in the file system rather than using the Keychain, this could mean that the username and password for this instant messaging service may also be recoverable.

Even when data protection and the Keychain are used in an app, they can easily be implemented incorrectly. For example:

- some files may have an inappropriate data protection class
- existing files from an older version of the app have not had their protection class upgraded
- an incorrect Keychain or data protection class may have been used.

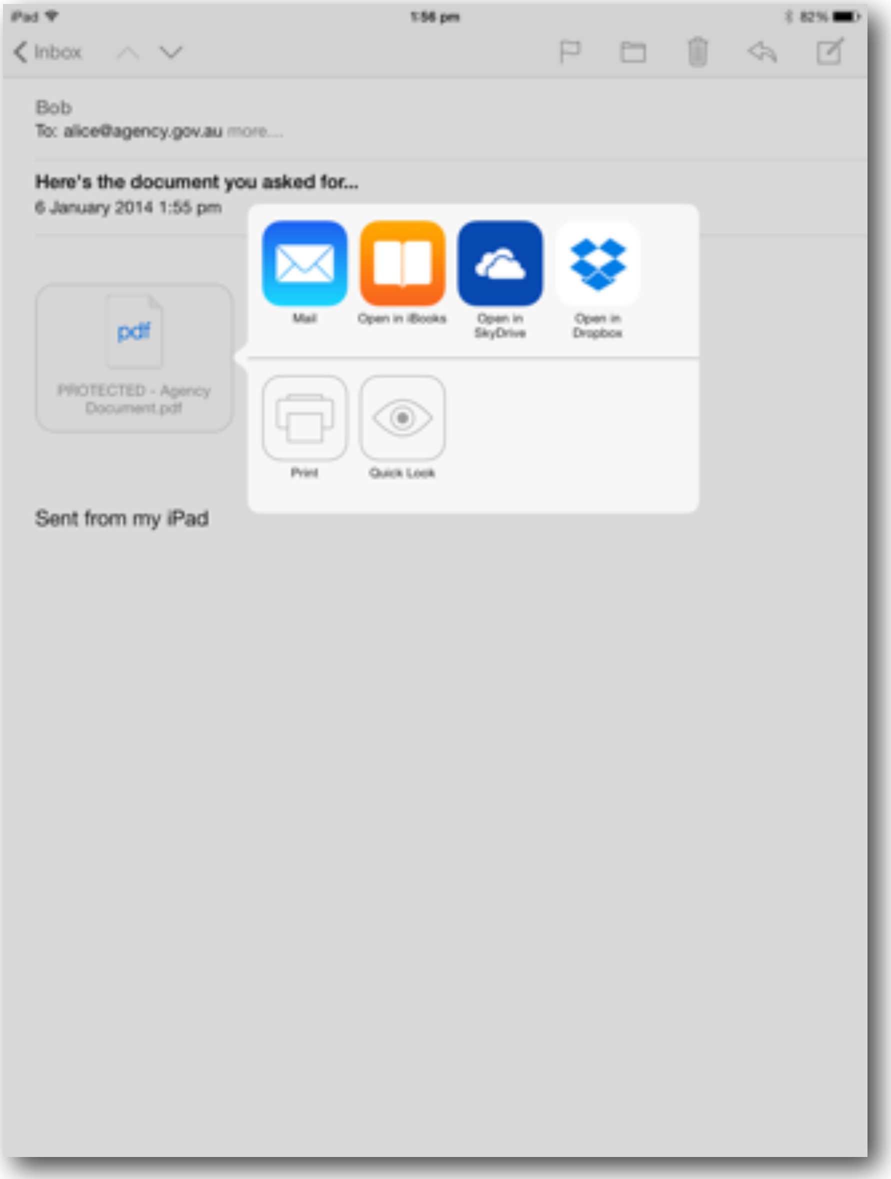
Sensitive information leak

There are a few common ways which apps may leak sensitive information. Apps may:

- allow a file to be opened in another app with inappropriate data protection
- transmit sensitive information over a network with inadequate encryption
- as part of normal app behaviour, transmit sensitive information over a network to external servers.

In the first case, a good example of an app that shows this behaviour is the iOS Mail app. Using Mail, it is possible to open an attachment in another app. For example, an attached PDF file may be opened in the iBooks app. If more than one app has registered a particular file type, Mail will allow the user to choose which app they would like to open the file in. Since the Dropbox app also registers itself as being able to open PDF files, if the user has both iBooks and Dropbox installed mail will allow a user to open a PDF document in their chosen app, as shown in Figure 5.1.

Although Mail has been approved by ASD for use up to PROTECTED, if a user chooses to open an attachment in another app it may not be subject to adequate data protection. Additionally, many apps (including iBooks and Dropbox) may sync files and metadata to a server on the Internet.



Bob
To: alice@agency.gov.au more...

Here's the document you asked for...
6 January 2014 1:55 pm

PROTECTED - Agency Document.pdf

Sent from my iPad

Figure 5.1: Mail app Open-In

Many iOS apps transmit information to other devices on a network or on the Internet. Often the information transmitted is not sensitive; however there have been incidents where private or sensitive data has been transmitted over the Internet without encryption. For baseline Government systems, the ISM (Control 1162) specifies that: “Agencies must use an encryption product that implements an AACP if they wish to communicate sensitive information over public network infrastructure.” For

PROTECTED systems, the ISM (control 0465) specifies that: “Agencies must use a Common Criteria-evaluated encryption product that has completed an ACE if they wish to communicate classified information over public network infrastructure.”

Where agencies are utilising On Demand VPN, it is possible that a user may deliberately or accidentally disable the VPN tunnel. In this case, your data’s transport security is limited to whatever scheme the app developer has implemented.

Lastly, there are risks which cannot be mitigated via iOS technical controls alone:

- copy/pasting sensitive data
- printing sensitive data to the wrong printer
- photographing the screen of the device.

Policy and user education can partially mitigate the case where any of the above events occur accidentally. Deliberate misuse of copy/paste and printing can be managed using a combination of careful custom app development, negotiation with App Store app developers and in some cases, modification of existing apps using 3rd party add ons.

Copy/paste can be managed through careful app development using named pasteboards. Likewise, the risk of a user printing sensitive data to the wrong printer can be managed when developing custom apps. Some commercial software vendors offer an “App Wrapping” solution which can be used to alter copy/paste and print behaviour of existing non App Store apps.

Exploitable Code Errors

Most apps contain software bugs, some of which can be exploited. Some bugs can be exploited in a way that allows code execution; others may cause the app to operate in a way other than it was intended.

Some common types of vulnerabilities that may be exploited in iOS apps are:

- buffer overflows
- uncontrolled format strings
- use after free
- SQL injection.

Apple has implemented a number of anti-exploitation mitigations in iOS that make successful exploitation of the above vulnerabilities more difficult. However, it is still important for in-house app developers to understand the types of coding errors that can lead to an exploitable vulnerability, and that operating system generic exploit mitigations do not provide complete protection for exploitable apps.

Developers should refer to the following resources for more information:

iOS Security Starting Point

https://developer.apple.com/library/ios/referencelibrary/GettingStarted/GS_Security_iPhone/index.html

Apple Secure Coding Guide

https://developer.apple.com/library/ios/documentation/Security/Conceptual/SecureCodingGuide/

iOS Developer Library Security Topic

https://developer.apple.com/library/ios/navigation/#section=Frameworks&topic=Security

Mitigations

Though it is not possible to fully mitigate all the risks mentioned, it is possible to substantially reduce their likelihood. This is done by:

- ensuring apps that handle sensitive data utilise appropriate iOS data protection classes
- configuring agency devices to disallow host pairing
- restricting Open-In behaviour between managed and unmanaged apps
- ensuring that agency deployed managed apps are assessed for weaknesses before deployment.

Though the following guidelines specifically address apps, they must equally be applied to app extensions.

Data Protection

If an app is required to write files containing PROTECTED data on a locked device from the background, such files should be protected using Class B *NSFileProtectionCompleteUnlessOpen*, otherwise:

All files that contain PROTECTED data, created or referenced by an app must be protected using Class A *NSFileProtectionComplete*.

Keychain

If the app requires access to credentials on a locked device from the background, such credentials should be protected using the *…AfterFirstUnlock* or *…AfterFirstUnlockThisDeviceOnly* Keychain classes, otherwise:

Credentials must be protected using the *…WhenUnlocked* or *…WhenUnlockedThisDeviceOnly* Keychain classes.

Questions to ask app developers

By asking the following questions, administrators put themselves in a good position to properly evaluate the risks associated with installing a particular iOS app:

1. What is the flow of data throughout the application; source, storage, processing and transmission?
2. Which data protection classes are used to store data?
3. When data is transmitted or received, is it done through a secure means? Is Secure Transport used? If not why not?
4. What system or user credentials are being stored? Are they stored using the Keychain Class A? If not why not?
5. Are any URL Schemes or UTIs handled or declared?
6. Is the app compiled as a position independent executable (PIE)?
7. Is iCloud, or other "Cloud" functionality used?

Note: For further information about iOS app assessment please refer to the iOS App Assessment Guide published on OnSecure (https://www.onsecure.gov.au). This guide is also available on request.

Managed Open-In

Despite best efforts to ensure that agency apps protect data appropriately, having a single poorly designed app with registered document types can compromise the security of all the data on the device.

iOS features a pair of restrictions that help organisations control this risk:

- "Allow documents from managed sources in unmanaged destinations"
- "Allow documents from unmanaged sources in managed destinations"

These restrictions can be used to control Open-In behaviour.

In a deployment where:

- agency apps are deployed by the MDM as *Managed apps; and*
- classified files are only able to be accessed by the *Managed apps*

Disabling the Managed to Unmanaged Open-In behaviour can be used to mitigate the risk posed by users moving classified documents in to their own unmanaged apps.

Important: Agencies may allow unmanaged user app installation on PROTECTED iOS deployments if the *"Allow documents from managed sources in unmanaged destinations"* restriction is disabled.

Allowing unmanaged user app installation carries with it the following risks:

1. Improper utilisation of unmanaged apps for sensitive work

   This sensitive data may be recoverable if the data was not stored in an appropriate data protection class if the device was lost or stolen. There is also the possibility that such data may be transmitted over the network with or without transport security to an uncontrolled end point.

2. Device exploitation via hostile App Store app

   An App Store app may have hidden functionality designed to gather and transmit personal or sensitive data to a third party. It is also possible for an App Store app to maliciously execute code which is designed to exploit operating system vulnerabilities. Both risks are significantly mitigated by the relatively hardened iOS runtime environment, and by a lesser extent, Apple's App Store review process.

CHAPTER 6

Suggested Policies

●●○○○ Telstra 2:38 pm 61%
Touch ID

Complete

Touch ID is ready. Your print can be used for unlocking your iPhone.

Continue
●●○○○ Telstra 10:42 am 36%
Messages
Tuesday 7
Calendar
Photos
Camera
1:45:00
-4:15
Show 43 - Wrath of the Khans I
Dan Carlin's Hardcore History
AirDrop
AirPlay

Our suggested policies for iOS devices used by Australian government agencies.

Suggested Policies

This chapter lists suggested policies in graduated levels of response, applied to iOS devices at varying security classifications. The agency's Information Technology Security Advisor should be consulted for the specific usage scenarios for a deployment.

If iOS devices are being considered for use at classifications above PROTECTED, agencies must undertake a risk assessment following the guidance in the ISM as well as their own agency security policies and determine mitigation procedures and policy. Agencies must also obtain appropriate approval for any non-compliance in accordance with the ISM.

Feature	Unclassified	Unclassified (DLM)	Protected
Device selection	Agency’s decision	A5 processor or later	A5 processor or later
BYOD (Bring Your Own Device)	Agency’s decision	May be possible (MDM opt-in for AUP agreement and enforcement recommended). See ISM section on Mobile Devices	May be possible (MDM opt-in for AUP agreement and enforcement recommended). See ISM section on Mobile Devices
Passcode/TouchID	Must use passcode or TouchID	Must use passcode or TouchID	Must use passcode
Apple ID	Personal or Agency	Personal or Agency	Personal or Agency
Home Computer backup enforcement	Stated in agency usage policy	Stated in agency usage policy	Must use Supervised mode and prevent host pairing
iCloud	Agencies need to assess the risk in their own situation	Agencies need to assess the risk in their own situation	No syncing documents and data, no Backup, no iCloud Keychain. iTunes Purchases and iTunes Match at Agency discretion.
Email	Third party email apps which utilise native data protection and transport security may be used. Recommend use of native mail app	Third party email apps which utilise iOS native data protection and transport security may be used. Recommend use of native mail app. Exchange with certificate authentication	Third party email apps must meet Chapter 5 data protection/keychain app requirements.Recommend use of native mail app. Must use Exchange with certificate authentication and should use TLS 1.2 for transport security
MDM	Optional depending on role of device/scale of deployment	Optional depending on role of device or scale of deployment, recommended for BYOD model	Recommended

Table 6.1: Suggested policies

Feature	Unclassified	Unclassified (DLM)	PROTECTED
VPN-on-Demand	Optional depending on role	Recommended	Required, if not using Per App VPN or VPN “Always-On”
Per App VPN	Optional depending on role	Recommended	Required, if not using VPN On-Demand or VPN “Always-On”
Secure browser	Optional	Optional	Recommended
Configuration Profiles	Should be cryptographically signed	Should be cryptographically signed	Must be cryptographically signed
User installation of App Store apps	Agency’s decision, recommend use of Managed Open-In	Agency’s decision, recommend use of Managed Open-In	Possible, must use Managed Open-In restriction to prevent managed to unmanaged app document transfer
AirDrop	Agency’s decision	Agency’s decision	Agency should disable use of AirDrop through Configuration Profile restriction
AirPlay	AirPlay receiver should require passcode authentication	AirPlay receiver should require passcode authentication	AirPlay receiver should require passcode authentication
Enterprise SSO	Agency’s decision	Agency’s decision	Recommend use of enterprise apps which support this feature
Handoff	Agency’s decision	Agency’s Decision	Agency should disable Handoff through Configuration Profile Restriction

