Australian Government

Department of Defence
Intelligence and Security

PROTECT

iOS Hardening Configuration Guide

FOR iPOD TOUCH, iPHONE AND iPAD RUNNING iOS 4.3.3 OR HIGHER

June 2011

iOS Hardening Configuration Guide

For iPod Touch, iPhone and iPad iOS 4 devices running iOS 4.3.3 or higher.

June 2011

About this Guide

This guide provides instructions and techniques for Australian government agencies to harden the security of iOS 4 devices.

> ***Important:*** *This document does not constitute a DSD certification or formal evaluation of iOS.*
>
> *At this time, DSD does not recommend iOS for use at the PROTECTED/RESTRICTED level. This guide is intended for use at UNCLASSIFIED and UNCLASSIFIED IN-CONFIDENCE.*
>
> *Agencies choosing to use iOS devices for RESTRICTED/PROTECTED information must obtain a dispensation in accordance with the Australian Government Information Security Manual (ISM).*
>
> *Implementing the techniques and settings found in this document can affect system functionality, and may not be appropriate for every user or environment.*

iOS Evaluation

Due to the high level usage of iOS devices in government, DSD is working closely with Apple in its evaluation of Apple iOS. At that time DSD will advise on the suitability of Apple iOS to protect information up to RESTRICTED/PROTECTED level.

iOS and the Australian Government Information Security Manual

This guide reflects policy specified in the ISM. Not all ISM requirements can currently be implemented on iOS 4 devices. In these cases, risk mitigation measures are provided (see Appendix E).

Chapter Five provides recommended passcode settings for iOS devices. This advice has been developed based on an assessment of security risks related specifically to iOS 4, and takes precedence over the non-platform specific advice in the ISM.

About the Defence Signals Directorate

As the Commonwealth authority on the security of information, the Defence 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 www.dsd.gov.au

Audience

This guide is for users and administrators of iOS 4.3.3 or later devices. These devices include the iPod Touch, iPhone and iPad.

To use this guide, you should be:

- familiar with basic networking concepts;
- an experienced Mac OS X or Windows administrator: and
- familiar with the Mac OS X or Windows interface.

Parts of this guide refer to features that require the engagement of the technical resources of your telephony carrier, firewall vendor, or Mobile Device Management vendor. While every effort has been made to ensure content involving these third party products is correct at the time of writing, you should always check with these vendors when planning an implementation.

Additionally, 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 could cause serious effects to the device, your network and your agency’s security posture. These instructions should only be used by experienced administrators, and should be used in conjunction with thorough testing.

Finally, for further clarification or assistance, IT Security Advisors of Australian government agencies can consult the Defence Signals Directorate by contacting emailing assist@dsd.gov.au or the DSD Cyber Hotline on 1300 CYBER1 (1300 292 371).

What is in this Guide

This guide can assist you in securing an iOS 4 device. It does not attempt to provide comprehensive information about securing computers and servers.

This guide includes the following chapters:

Note: *Because Apple periodically releases new versions and updates to its software, images shown in this book may vary from what you see on your screen.*

Using this Guide

The following list contains suggestions for using this guide:

- Read the guide in its entirety. Subsequent sections build on information and recommendations discussed in prior sections.
- The instructions in this guide should always be tested in a non-operational environment before deployment. This non-operational environment should simulate, as much as possible, the environment where the device will be deployed.
- This information is intended for mobile devices running iOS 4. Before securely configuring a device, determine what functions that device needs to perform, and apply security configurations to the device or supporting infrastructure where applicable.
- A security checklist is provided in the appendix to track and record the settings you choose for each security task and note what settings you change to secure your iOS device. This information can be helpful when developing a security standard within your agency.

Important: *Any deviation from this guide should be evaluated to determine security risks and take measures to monitor or mitigate those risks.*

Getting Additional Information

Note: Documentation and advice is periodically updated by both DSD and relevant vendors. DSD recommends that agencies review revised help pages and new editions of guides.