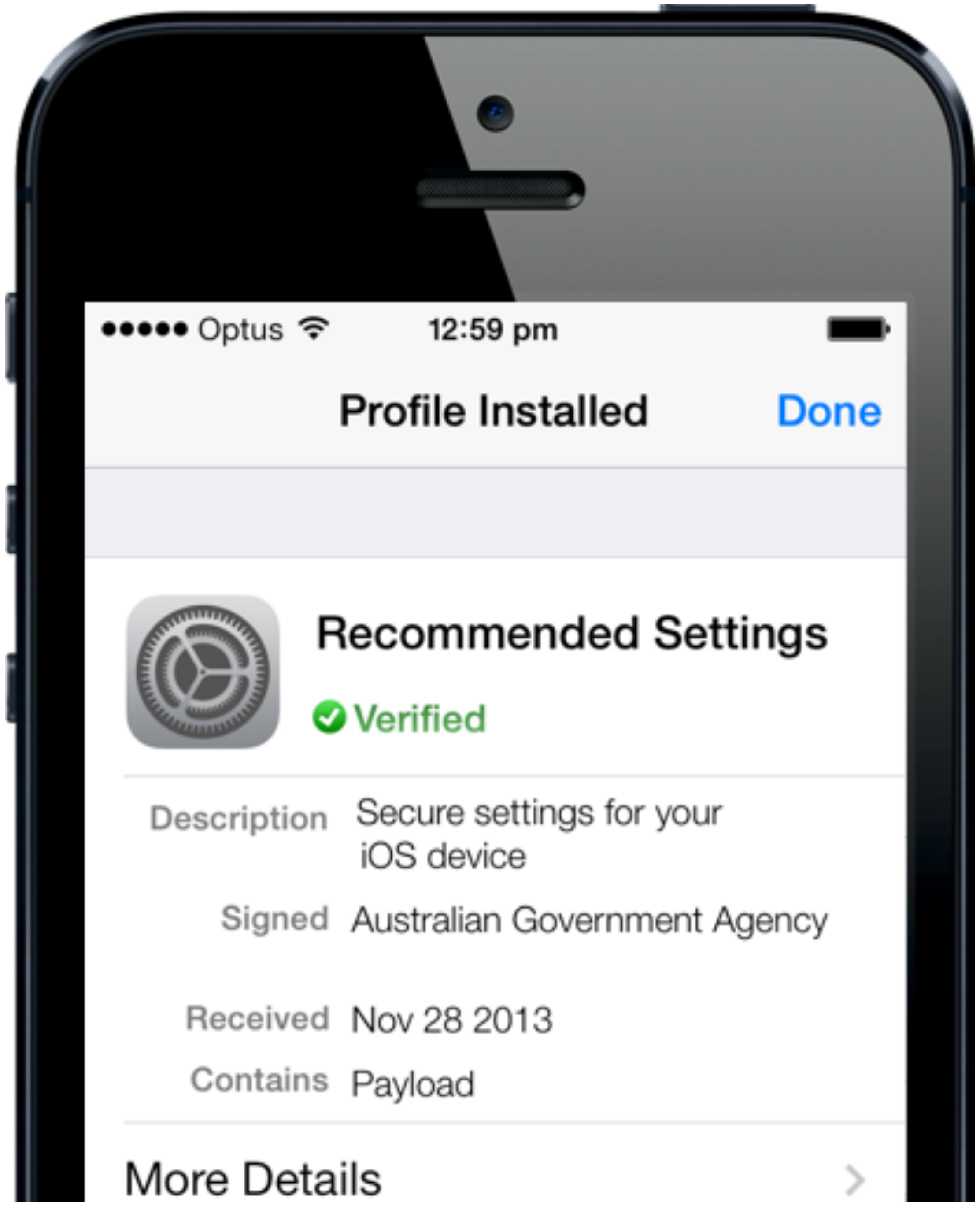
Table 6.1 (continued): Suggested policies

Feature	Unclassified	Unclassified (DLM)	PROTECTED
Extensions	Agency's decision, recommend use of Managed Open-In	Agency's decision, recommend use of Managed Open-In	Possible, must use Managed Open-In restrictions to maintain managed/unmanaged container separation. Extensions processing PROTECTED data are required to comply with the same guidelines as apps.
User storage of Home/Health data on device	Stated in agency usage policy	Stated in agency usage policy	Recommend disallowing storage of personal Home/Health data, stated in agency usage policy
iCloud Drive	Agencies need to assess the risk in their own situation	Agencies need to assess the risk in their own situation	Disabled
Managed documents in iCloud	Agency’s decision	Agency’s decision	Disabled
VPN “Always-On”	Optional depending on role	Recommended	Required if not using VPN On-Demand or Per-App VPN
Touch-ID for in-house App authentication	Recommended in addition to existing passcode policy	Recommended in addition to existing passcode policy	Recommended in addition to existing passcode policy
Voice and SMS	Unclassified only	Unclassified only	Unclassified only
SIM PIN	Recommended	Recommended	Recommended
Bluetooth	Disabled, unless required for specific business purpose.	Disabled, unless required for specific business purpose.	Disabled, unless required for specific business purpose.

Table 6.1 (continued): Suggested policies

CHAPTER 7

Recommended Device Profile Settings



Recommended Settings

✓ Verified

Description	Secure settings for your iOS device
Signed	Australian Government Agency
Received	Nov 28 2013
Contains	Payload

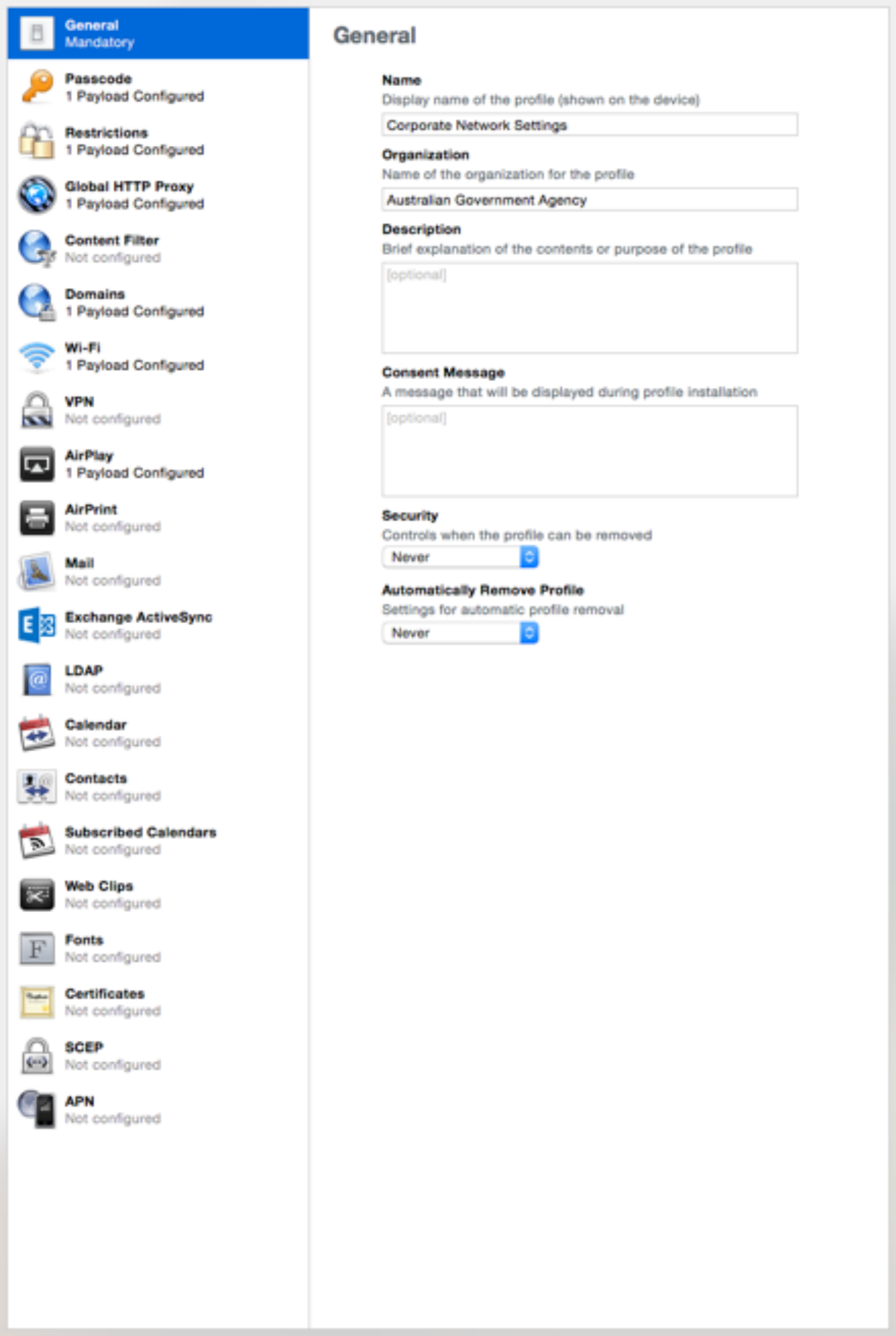
The profile settings that should typically be used when an iOS device is used on an Australian government network.

Recommended Device Profile Settings

The following settings are a baseline for use on PROTECTED networks. Agency discretion can be applied to be more restrictive to suit special requirements, or lowered at lower classifications in accordance with ISM policy. Where a profile setting is not discussed below, agencies should examine their own particular technical and policy needs. Apple Configurator can be used to view the full range of profile settings that can be deployed.

Profiles should be pushed to the device with restrictions and resources bundled. So if the profile is removed by a user, all access to agency resources is removed.

Pre-loaded Configuration Profiles and MDM managed profiles can be mixed on devices. In this case the MDM server cannot remove the pre-loaded profiles manually installed on the device.



General

Name
Display name of the profile (shown on the device)
Corporate Network Settings

Organization
Name of the organization for the profile
Australian Government Agency

Description
Brief explanation of the contents or purpose of the profile
[optional]

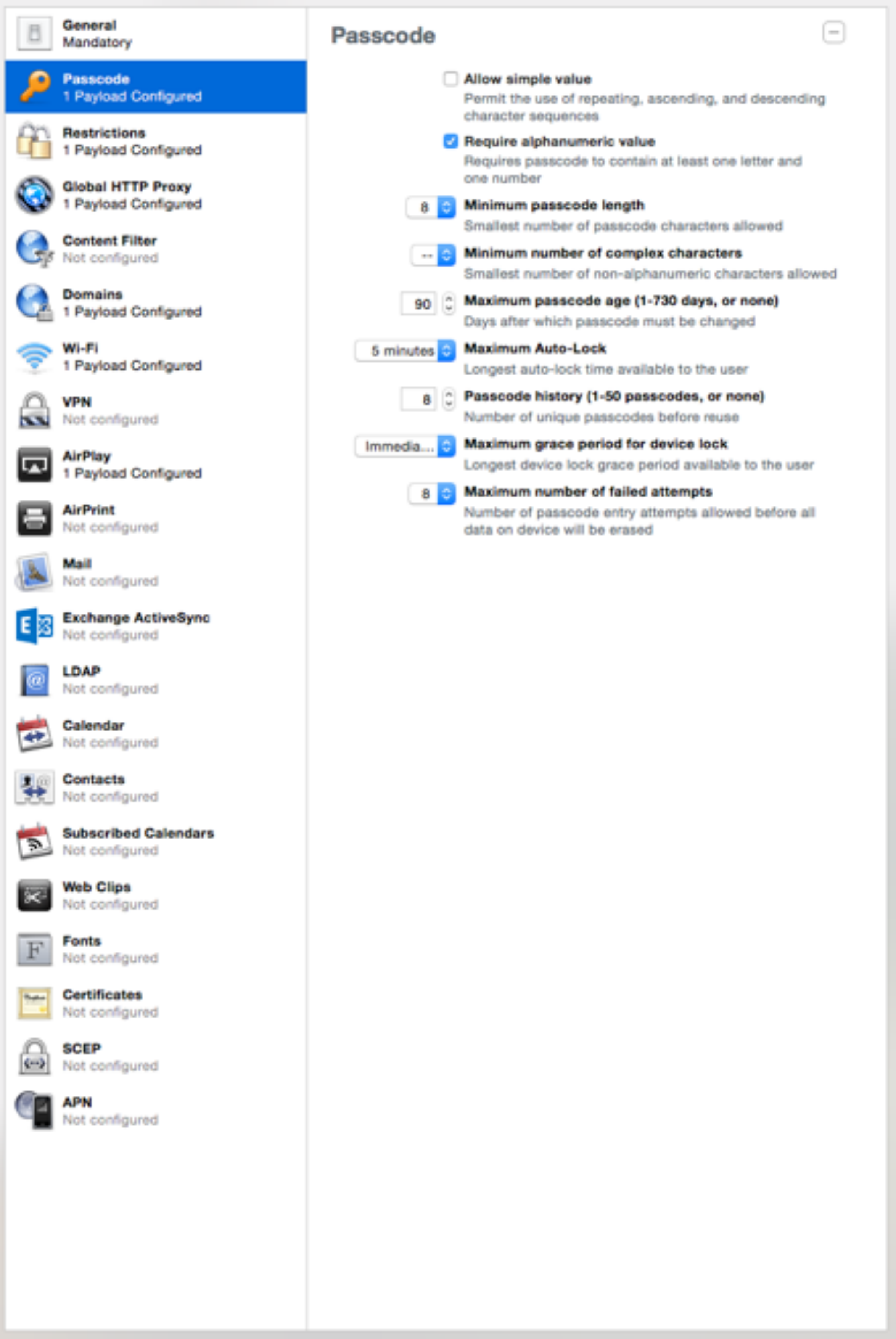
Consent Message
A message that will be displayed during profile installation
[optional]

Security
Controls when the profile can be removed
Never

Automatically Remove Profile
Settings for automatic profile removal
Never

General Settings

Setting	Recommendation
Security	• Profile Security should be set to “Always” if setting is for the convenience of users accessing non-sensitive data (e.g. a subscribed calendar of Australian public holidays). Opt-In MDM profiles would usually fit into this category as well. • Profile security should be set to “With Authorization” for profiles that IT staff can remove temporarily. Generally users would not receive the passcode to such profiles. • Most profiles that are not MDM managed should be set to “Never”. The passcode policy profile, if used, should be set to “Never”.
Automatically Remove Profile	Configuration Profiles can be set for automatic removal on a specific date or after a defined interval. This function can be used at agency discretion, typical use cases include: • Guest user profile • Temporary profile for overseas travel



General
Mandatory

Passcode
1 Payload Configured

Restrictions
1 Payload Configured

Global HTTP Proxy
1 Payload Configured

Content Filter
Not configured

Domains
1 Payload Configured

Wi-Fi
1 Payload Configured

VPN
Not configured

AirPlay
1 Payload Configured

AirPrint
Not configured

Mail
Not configured

Exchange ActiveSync
Not configured

LDAP
Not configured

Calendar
Not configured

Contacts
Not configured

Subscribed Calendars
Not configured

Web Clips
Not configured

Fonts
Not configured

Certificates
Not configured

SCEP
Not configured

APN
Not configured

Passcode

□ **Allow simple value**
Permit the use of repeating, ascending, and descending character sequences

☑ **Require alphanumeric value**
Requires passcode to contain at least one letter and one number

8 **Minimum passcode length**
Smallest number of passcode characters allowed

-- **Minimum number of complex characters**
Smallest number of non-alphanumeric characters allowed

90 **Maximum passcode age (1-730 days, or none)**
Days after which passcode must be changed

5 minutes **Maximum Auto-Lock**
Longest auto-lock time available to the user

8 **Passcode history (1-50 passcodes, or none)**
Number of unique passcodes before reuse

Immedia... **Maximum grace period for device lock**
Longest device lock grace period available to the user

8 **Maximum number of failed attempts**
Number of passcode entry attempts allowed before all data on device will be erased

Passcode

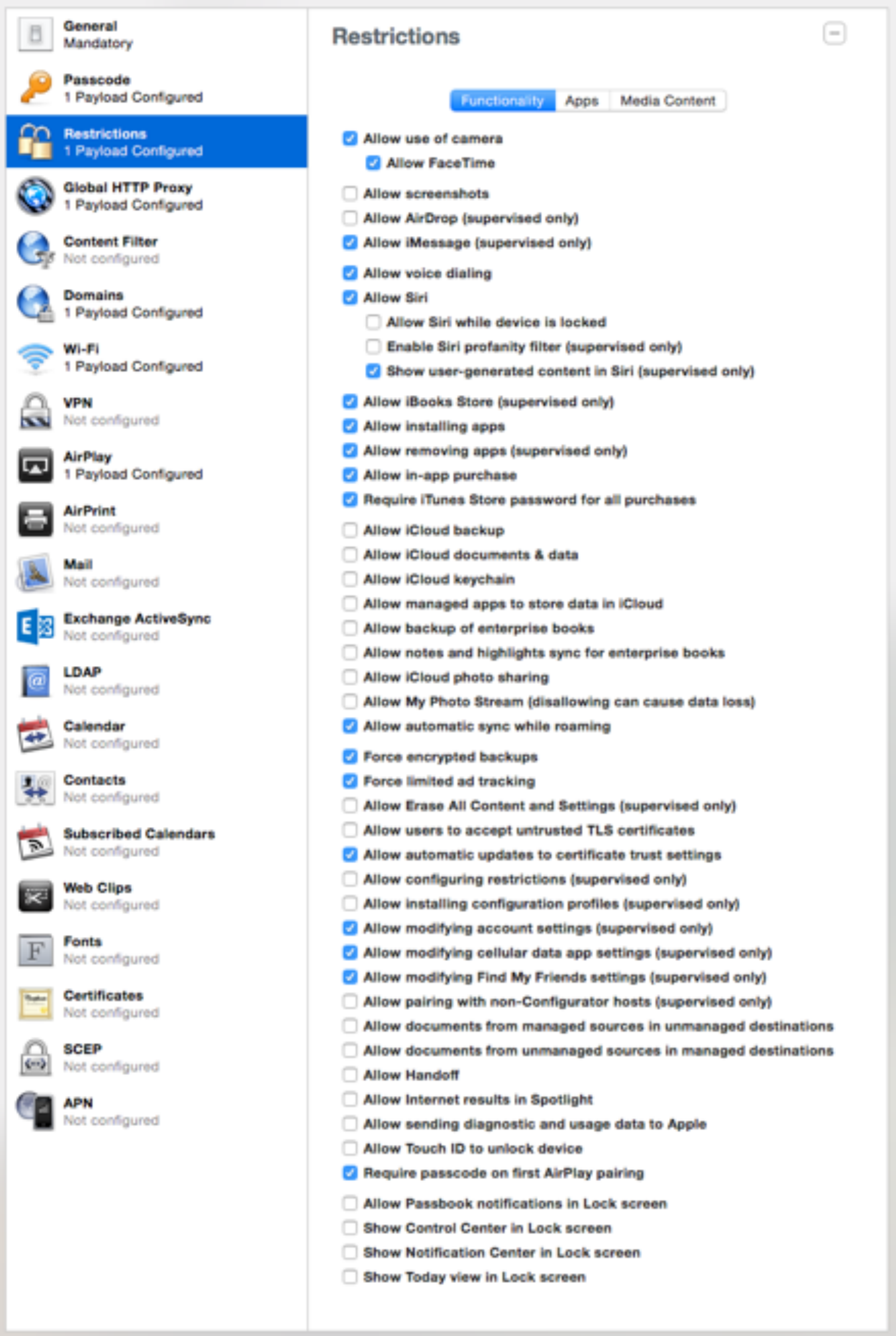
(Can be set via EAS or Configuration Profile)

Setting	Recommendation
Allow simple value	Disabled
Require alphanumeric value	Enabled
Minimum passcode length	8
Minimum number of complex characters	0
Maximum passcode age	90 days
Auto-lock	5 minutes
Passcode history	8
Grace period for device lock	None
Maximum number of failed attempts	8*

* Passcode exponential back off timing begins after 5 attempts. Allowing 8 attempts will require users wait 21 minutes cumulatively before forcing a device wipe.

Note: Depending on the EAS version, only some of the above may be set by the EAS Server and a Configuration Profile would be required.

Restrictions (Functionality)



General
Mandatory

Passcode
1 Payload Configured

Restrictions
1 Payload Configured

Global HTTP Proxy
1 Payload Configured

Content Filter
Not configured

Domains
1 Payload Configured

Wi-Fi
1 Payload Configured

VPN
Not configured

AirPlay
1 Payload Configured

AirPrint
Not configured

Mail
Not configured

Exchange ActiveSync
Not configured

LDAP
Not configured

Calendar
Not configured

Contacts
Not configured

Subscribed Calendars
Not configured

Web Clips
Not configured

Fonts
Not configured

Certificates
Not configured

SCEP
Not configured

APN
Not configured

Restrictions

Functionality | Apps | Media Content

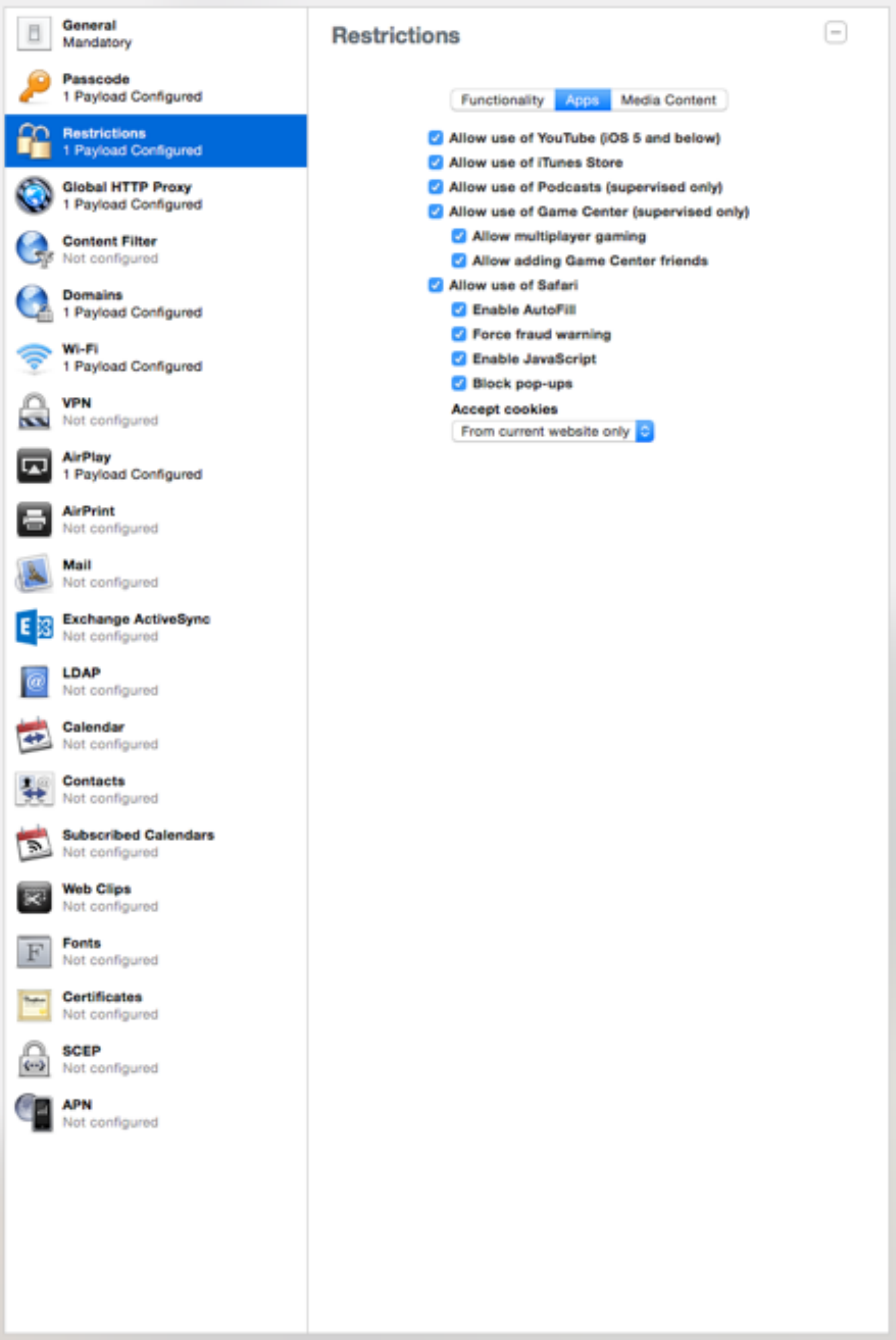
- ☑ Allow use of camera
  - ☑ Allow FaceTime
- ☐ Allow screenshots
- ☐ Allow AirDrop (supervised only)
- ☑ Allow iMessage (supervised only)
- ☑ Allow voice dialing
- ☑ Allow Siri
  - ☐ Allow Siri while device is locked
  - ☐ Enable Siri profanity filter (supervised only)
  - ☑ Show user-generated content in Siri (supervised only)
- ☑ Allow iBooks Store (supervised only)
- ☑ Allow installing apps
- ☑ Allow removing apps (supervised only)
- ☑ Allow in-app purchase
- ☑ Require iTunes Store password for all purchases
- ☐ Allow iCloud backup
- ☐ Allow iCloud documents & data
- ☐ Allow iCloud keychain
- ☐ Allow managed apps to store data in iCloud
- ☐ Allow backup of enterprise books
- ☐ Allow notes and highlights sync for enterprise books
- ☐ Allow iCloud photo sharing
- ☐ Allow My Photo Stream (disallowing can cause data loss)
- ☑ Allow automatic sync while roaming
- ☑ Force encrypted backups
- ☑ Force limited ad tracking
- ☐ Allow Erase All Content and Settings (supervised only)
- ☐ Allow users to accept untrusted TLS certificates
- ☑ Allow automatic updates to certificate trust settings
- ☐ Allow configuring restrictions (supervised only)
- ☐ Allow installing configuration profiles (supervised only)
- ☑ Allow modifying account settings (supervised only)
- ☑ Allow modifying cellular data app settings (supervised only)
- ☑ Allow modifying Find My Friends settings (supervised only)
- ☐ Allow pairing with non-Configurator hosts (supervised only)
- ☐ Allow documents from managed sources in unmanaged destinations
- ☐ Allow documents from unmanaged sources in managed destinations
- ☐ Allow Handoff
- ☐ Allow Internet results in Spotlight
- ☐ Allow sending diagnostic and usage data to Apple
- ☐ Allow Touch ID to unlock device
- ☑ Require passcode on first AirPlay pairing
- ☐ Allow Passbook notifications in Lock screen
- ☐ Show Control Center in Lock screen
- ☐ Show Notification Center in Lock screen
- ☐ Show Today view in Lock screen

Setting	Recommendation
Allow use of camera	Up to agency, depending upon acceptable use policy.
Allow FaceTime	Up to agency. All FaceTime communication must be Unclassified.
Allow screenshots	Disabled
Allow Airdrop	Disabled
Allow iMessage	Up to agency. All iMessage communication must be Unclassified.
Allow voice dialing	Up to agency
Allow Siri	Up to agency. All uses of Siri and Siri dictation must be treated as Unclassified.
Allow Siri while device is locked	Disabled
Enable Siri profanity filter	Up to agency. Depending upon acceptable use policy.
Show user-generated content in Siri	Up to agency. All uses of Siri and Siri dictation must be treated as Unclassified.
Allow iBookstore	Up to agency. Depending upon acceptable use policy.
Allow installing apps	Up to agency. May be enabled at PROTECTED when used with “Managed Open-In” restrictions described below.

Setting	Recommendation
Allow removing apps	Up to agency. Disabling may be used to prevent users from removing business critical apps.
Allow In-app purchase	Up to agency. Depending upon acceptable use policy.
Require iTunes Store password for all purchases	Enabled
Allow iCloud backup	Disabled
Allow iCloud documents & data	Disabled
Allow iCloud keychain	Disabled
Allow managed apps to store data in iCloud	Disabled unless managed apps meet ISM requirements for reducing storage/handling requirements of the remotely stored data to Unclassified.
Allow backup of enterprise books	Up to agency. Recommend disabled when agency distributes enterprise iBooks containing sensitive data.
Allow notes and highlights sync for enterprise books	Up to agency. Recommend disabled when agency distributes enterprise iBooks containing sensitive data.
Allow iCloud photo sharing	Up to agency. If enabled, photos may be backed up to Apple's iCloud infrastructure and distributed to another user's iOS devices.

Setting	Recommendation
Allow My Photo Stream	Up to agency. If enabled, photos may be backed up to Apple's iCloud infrastructure and distributed to a user's other iOS devices.
Allow automatic sync while roaming	Enabled
Force encrypted backups	Enabled
Force limited ad tracking	Enabled
Allow Erase All Content and Settings	Disabled unless required for users with a specific need to erase devices themselves.
Allow users to accept untrusted TLS certificates	Disabled
Allow automatic updates to certificate trust settings	Enabled
Allow configuring restrictions	Disabled
Allow installing Configuration Profiles	Disabled unless required for agency deployment
Allow modifying account settings	Enabled

Setting	Recommendation
Allow modifying cellular data app settings	Up to agency.
Allow modifying Find my Friends settings	Enabled
Allow pairing with non-Configurator hosts	Disabled
Allow documents from managed source in unmanaged destinations	Disabled. This control helps to prevent documents being opened in unmanaged user applications.
Allow documents from unmanaged sources in managed destinations	Up to agency. If enabled, a user may open documents from their own unmanaged apps into agency managed apps. If enabled, there is a risk that a managed app could be exploited by hostile content from an unmanaged user application. Recommended disabled at PROTECTED.
Allow Handoff	Disabled
Allow Internet results in Spotlight	Up to agency. Recommended disabled.
Send diagnostic and usage data to Apple	Disabled
Allow Touch ID to unlock device	Disabled at PROTECTED
Require passcode on first AirPlay pairing	Enabled
Allow Passbook notifications while locked	Up to agency. If enabled, passbook items may be accessible from the lock screen.
Show Control Center in lock screen	Up to agency. If enabled, Wi-Fi and Bluetooth may be enabled or disabled from the lock screen.
Show Notification Center in lock screen	Disabled
Show Today view in lock screen	Disabled



Restrictions

☑ Allow use of YouTube (iOS 5 and below)

☑ Allow use of iTunes Store

☑ Allow use of Podcasts (supervised only)

☑ Allow use of Game Center (supervised only)

- ☑ Allow multiplayer gaming
- ☑ Allow adding Game Center friends

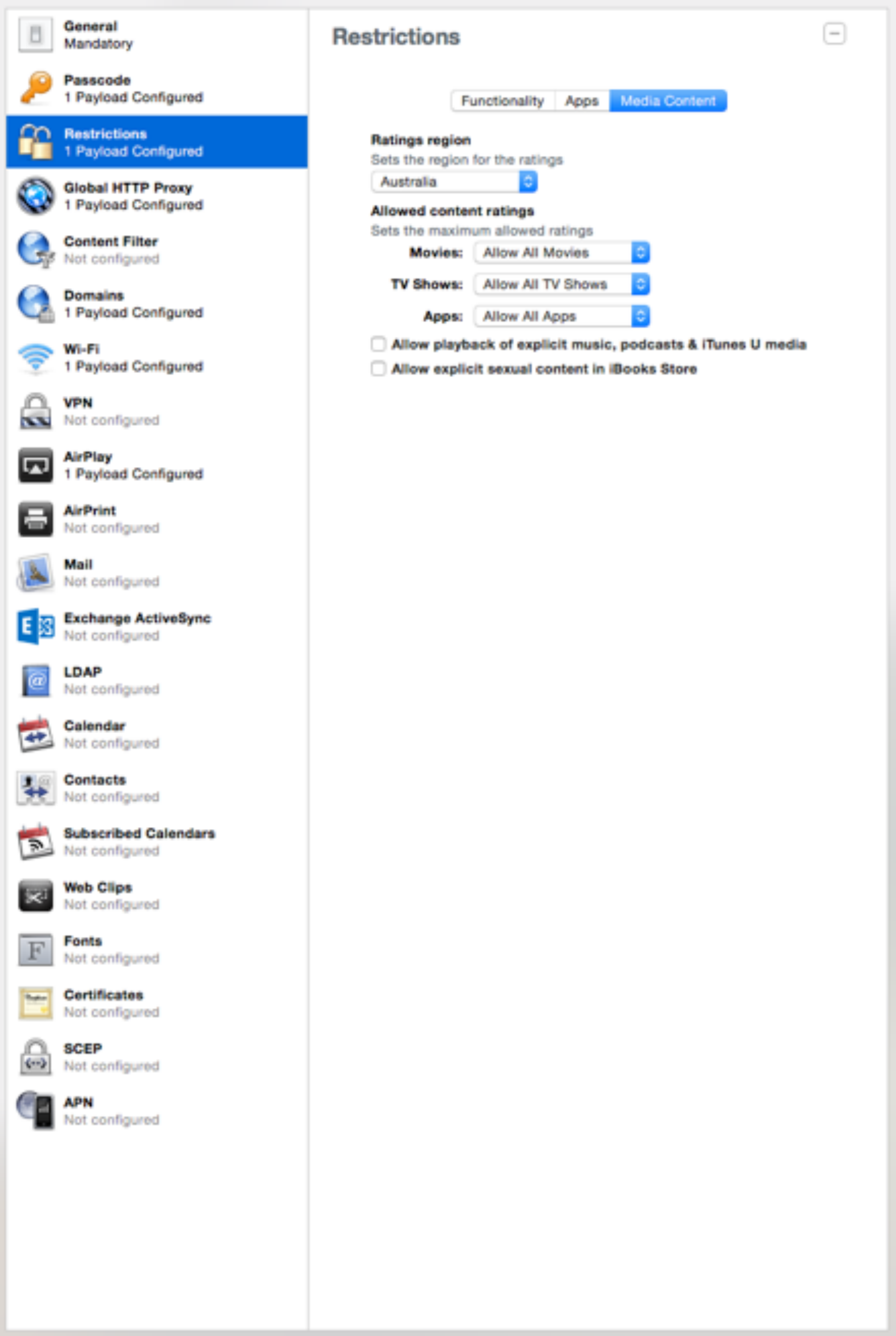
☑ Allow use of Safari

- ☑ Enable AutoFill
- ☑ Force fraud warning
- ☑ Enable JavaScript
- ☑ Block pop-ups

Accept cookies: From current website only

Restrictions (Applications)

Setting	Recommendation
Allow use of YouTube	Up to agency. Depending upon acceptable use policy.
Allow use of iTunes Store	Up to agency. Depending upon acceptable use policy.
Allow use of Podcasts	Up to agency. Depending upon acceptable use policy.
Allow use of Game Center	Up to agency. Depending upon acceptable use policy.
Allow multiplayer gaming	Up to agency. Depending upon acceptable use policy.
Allow adding Game Center friends	Up to agency. Depending upon acceptable use policy.
Allow use of Safari	Enabled
Enable AutoFill	Enabled
Force fraud warning	Enabled
Enable JavaScript	Enabled
Block pop-ups	Enabled
Accept cookies	Up to agency. Recommend “From current website only”



Ratings region

Sets the region for the ratings

Australia

Allowed content ratings

Sets the maximum allowed ratings

Movies: Allow All Movies

TV Shows: Allow All TV Shows

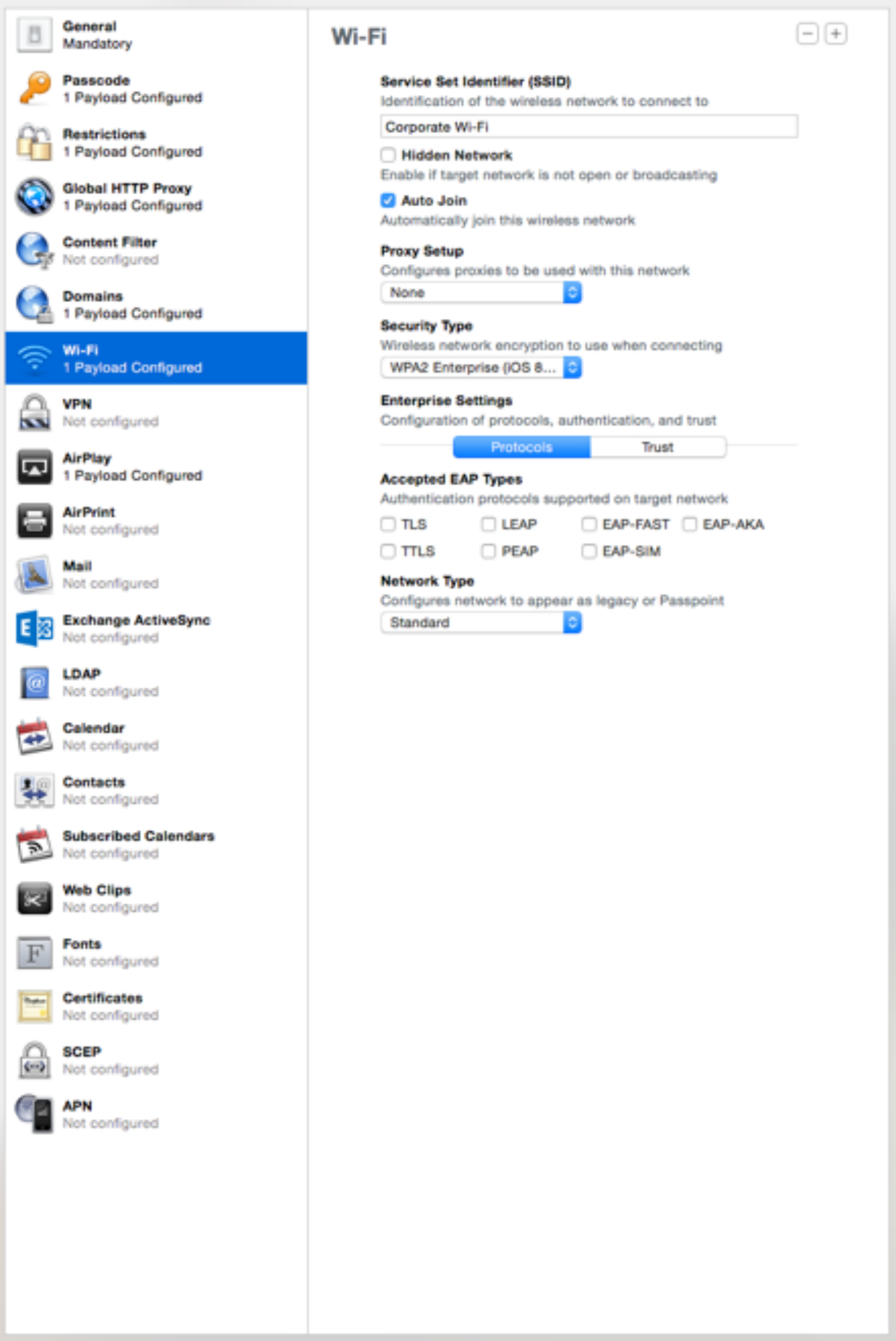
Apps: Allow All Apps

□ Allow playback of explicit music, podcasts & iTunes U media

□ Allow explicit sexual content in iBooks Store

Restrictions (Media Content)

Setting	Recommendation
Ratings Region	Australia
Allowed content ratings (all)	Up to agency. Depending upon acceptable use policy.
Allow explicit music, podcasts & iTunes U	Up to agency. Depending upon acceptable use policy.
Allow explicit sexual content in iBooks Store	Up to agency. Depending upon acceptable use policy.



Wi-Fi

Service Set Identifier (SSID)
Identification of the wireless network to connect to
Corporate Wi-Fi

□ **Hidden Network**
Enable if target network is not open or broadcasting

☑ **Auto Join**
Automatically join this wireless network

Proxy Setup
Configures proxies to be used with this network
None

Security Type
Wireless network encryption to use when connecting
WPA2 Enterprise (iOS 8...

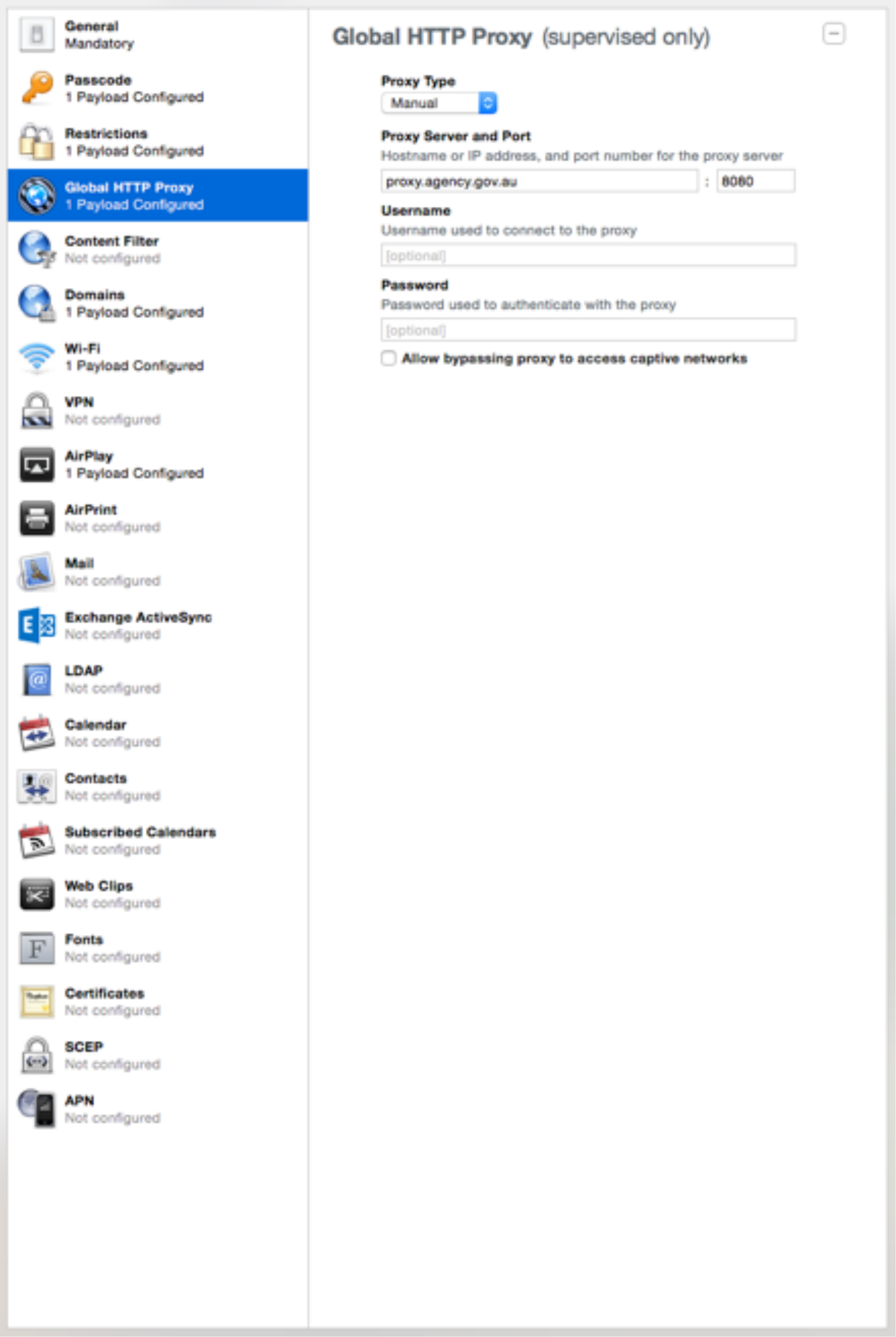
Enterprise Settings
Configuration of protocols, authentication, and trust

Accepted EAP Types
Authentication protocols supported on target network
□ TLS □ LEAP □ EAP-FAST □ EAP-AKA
□ TTLS □ PEAP □ EAP-SIM

Network Type
Configures network to appear as legacy or Passpoint
Standard

Wi-Fi

Setting	Recommendation
Service Set Identifier (SSID)	As appropriate for agency network
Hidden Network	As appropriate for agency network
Auto Join	Recommended enabled
Proxy Setup	As appropriate for agency network
Security Type	WPA2 Authentication with EAP-TLS and a pre-shared key as a minimum, per use RADIUS or 802.1X recommended.
Enterprise Settings	Protocols, authentication and trust to match network requirements. 802.1X with device identity certificate and username/password is the preferred authentication mechanism for Unclassified (DLM) and higher.
Network Type	Standard



Global HTTP Proxy (supervised only)

Proxy Type
Manual

Proxy Server and Port
Hostname or IP address, and port number for the proxy server
proxy.agency.gov.au : 8080

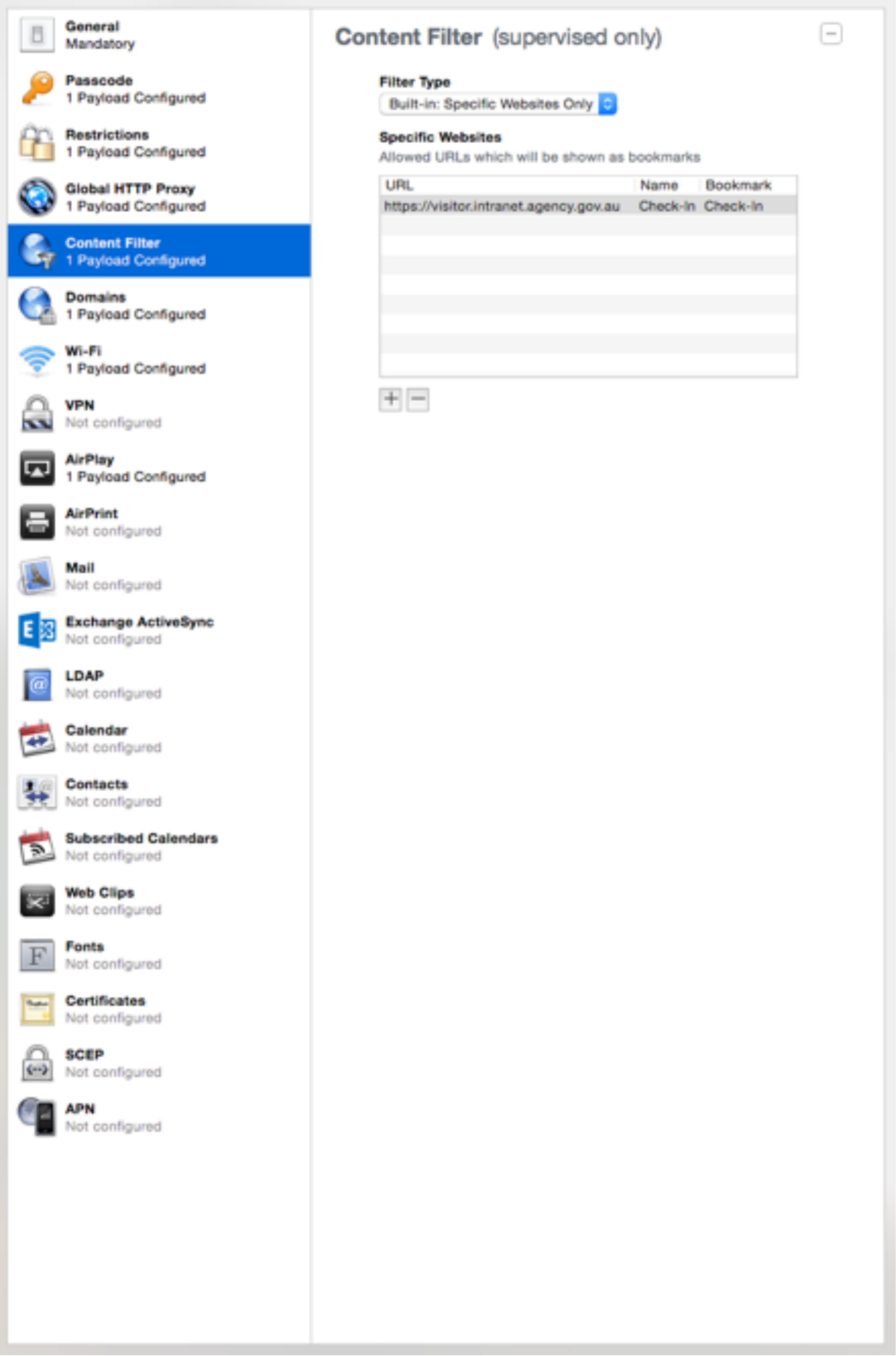
Username
Username used to connect to the proxy
[optional]

Password
Password used to authenticate with the proxy
[optional]

□ Allow bypassing proxy to access captive networks

Global Proxy

Setting	Recommendation
Proxy Type, Server, Port, Username & Password	As appropriate for agency network.
Allow bypassing proxy to access captive networks	Up to agency. If enabled, the proxy setting will be bypassed when an iOS device assesses the connected network to be “captive” (eg. Paid hotel or airport Wi-Fi). For most usage scenarios enabling this defeats the purpose of using global proxy. Recommended disabled.



Content Filter (supervised only)

Filter Type

Built-in: Specific Websites Only

Specific Websites

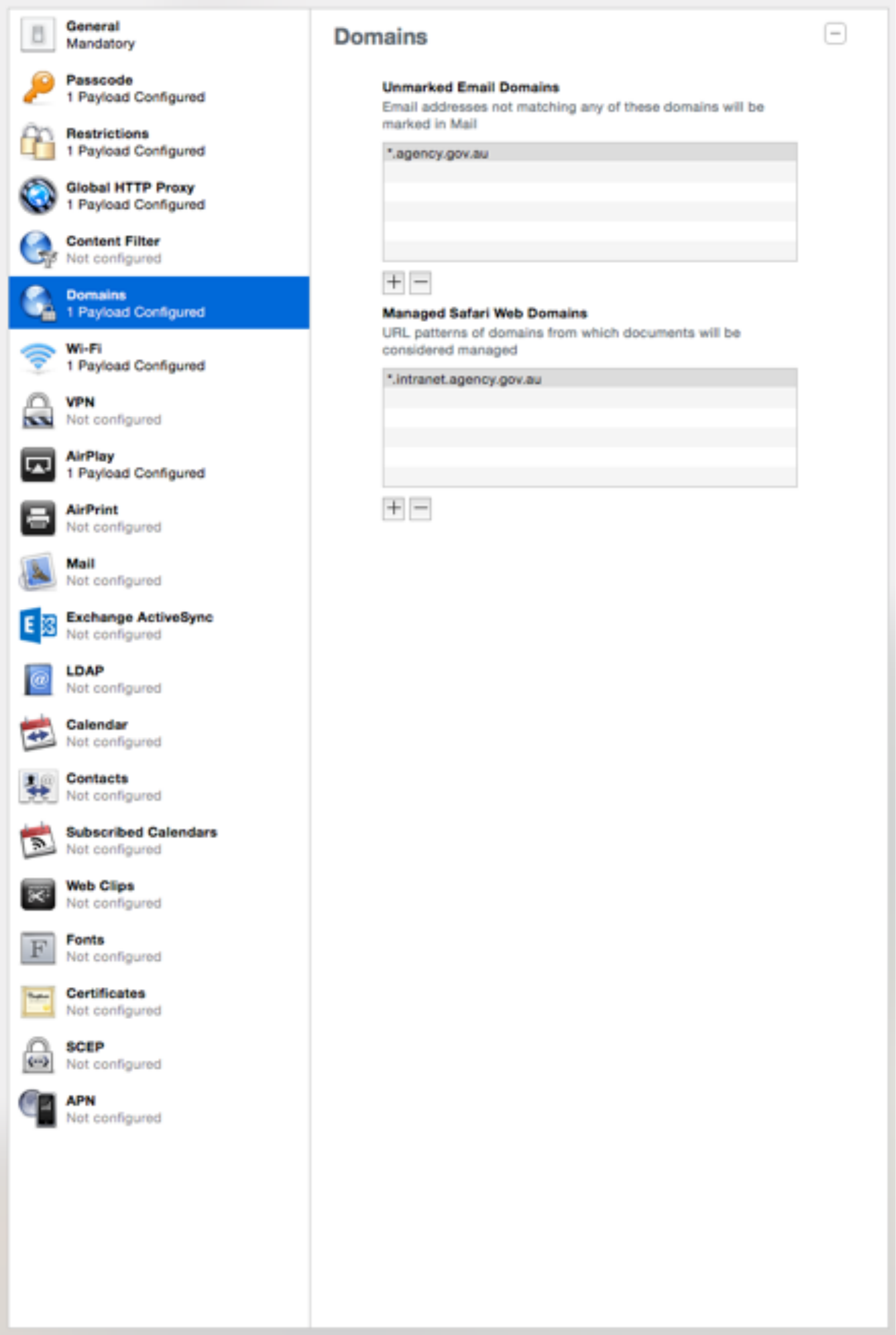
Allowed URLs which will be shown as bookmarks

URL	Name	Bookmark
https://visitor.intranet.agency.gov.au	Check-In	Check-In

Content Filter

The content filter configuration payload may be used to limit access to adult websites or to restrict web access to a whitelist of specific allowed websites. These restrictions are applied universally regardless of which network interface is used. Use of these restrictions is up to the Agency. Some use cases where these restrictions may be useful:

- where filtering is required and a VPN + proxy configuration is not feasible
- iOS based information kiosk



General
Mandatory

Passcode
1 Payload Configured

Restrictions
1 Payload Configured

Global HTTP Proxy
1 Payload Configured

Content Filter
Not configured

Domains
1 Payload Configured

Wi-Fi
1 Payload Configured

VPN
Not configured

AirPlay
1 Payload Configured

AirPrint
Not configured

Mail
Not configured

Exchange ActiveSync
Not configured

LDAP
Not configured

Calendar
Not configured

Contacts
Not configured

Subscribed Calendars
Not configured

Web Clips
Not configured

Fonts
Not configured

Certificates
Not configured

SCEP
Not configured

APN
Not configured

Domains

Unmarked Email Domains
Email addresses not matching any of these domains will be marked in Mail

*.agency.gov.au

Managed Safari Web Domains
URL patterns of domains from which documents will be considered managed

*.intranet.agency.gov.au

Domains

The Domains payload performs two roles; marking external email addresses in Mail app, and ensuring that Safari treats downloaded documents as “Managed” while browsing managed web domains.

Managed Email Domains consists of a whitelist of string matching expressions for email suffixes. When this payload is configured, the iOS Mail app will highlight email addresses which are not in the whitelist.

Managed Web Domains consists of a list of string matching expressions for URLs.

A good example of how this may be used with intranet domains might be to add. “*.intranet.agency.gov.au” which would match:

- https://intranet.agency.gov.au/selfservice

- https://wiki.intranet.agency.gov.au

It would not match the internet facing agency website:

- https://www.agency.gov.au

Note: It is strongly recommended that Managed Web Domains be configured to lower the likelihood of sensitive data breach.

VPN

IPSec and TLS are Approved Cryptographic Protocols, please refer to the ISM for more information:

http://www.asd.gov.au/infosec/ism/

To help determine the server side settings that iOS supports, refer to the iOS Deployment Technical reference at:

http://www.apple.com/iphone/business/it/deployment.html

Prior to iOS 7, ASD's recommended On Demand configuration was to trigger on a URL whitelist using the *OnDemandMatchDomainAlways* Configuration Profile rule. In iOS 7 this rule has been deprecated and replaced with the new *EvaluateConnection* rule set. To create a VPN profile that works on both iOS 7 and earlier releases, it is necessary to utilise both *EvaluateConnection* and *OnDemandMatchDomainAlways* together. In such a configuration, iOS 7 and later will use *EvaluateConnection* while previous releases will ignore it.

There are several VPN On-Demand configurations that are possible at PROTECTED. Examples are:

- Action:Connect on DNSDomainMatch:(array of whitelisted domains OR wildcard)
- Action:Connect on InterfaceTypeMatch:Cellular, Action:EvaluateConnection on InterfaceTypeMatch:Wi-Fi Domains:(whitelist or wildcard) DomainAction:ConnectIfNeeded RequiredURLStringProbe:(trusted internal HTTPS server)

Always-on VPN

Always-On VPN is available as a supervised only option for IKEv2 VPN. Available only on the IKEv2 VPN payload, it ensures that all network traffic is routed to the VPN. When the VPN can't be established, no network traffic is be transmitted.

Always-On VPN may be used in PROTECTED deployments, and is the simplest VPN configuration solution at this classification.

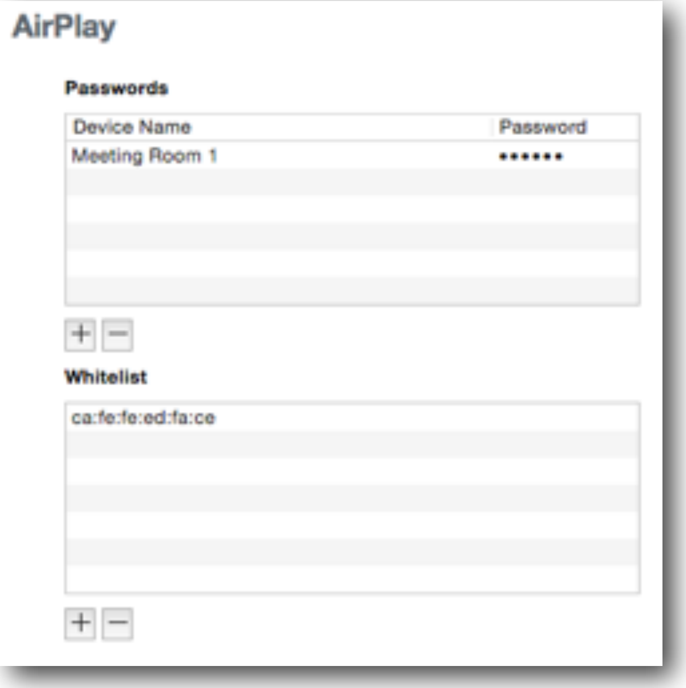
Setting	Recommendation
Machine Authentication	Certificate. Full chain of trust must be included in certificate (credentials) payload.
Include User PIN	As appropriate for agency network. User PIN is not necessary, certificate for machine authentication is sufficient for PROTECTED.
Enable VPN On Demand	iOS 7+: As above, please contact ASD for assistance at PROTECTED Earlier releases: Enabled with whitelist of agency URLs or domains that device is allowed to access.
Proxy Setup	As appropriate for agency network.

Note: Split tunnel VPN should be disabled (set VPN concentrator side).

AirPlay Mirroring

The AirPlay mirroring payload may be used to pre-populate a device with a whitelist of AirPlay devices and AirPlay passwords. These options can be configured to assist in controlling access to AirPlay resources. For AirPlay to AppleTV, it is recommended that agencies utilise alphanumeric passcodes to prevent unauthorised use of AirPlay.

Reminder: AirPlay should never be used to transmit video/audio of a classification greater than that of the network the device is using.



AirPlay

Passwords

Device Name	Password
Meeting Room 1	••••••

Whitelist

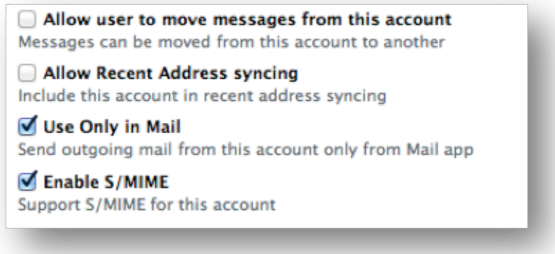
ca:fe:fe:ed:fa:ce

AirPrint

The AirPrint payload may be used to pre-populate a device with a list of discoverable or undiscoverable AirPrint devices. These settings are intended for user convenience.

Mail

A Mail payload is not typically needed if EAS (e.g. Exchange ActiveSync Gateway, Lotus Notes Traveller) is in use. The Mail payload can co-exist with Exchange. If used, fill with settings appropriate to agency network.



☐ Allow user to move messages from this account
Messages can be moved from this account to another

☐ Allow Recent Address syncing
Include this account in recent address syncing

☑ Use Only in Mail
Send outgoing mail from this account only from Mail app

☑ Enable S/MIME
Support S/MIME for this account

Setting	Recommendation
Use SSL	Enabled, with authentication.
Allow user to move messages from this account	Disabled in deployments where multiple email accounts of different classifications are expected.
Allow Recent Address syncing	Disabled
Use Only in Mail	Enabling this setting prevents other apps from sending mail with this account. Though enabling this option is preferable, it will break functionality in some third party apps – including some MDM client apps. Enable this setting if possible in your deployment.
Enable S/MIME	Enabled if agency infrastructure supports S/MIME

Exchange ActiveSync

The EAS server settings should be filled in as required for the agency network noting the following consideration:

- Authentication credentials required to control which device and which users have access to EAS must be added to the Certificate/Credentials Payload. The credential required for authenticating the ActiveSync account can then be selected.

Note: If a profile with an EAS payload is removed, all EAS synced email and attachments are deleted from the device.

Setting	Recommendation
Use SSL	Enabled, with authentication.
Allow user to move messages from this account	Disabled in deployments where multiple email accounts of different classifications are expected.
Allow Recent Address syncing	Disabled
Use Only in Mail	Enabling this setting prevents other apps from sending mail with this account. Though enabling this option is preferable, it will break functionality in some third party apps – including some MDM client apps. Enable this setting if possible in your deployment.
Enable S/MIME	Enabled if agency infrastructure supports S/MIME

LDAP

LDAP settings should be filled in as required for the agency network. LDAP is not typically needed if Exchange GAL is used, but can co-exist.

- The “SSL Enabled” option toggles support for TLS. This should be enabled if supported by agency infrastructure.

Calendar (CalDAV)

CalDAV settings should be filled in as required for the agency network. CalDAV may not be needed if Exchange is used, but can co-exist.

- TLS Enabled if supported by agency infrastructure.

Contacts (CardDAV)

CardDAV settings should be filled in as required for the agency network. CardDAV may not be needed if Exchange is used, but can co-exist.

- TLS Enabled if supported by agency infrastructure.

Subscribed Calendars

Subscribed Calendars settings should be filled in as required for the agency network.

- TLS Enabled if supported by agency infrastructure.

Web Clips

Web Clips are “aliases” or links to URLs with a custom icon that can be installed on a device home screen. Settings should be filled in according to the agency’s deployment requirements.

- Typical use would include links to pages for AUP, helpdesk contact details, telephone URLs, and SCEP re-enrolment pages. Note that these web pages could use preference manifest settings in their HTML to work when the site is offline or the device is off the network.

- Web clips can also be used to install Enterprise In-House Applications.

Certificate (Credentials)

Include SSL chain of trust back to the root CA certificate, including intermediates.

SCEP

Simple Certificate Enrolment Protocol (SCEP) is normally configured during Over-The-Air MDM enrolment, however the Configuration Profile SCEP payload can be used when pre-configuring SCEP enrolment prior to device issue. Configure as necessary for agency deployment.

Advanced/APN

If an APN is used, settings should be filled in as required for agency network noting the following considerations:

- Access Point User Name and Password must be used.

- Proxy should be configured as appropriate.

Details should be discussed with your telecommunications carrier.

CHAPTER 8

Mobile Device Management

Enroll this iPhone to allow it to be remotely managed.

Once enrolled you will also be able to wipe all data from and lock access to this iPhone.

How to use Mobile Device Management software to provision, configure and manage iOS devices.

Mobile Device Management

Organisations may use Mobile Device Management (MDM) software to provision, configure and manage iOS devices. Basic MDM functionality can be obtained using Mac OS X Server Profile Manager. Third party MDM software often features extended functionality.

Functions

There are four categories of tasks which are implemented under the Apple MDM protocol: enrolment, device configuration, device query and device command. Most third party MDM servers implement the functions which are supported natively by iOS, some extend the feature set with a client app. This chapter describes the useful functions which should be common to most MDM implementations.

Workflow Overview

Before a device can be managed it must be enrolled with an MDM server. There are a variety of ways that this can be performed. A user may be directed to login to a web portal where they will be asked to log in and then install an MDM Configuration Profile.

In other MDM implementations a client app may be installed on an iOS device. This app may be used to initiate MDM Configuration Profile installation and device provisioning. Both methods rely upon Safari to perform the enrolment.

Deployment with Supervision

Though the MDM enrolment process has been designed to function over the air, at this time device supervision can only be performed via the USB interface. For PROTECTED deployments, devices must be put in to supervised mode before MDM enrolment.

Managing iOS Devices

After devices have been deployed, administrators may need to change or remove Configuration Profiles. Apple's MDM protocol allows MDM servers to remove and install profiles, but only under the following conditions:

1. The MDM Payload must have the “Allow installation and removal of Configuration Profiles” access right set.

2. The Configuration Profile in question must have been installed by the MDM.

In some cases devices may simply need to be reconfigured to support a change in infrastructure or to update certificates, however this functionality can also be used to add or remove more restrictive settings on demand. It should be noted that some third party MDM vendors provide a geo-fencing function, which installs or removes Configuration Profiles depending upon location.

If a device is lost or stolen, an MDM administrator can take several actions to protect agency information. One option available is to issue a remote wipe command. This action replaces the file system key with a new randomly generated key, permanently rendering all data in the file system irrecoverable.

In the event that a user forgets their passcode, the Apple MDM protocol allows for a remote clear passcode command. Not only does this command unlock the device, by removing the passcode it also disables data protection. Consequently, the issuing of this command immediately modifies the storage and handling requirements of the device to that of the maximum classification of data stored on the device.

Note: The clear passcode command must not be issued unless the device owner is in physical possession of the device. The clear passcode command must never be issued to a lost or stolen device.

There are a number of methods that are normally used for de-provisioning iOS devices. These may involve remotely removing MDM and associated profiles or issuing a remote wipe. In PROTECTED deployments, iOS devices should be returned to base and de-provisioned using the methods described in Chapter 4.

Querying Devices

There are a number of query operations supported by Apple's MDM protocol, which can be used to ensure that devices remain in compliance with agency policy. As an example, it is possible to query a device to find out:

- the device's iOS version
- which Configuration Profiles are installed
- the presence/complexity of passcode
- which apps are installed.

Some MDM implementations may allow for predefined or scripted actions to take place when a device is found to be out of compliance with policy.

Managed Settings

Though iOS device configuration is almost entirely managed using Configuration Profiles, it is possible for an MDM server to modify certain specific options without Configuration Profiles. These managed settings may be modified at any time and without user interaction. Managed settings may only be used if the "Apply Settings" right is set in the MDM payload.

Managed Apps

An MDM server may issue an Install Application command via the Apple MDM protocol. This command contains either:

- an app's iTunes store ID for App Store apps
- a URL link to an App's manifest XML file for in-house or custom apps.

Additionally, the command must specify how the app is to be managed. Namely, whether the app is to be removed when the MDM profile is removed and whether app data can be backed up. After receiving a valid Install Application command, an iOS device will prompt a user to accept the app installation. Apps that are installed in this way are called Managed apps.

When apps require payment, it is possible for an MDM to provide a VPP redemption code. In many third party MDM implementations this function is tightly integrated with an enterprise app store. It should be noted that App Store apps cannot be installed if the App Store has been disabled through Configuration Profile restriction.

Finally, it is possible for an MDM server to issue a Remove Application command to remotely remove a managed app and its data. Apps that were not installed as a managed app by the MDM cannot be removed in this way.

Choosing MDM Software

At the time of writing this guide there are a number of vendors shipping MDM solutions that have full support for Apple's MDM protocol. Some of these MDM solutions focus on the core functionality provided by Apple's MDM protocol, others enhance this by providing additional features via a client app. Many MDM vendors distribute an MDM solution that can manage multiple mobile and desktop client platforms. The following information is provided to help agencies understand functionality commonly offered by vendors and to describe the advantages and risks of various deployment options.

Proprietary Functionality

MDM software vendors may have a client app that can interact with an MDM server. Such apps can interact with a device in ways beyond that which the Apple MDM protocol allows for. These MDM client apps do not operate at any elevated level of privilege, and if installed from the App Store are subject to normal App Store approval processes.

Email attachment security is a feature that some MDM vendors provide outside of Apple's MDM protocol. The purpose of this function is to prevent the iOS Mail app "Open In" functionality from opening a sensitive attachment in an untrusted app. One way that this type of service can work is by an email proxy transparently encrypting attachments and then having the file opened by a client app that has registered the appropriate file or data type information with iOS. Typically this allows the file to be opened and decrypted by the client app from the iOS Mail app using "Open In" functionality. Managed Open-In can be used to achieve a similar outcome.

A valuable proprietary feature that some MDM vendors provide is an Enterprise App Store. This allows a user to pull the apps that they require rather than have apps pushed at them. An Enterprise App Store may exist as a mobile web application or a native app initially pushed to a device. In both cases this functionality requires use of native iOS MDM protocol functionality, but may contain proprietary extensions. Such Enterprise App Stores often allow administrators to distribute not only in-house applications but also App Store apps and Volume Purchase Program (VPP) apps. Such a feature is a good way for administrators to have some control over which apps can be installed and to reduce costs by only distributing paid apps to users that require them.

Frequently MDM vendors also provide a secure container client app. The purpose of this type of app is to act as a secure repository for common file types. Most implementations allow users to view common file types while some allow file editing. The way in which these types of apps provide security for files varies and can include:

- standard iOS data protection
- encryption provided by iOS cryptography libraries
- encryption provided by 3rd party cryptographic software.

Important: Class A data protection in iOS is sufficient for PROTECTED data.

On-premise and MDM Software as a Service

In addition to on-premise options, several MDM vendors offer “cloud” MDM Software as a Service (SaaS). The benefit of this solution is that it frees administrators from having to set up and maintain a MDM server and often may offer a lower cost of ownership. In some cases a SaaS MDM solution may have a tightly integrated client app that improves overall user experience and reduces administrative burden.

Although there are many advantages to this MDM model, there are also significant risks. At a fundamental level, an MDM server controls access to agency information and authority over the configuration of the devices it manages. For example, an MDM routinely processes or stores:

- key material that can be used to unlock a device that is passcode protected
- Configuration Profile data for MDM enrolment and credentials for access to an agency’s network.

Since key material is classified at the same level of the data it is protecting, the systems used by the MDM service provider must be accredited to the same minimum standard as the sponsoring agency’s systems.

Should the MDM be compromised, an adversary may be able to perform all tasks an MDM is capable of. This may include:

- using escrow keybag material to unlock passcode protected devices
- provisioning unauthorised devices
- distributing hostile apps.

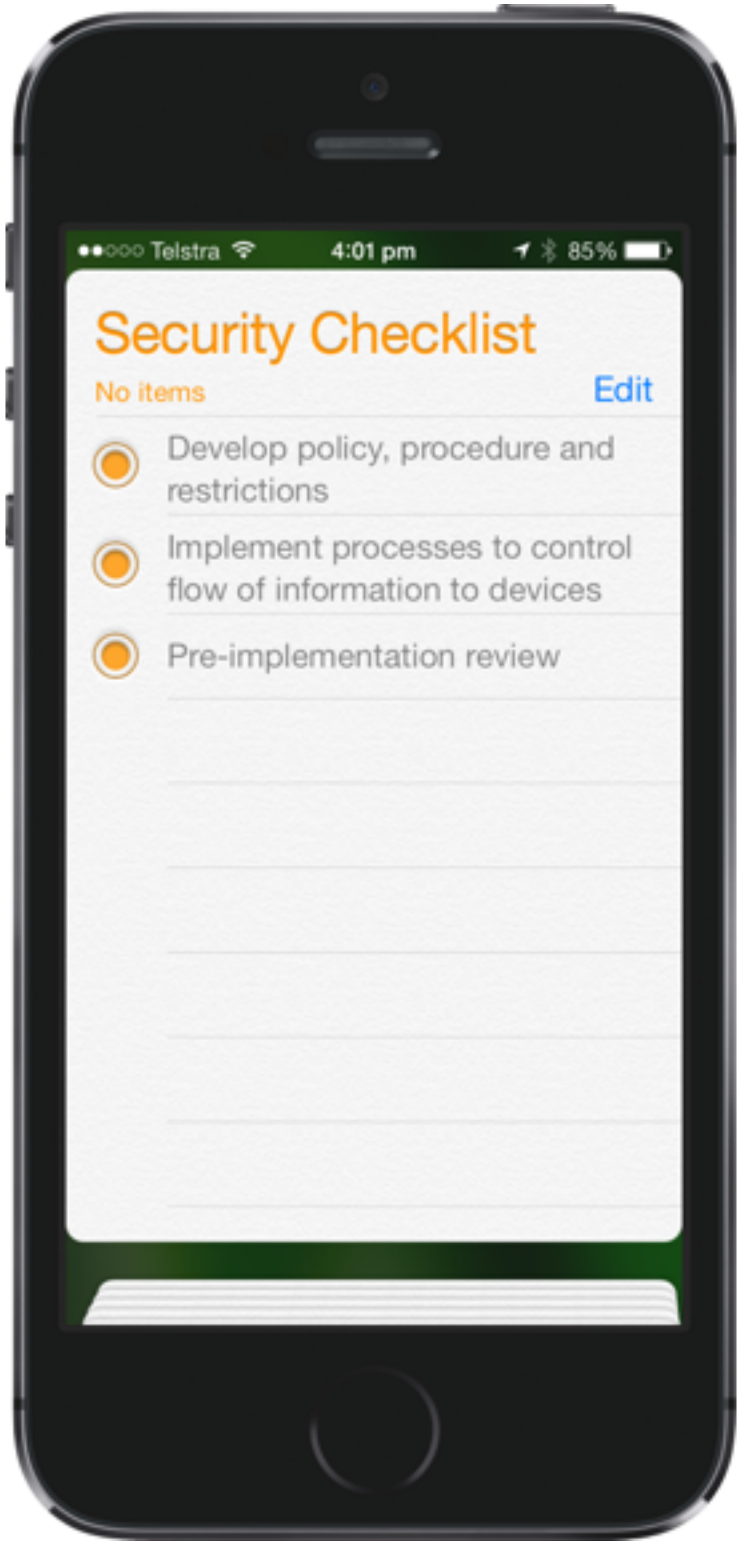
Additionally, an adversary may also be able to leverage information in Configuration Profiles to establish VPN or Wi-Fi connections to agency networks.

To protect against the risk of unauthorised access to data by a third party, agencies must follow ASD’s Industry Engagement and Outsourcing guidance in the ISM. Administrators are also strongly advised to read ASD’s *Cloud Computing Security Considerations* before proceeding with a SaaS MDM deployment, available at:

http://www.asd.gov.au/infosec/cloudsecurity.htm

Chapter 9

Security Checklist



●●○○○ Telstra 4:01 pm 85%

Security Checklist

No items Edit

○ Develop policy, procedure and restrictions

○ Implement processes to control flow of information to devices

○ Pre-implementation review

Ensure that all key tasks in securely deploying iOS devices have been completed.

Before Deploying iOS Devices

Develop agency policy and procedures, including any restrictions, for the use of iOS devices that align with Australian Government legislation, policies and standards, and that adhere to Australian government requirements.

Effective policies and procedures help to ensure that an agency considers relevant issues and operates in accordance with legislation and whole-of-government guidelines. Documenting and making these available to users will help ensure that users are aware of an agency's expectations of them when using mobile devices. On iOS devices, placing a policy Web Clip on the device makes it highly accessible to the user.

Implement processes to security classify, protectively mark, and control the flow of information that may be transmitted to/from the iOS device.

Email filtering solutions can filter and mark email based on header metadata and shorthand notation in the subject line. Agencies must security classify and protectively mark all email, and controls must be implemented at email servers and gateways to restrict delivery of inappropriately classified information to and from an agency, including to mobile devices.

Undertake an iOS device pre-implementation review.

Agencies deploying iOS devices may consider undertaking a pre-implementation review. This review would assess the planned deployment strategy, mitigation controls, policies and procedures against the requirements defined in the relevant policy and guidance documents. ASD can assist in ensuring the necessary steps have been followed.

Manage Use of iOS Devices

Provide users with training on the use of iOS devices and security requirements.

In many areas of administration, failure to follow policies and procedures is not a result of deliberate actions, but a lack of awareness of requirements. Training can assist users to implement policies and procedures. The existence of training can also help distinguish deliberate misuse from incompetent usage. As part of this training agencies should also inform users that these devices are likely to be an attractive target for thieves, and that the implications of the information contained in them being accessed by others could be detrimental to the Australian government.

Ensure that users formally acknowledge their agreement to adhere to agency specific Acceptable Usage Policy and procedures.

Users must be aware of and agree with the agency's policy and procedures. The ramifications of failing to apply those policies and procedures must also be clear to users.

Ensure that users classify and protectively mark all email with the highest classification of the content or attachment, in accordance with Australian government standards.

Users must be conscious of the security classification of information that they are sending to or from mobile devices. Agencies must ensure that users classify and protectively mark all agency-originated email or attachments in accordance with the highest classification of the content.

Infrastructure Considerations

Server infrastructure for EAS, MDM, Web and associated CA infrastructure that supports an iOS deployment must be controlled, either directly or under contract, by the Australian government.

These servers should be situated in a controlled environment, and will permit the implementation of consistent policy and device settings.

In many cases, SaaS solutions may not be acceptable for iOS MDM deployments.

Agencies must ensure that content is transferred between an iOS device and an agency's ICT systems in accordance with Australian government policy.

Email protective marking filtering mechanisms must be implemented to provide a higher level of security by automatically preventing information of an inappropriate classification being sent to a mobile device. These mechanisms are described in the *Email Protective Marking Standard Implementation Guide for the Australian Government*, available at:

http://www.finance.gov.au/files/2012/04/email_pmsig.pdf

Ensure that email originating outside the agency is not sent to the iOS device unless it is classified and labelled appropriately.

Communications originating outside the agency may also include classified information. The policies and standards applied to external communications must also be applied to internally generated information. Emails that do not have protective markings should not be transmitted to mobile devices. Agency policy may define a subset, e.g. an agency may only permit Unclassified information to be forwarded to a mobile device. These mechanisms are described in the *Email Protective Marking Standard Implementation Guide for the Australian Government.*

Review and Audit

Undertake an iOS post implementation review.

Agencies that deploy iOS devices must undertake a post implementation review. This may assist in identifying policy and implementation inconsistencies and assess the mitigation controls for completeness against the Security Risk Management Plan (SRMP), the System Security Plan (SSP), Standard Operating Procedures (SOP) and the implementation of email protective marking controls. This review must be completed within twelve months of the live production deployment.

Audit compliance with policies and standards for the use of iOS devices.

Setting out policy without monitoring compliance is unsound practice. There should be appropriate internal and – from time to time – external checks of compliance with policies regarding the use of mobile devices. There should also be regular reviews of internal policies, to test their currency and adequacy.

CHAPTER 10

Example Scenarios

This chapter describes hypothetical scenarios showing how the various techniques can be combined.

iPad
2:00 pm
97%
asd.gov.au
Risk Management of Enterprise Mobility including Bring Your Own Device (BYOD): ASD Australian Signals Directorate (formerl...
Australian Government
Department of Defence
Australian Signals Directorate
Reveal Their Secrets - Protect Our Own
Home
Information security
Publications
Careers
About
Contact
Search
Information security advice
For all levels of government

ASD > Publications > Risk Management of Enterprise Mobility including Bring Your Own Device (BYOD)

Risk Management of Enterprise Mobility including Bring Your Own Device (BYOD)

Overview of Enterprise Mobility

Download ***CSOC Protect Notice:*** ***Risk Management of Enterprise Mobility including Bring Your Own Device (BYOD) (PDF)***, June 2013

Table of Contents

- Executive Summary - Introduction to Enterprise Mobility
- Potential Benefits of Enterprise Mobility
- Potential Benefits of Using Personally-Owned Devices
- Develop an Enterprise Mobility Strategy
- Determine the Extent of Existing Enterprise Mobility
- Develop Business Cases with Suitable Mobility Approaches
  - Example Business Cases
  - Example Enterprise Mobility Approaches and Scenarios
  - Considerations for Choosing Enterprise Mobility Approaches
- Identify Regulatory Obligations and Legislation
- Allocate Budget and Personnel Resources
- Develop and Communicate Enterprise Mobility Policy
  - Technical Support
  - Financial Support
- Monitor the Implementation and Report to Management
- Facilitate Organisational Transformation
- Further Information
- Contact
- Appendix A: Arbitrary Unmanaged Devices for Internet Access
  - Corporately-Enforced Risk Management Controls
    - Filtered and Monitored Network Traffic
    - Separation between the Organisation's Corporate Network and the Guest Wi-Fi Network
    - Corporate Workstations Configured to Block Access to Unauthorised Devices
  - User-reliant Risk Management Controls
    - Anti-Malware Software
    - Avoid Behaviour that is Unauthorised, Excessive, Offensive or Unlawful
- Appendix B: Arbitrary Unmanaged Devices for Non-Sensitive Data
  - Corporately-Enforced Risk Management Controls
    - Segmentation and Segregation between Devices and Organisational Systems
    - Web Application and Operating System Vulnerability Assessment and Security Hardening
- Appendix C: Corporately Approved and Partially-Managed Devices for Sensitive Data
  - Corporately-Enforced Risk Management Controls

Unclassified kiosk

An art gallery wishes to use iPod touches as an interactive tour guide for Unclassified information at a specific site. The tour guide information is largely contained within a single app.

The gallery purchased an Enterprise Developer Agreement, and uses this to code-sign the app they have had developed by a contractor.

The gallery set up a Wi-Fi network for the site, and uses a provisioning computer with Apple Configurator to supervise and then “lock to” their developed app. Devices can be deployed, managed and reset with minimal effort.

Unclassified (DLM) BYOD

An agency has decided to allow limited corporate network access to employee owned devices. Users are required to enrol their device in to the agency MDM and agree with an acceptable use policy.

The agency uses a 3rd party MDM server to enforce Configuration Profile restrictions and audit devices for compliance. Non-compliant devices have their MDM profile and associated managed apps and data revoked immediately. Configuration Profiles take advantage of the Managed Open-In function to prevent movement of documents from agency managed apps and email to user personal apps and email.

A Wi-Fi network is configured according to relevant ISM government system (G) controls is deployed on premise, permitting limited corporate network access via VPN and limited personal use through an authenticated proxy. Email is provided using the native iOS Mail app using Exchange Active Sync (EAS) over TLS.

PROTECTED with limited personal use

An agency has decided to issue iOS devices for work and limited personal use. The users require access to PROTECTED email and attachments as well as access to their PROTECTED intranet. The agency permits user installation of App Store apps subject to agreement with an acceptable use policy. Personal email is permitted using the iOS native mail app.

In this case, the agency uses an MDM server, a VPN concentrator for remote access, Exchange for email, a third party gateway filter and Apple Configurator to place devices in to supervised mode. The iOS devices use a client certificate for authentication to Exchange, and a client certificate is used for On-Demand VPN authentication. Configuration Profiles take advantage of the Managed

Open-In function to prevent movement of documents from agency managed apps and email to user personal apps and email. The third party gateway filter is configured to implement protective markings on email sent from devices. A Wi-Fi network configured according to relevant ISM government system (G) controls is deployed on premise permitting corporate network access via VPN and limited personal use through a authenticated proxy.

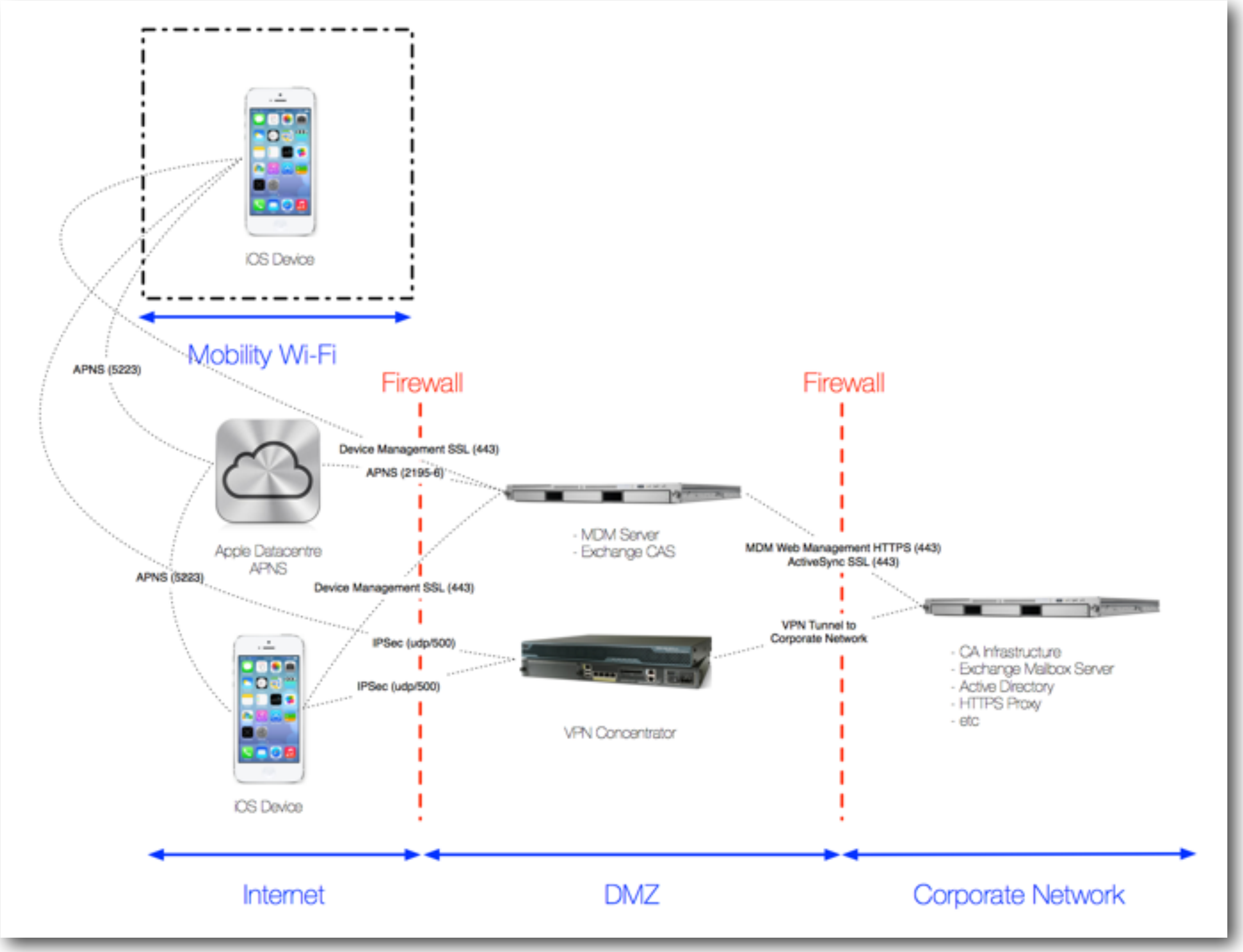


Figure 10.1: Example network diagram for limited personal use

PROTECTED business only

An agency has decided to issue iOS devices for their mobile fleet. Their users require access to their PROTECTED email and attachments, as well as access to a PROTECTED intranet.

The IT team will use Apple Configurator to configure the devices before they are issued to users. The devices will be configured as supervised devices and will be pre-enrolled with the agency's MDM server.

The devices connect to the agency's exchange server using a client certificate for authentication. The IKEv2 VPN is configured as "Always On" with certificate authentication; this forces all traffic over the VPN. Access to internal web resources on the corporate intranet is allowed through an authenticated proxy.

The agency requires all users to sign an acceptable use policy that requires them to install OTA updates when they are available. Compliance will be monitored by the IT team using the MDM.

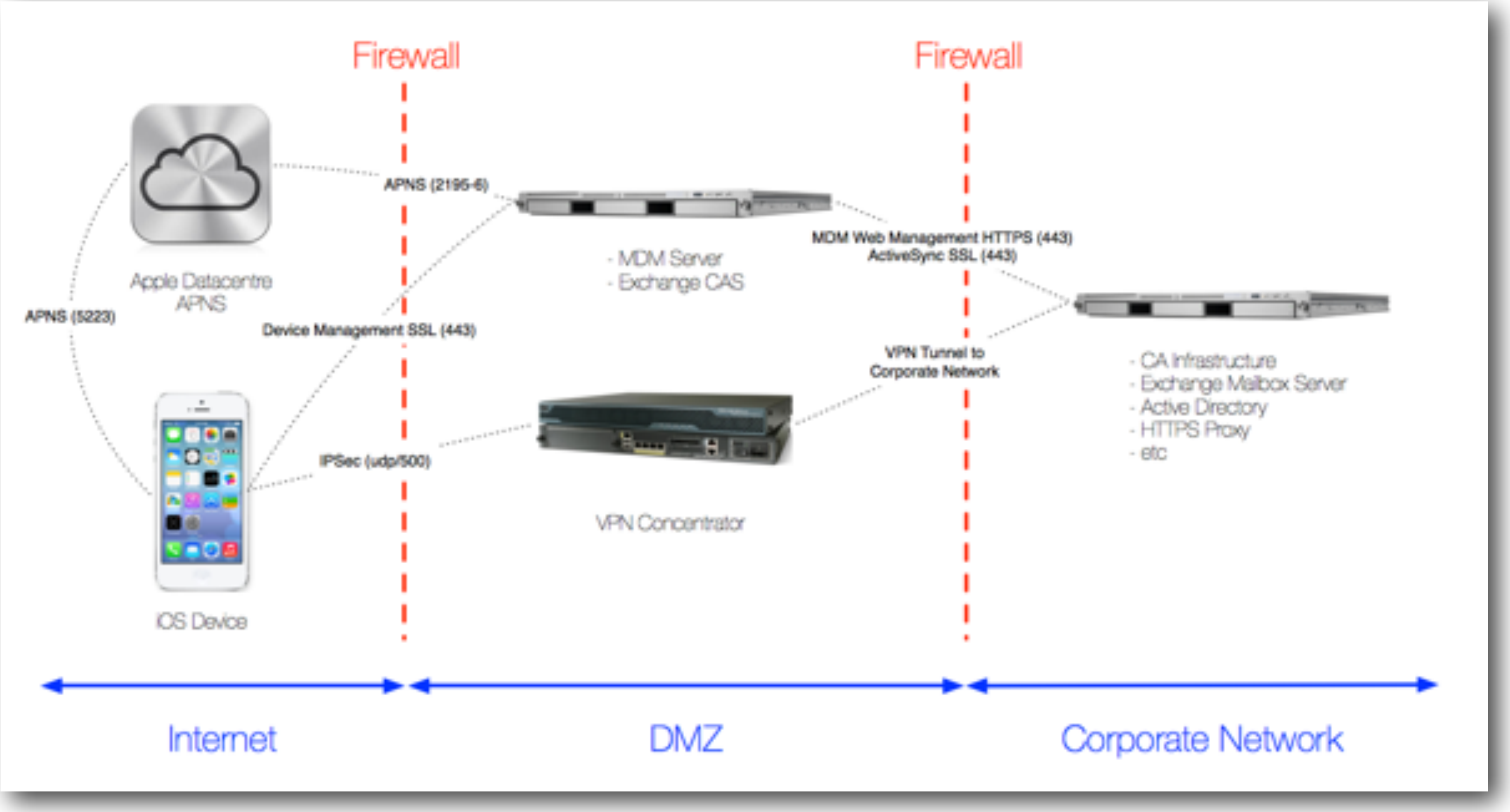
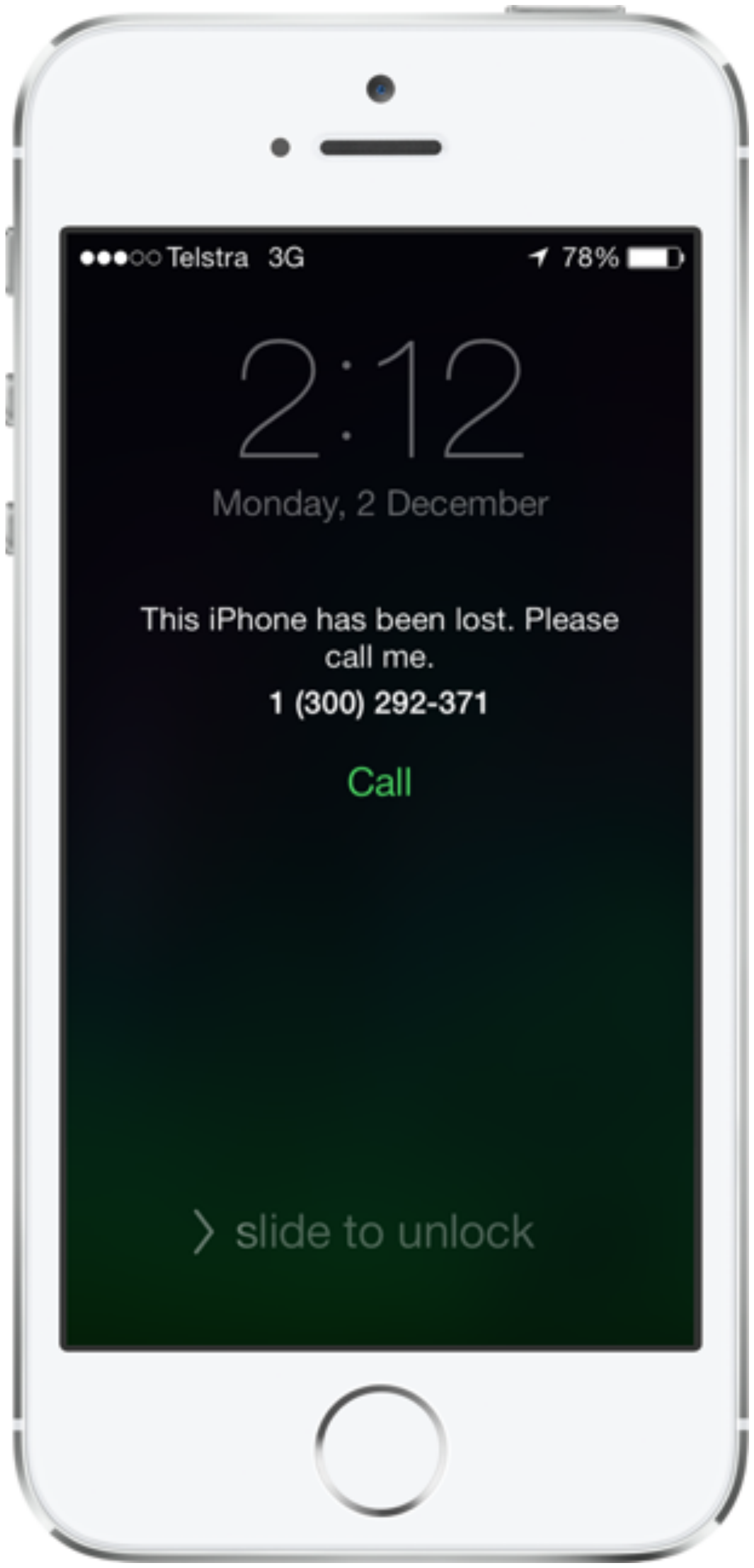


Figure 10.2: Example network diagram for limited personal use

CHAPTER 11

Risk Management Guide



This iPhone has been lost. Please call me.

1 (300) 292-371

This chapter provides a guide to typical risks associated with mobile devices and recommended mitigation measures.

Australian Government Information Security Manual (ISM)

This chapter should be read in conjunction with the ISM, available from the ASD website:

http://www.asd.gov.au/infosec/ism/

Currently, not all ISM requirements can be implemented on iOS 8 devices. Risk mitigation measures are provided in this chapter for such cases.

Mobile Device Risks

Typical risks, the recommended mitigation measures and the pre-conditions for those mitigation measures are covered in the table below. There are several residual risks in ISM policy that cannot be completely mitigated by technical controls. Agencies will need to assess, accept and manage any residual risks and develop appropriate policy guidance.

iOS does not have a local firewall. This is partially mitigated by agency firewalls, and significantly mitigated by the sandboxed runtime environment in iOS.

iOS allows the user to deliberately connect to an untrusted Wi-Fi network. Note that iOS devices will not auto-connect to any unknown Wi-Fi network. The only mitigations available at this time are pre-configured settings, user education and AUP.

iOS allows the user to deliberately enable or disable the radio transceivers (e.g. Wi-Fi, Bluetooth) in the device - there is no method for a Configuration Profile to force a radio transceiver off. The only mitigations available at this time are user education, AUP or hardware modification (the latter being permanent).

Risk	Mitigation	Implied Preconditions
Device lost, still on network	Strong passcode, data protection enabled, local wipe, remote wipe, Find My iPhone/iPad.	Configuration Profiles, EAS or MDM Server in a network reachable location or iCloud account.
Device lost, off network	Strong passcode, local wipe, data protection enabled.	Passcode requirement via config profile
Device lost, casual access attempt	Strong passcode, local wipe, data protection enabled.	Passcode requirement via config profile, supervised to prevent pairing
Device lost, forensic access attempt without passcode knowledge	Strong passcode, local wipe, use of supervised mode, data protection enabled, app usage of appropriate data protection class.	Configuration Profiles, device running up to date iOS. Device in supervised mode.
Jailbreaking	Strong passcode, data protection enabled, use of devices with A5 or later processor, use of MDM console, use of supervised mode, MDM app or enterprise apps with “canary” code to detect and report jailbreaking, AUP should prohibit jailbreaking.	Jailbreaking from host computer when device passcode is known is still likely to be feasible, unless supervised mode is used.
Malicious runtime code	Code signing, memory and filesystem sandboxing, no-execute heap, disable user-added applications, do not jailbreak operational devices and (for App Store apps) the App Store review process.	In-house application development capability, CA infrastructure. May mitigate on lower security levels by “approved” lists and MDM monitoring as mitigation.

Table 11.1: Risk management guide

Risk	Mitigation	Implied Preconditions
Users cut and paste agency data into a public email account (e.g. Yahoo or Gmail) and send it from the device.	Disable the creation of separate email accounts, and restrict access to webmail via custom APN and agency proxy, disable screen shots on device via Configuration Profile, filter sensitive mail or attachments at the EAS gateway, use of VDI for sensitive email, contain agency email to a third party email app container.	Configuration Profiles, use of agency proxy. Note that any data that is displayed on the screen of any device can be photographed or video recorded by a camera, and sent via other means. This kind of leakage by deliberate action generally cannot be mitigated against for a mobile device.
Users cut and paste sensitive data from a managed app to an unmanaged app.	Ensure that managed apps take advantage of named pasteboards, disable use of copy paste through third party app wrapping. Explain risk of accidental disclosure of classified information via copy/paste in AUP.	Custom apps for named pasteboards/wrapping. For App Store apps, agencies can engage with developers directly to procure custom builds.
Untrusted devices connect to agency network.	Use of 802.1X NAC, IPSEC or TLS VPN, encrypted VDI.	Use of 802.1X with CA & NAC on Wireless, VPN on Demand with client certificates for agency network access, use of TLS reverse proxy for low security data.

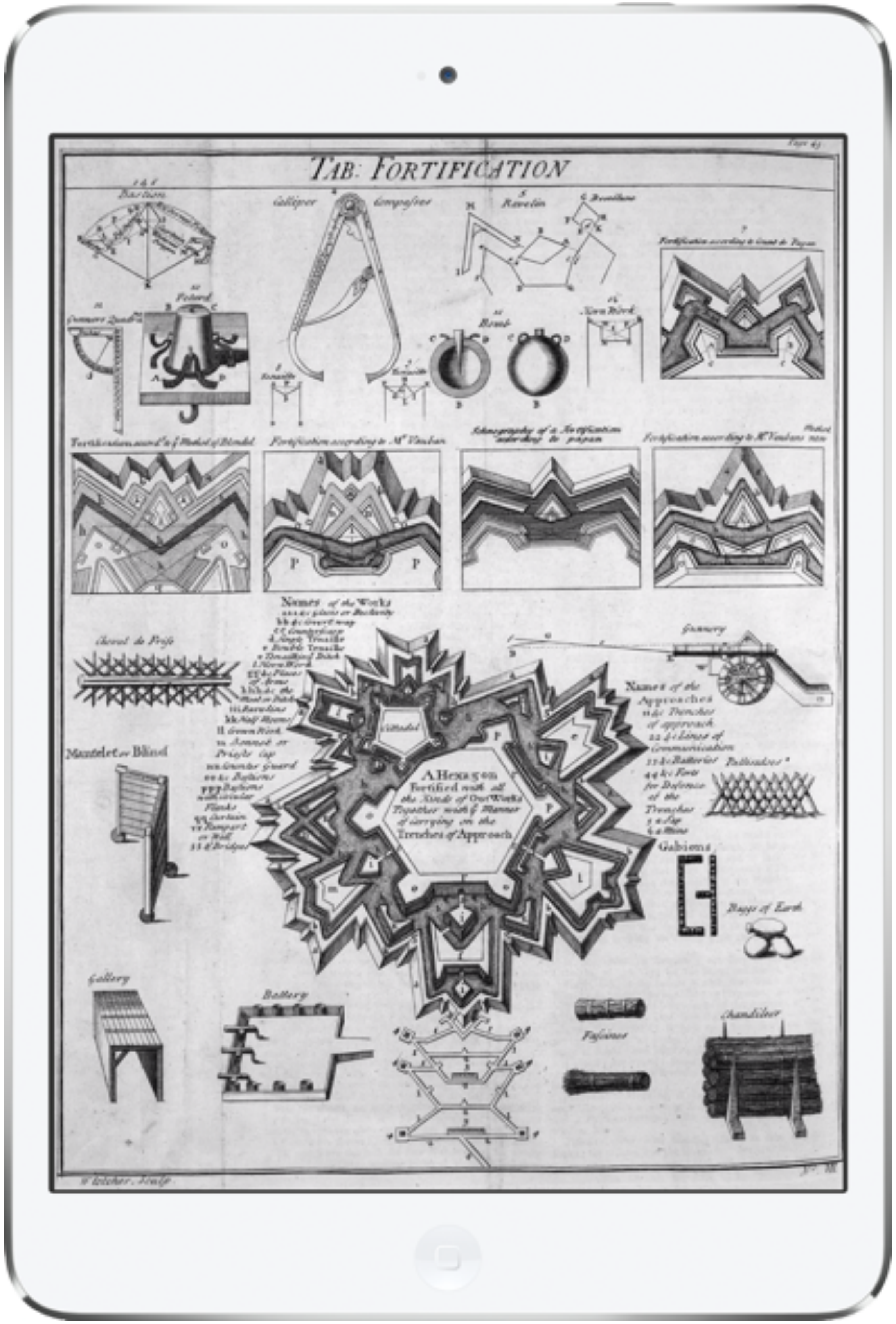
Table 11.1 (continued): Risk management guide

Risk	Mitigation	Implied Preconditions
Data compromise via host computer backup	Force encrypted backup profile restriction, user education, physical security of backup host. Prevent host pairing with supervised mode.	TLS CA infrastructure to sign and encrypt profiles into agency chain of trust.
Data compromise via Bluetooth	iOS allows a limited subset of Bluetooth profiles, depending on device, and specifically does not include file transfer related Bluetooth profiles. For included profiles see: http://support.apple.com/kb/HT3647	Apps that share information via Bluetooth not approved for use on devices where this vector is a concern.
Accidental disclosure of classified information via iMessage	Educate users of the risk of accidental disclosure of classified information via "Open-In" iMessage in AUP. Disable iMessage via Configuration Profile restriction.	That the risk of accidental disclosure of classified information via Open-In is greater than the utility of iMessage.
SMS message interception by hostile telecommunications infrastructure	Allow iMessage use via Configuration Profile.	Contact ASD to discuss particular user travel circumstances.

Table 11.1 (continued): Risk management guide

Chapter 12

Firewall Rules



Allow required iOS functionality while preserving the security of your network.

Firewall Rules

Several firewall rules may need to be implemented to allow correct functionality. Depending on what functionality is required from iOS devices, MDM servers and iTunes, several firewall rules may need to be implemented.

Firewall Ports

iTunes and iOS devices may need firewall rules adjusted, depending on the functionality required, or allowed, on an intranet. The main knowledge base articles describing ports required by Apple devices are given below, with a summary around iOS and iTunes in Table 12.1 (below):

http://support.apple.com/kb/TS1379

http://support.apple.com/kb/TS1629

Destination host name	Destination IP	Port	Reason
ocsp.apple.com	17.0.0.0/8	443	Online Certificate Status for code signing certificates
crl.apple.com	17.0.0.0/8	443	Certificate Revocation List for codesigning certificates
gateway.push.apple.com	17.0.0.0/8	2195	Apple Push Notification Service
feedback.push.apple.com	17.0.0.0/8	2196	Apple Push Notification Service
phobos.apple.com	17.0.0.0/8	80, 443	iTunes Store, Device activation
itunes.apple.com	17.0.0.0/8	80, 443	iTunes Store, Device activation
deimos.apple.com	17.0.0.0/8	80, 443	iTunes U
deimos3.apple.com	17.0.0.0/8	80, 443	iTunes Music Store and album cover media servers.
ax.itunes.apple.com	17.0.0.0/8	80, 443	iTunes Store, Device activation
gs.apple.com	17.0.0.0/8	80, 443	iTunes Store, Device activation
albert.apple.com	17.0.0.0/8	80, 443	iTunes Store, Device activation
ax.init.itunes.apple.com	17.0.0.0/8	80, 443	Device activation
evintl-ocsp.verisign.com	199.7.55.72	80, 443	Digital signature verification for iTunes content
evsecure-ocsp.verisign.com	199.7.55.72	80, 443	Digital signature verification for iTunes content
a1535.phobos.apple.com	17.0.0.0/8	80, 443	iTunes Music Store and album cover media servers.

Table 12.1: Firewall rules.