For security-specific information, consult the following:

- DSD *Information Security Manual* http://www.dsd.gov.au/infosec/ISM.htm —DSD provides information on securely configuring proprietary and open source software to Australian Government standards. Additional information for Australian government agencies, contractors and IRAP assessors, is available from DSD's "OnSecure" portal http://members.onsecure.gov.au
- NSA security configuration guides (www.nsa.gov/snac/)—The US National Security Agency provides a wealth of information on securely configuring proprietary and open source software.
- NIST Security Configuration Checklists Repository (checklists.nist.gov/repository/category.html)— is the US National Institute of Standards and Technology repository for security configuration checklists.
- *DISA Security Technical Implementation Guide* (www.disa.mil/dsn/policies.html)— is the US Defense Information Systems Agency guide for implementing secure government networks. A US Department of Defense (DoD) PKI Certificate is required to access this information.
- CIS Benchmark and Scoring Tool (www.cisecurity.org/bench_osx.html)—The Center for Internet Security benchmark and scoring tool is used to establish CIS benchmarks.
- Smart Card Services Project (smartcardservices.macosforge.org)—The Smart Card Services Project provides instructions for implementing smart cards in Apple's Common Data Security Architecture (CDSA).

For further information consult the following resources:

- Apple Product Security website (www.apple.com/support/security/)—access to security information and resources, including security updates and notifications.

- An RSS feed listing the latest updates to Snow Leopard Server documentation and on screen help is available. To view the feed use an RSS reader application: feed://helposx.apple.com/rss/snowleopard/serverdocupdates.xml

- Developer documentation is available from developer.apple.com/iphone. Registered developers get access to WWDC session videos and PDF documents. Free registration allowing access to documentation and developer SDK is available.

- Apple Product Security Mailing Lists website (http://lists.apple.com/mailman/listinfo/security-announce)—mailing lists for communicating by email with other administrators about security notifications and announcements.

- iPhone, iPad and iPod Touch manuals (http://support.apple.com/manuals) —PDF versions of all product documentations.

- iPhone, iPad and iPod Touch user guides - available as HTML5 web applications that work offline on the devices (http://help.apple.com/iphone, http://help.apple.com/ipad, http://help.apple.com/ipodtouch).

- iPhone in Business website (http://www.apple.com/iphone/business/integration/)—reference point for all enterprise related documentation for iOS integration.

- Apple Developer Website (http://developer.apple.com) registration required, contains extensive information on enterprise deployment of iOS devices, developer documentation on APIs and programming techniques for both web based and native iOS applications.

- iOS Enterprise Deployment Articles - (http://developer.apple.com/library/ios/) – provides a detailed reference on a variety of enterprise deployment themes. These can be found in the iOS Developer Library under the “Networking & Internet” – “Enterprise Deployment” topic.

- Apple Discussions website (http://discussions.apple.com)—a way to share questions, knowledge, and advice with other administrators.

- Apple Mailing Lists website (http://www.lists.apple.com)—subscribe to mailing lists so you can communicate with other administrators using email.

- Open Source website (http://developer.apple.com/opensource/)—access to Darwin open source code, developer information, and FAQs.

Chapter One

Introduction to Mobile Device Security Architecture

Mobile devices face the same security challenges as traditional desktop computers, but their mobility means they are also exposed to a set of risks quite different to those of a computer in a fixed location.

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 specific features available in iOS 4. Not all of these options discussed will be exercised in 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 as to 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[1];
- certain infrastructure supporting mobile devices can be trusted; and
- carrier infrastructure cannot always be trusted as secure in all countries.

[1] Although GSM for example is encrypted on some carrier networks, it is not encrypted on all, and some of the GSM encryption algorithms such as A5/1 on 2G networks are vulnerable to attack with rainbow tables. With moderate resources, it is also feasible to execute a MITM attack against GSM voice and have the MITM tell client devices to drop any GSM encryption.

Device Security off the Network

Once a device is off the data network, then 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 a remote wipe command, if there is no network present.

When off the network, the security of the device is determined by:

- what policy has been cached locally from Exchange ActiveSync (EAS) or Configuration Profiles;
- what the security settings set locally on the device are;
- the device's cryptographic capabilities; and
- the strength of the device passcode.

In addition, the device should have been restored to iOS 4 to enable all data protection filesystem features when the passcode is enabled.

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 cryptographic fundamentals section in 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:

- SSL to encrypt connections to specific hosts such as mail servers or management servers that need to be highly reachable;
- SSL for any traffic that has sensitive data on it;
- 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;
- a custom, authenticated APN[2] in conjunction with Carriers to compartmentalise 3G data traffic to defined security domains; and
- data at rest encryption on mobile devices and servers they connect to.

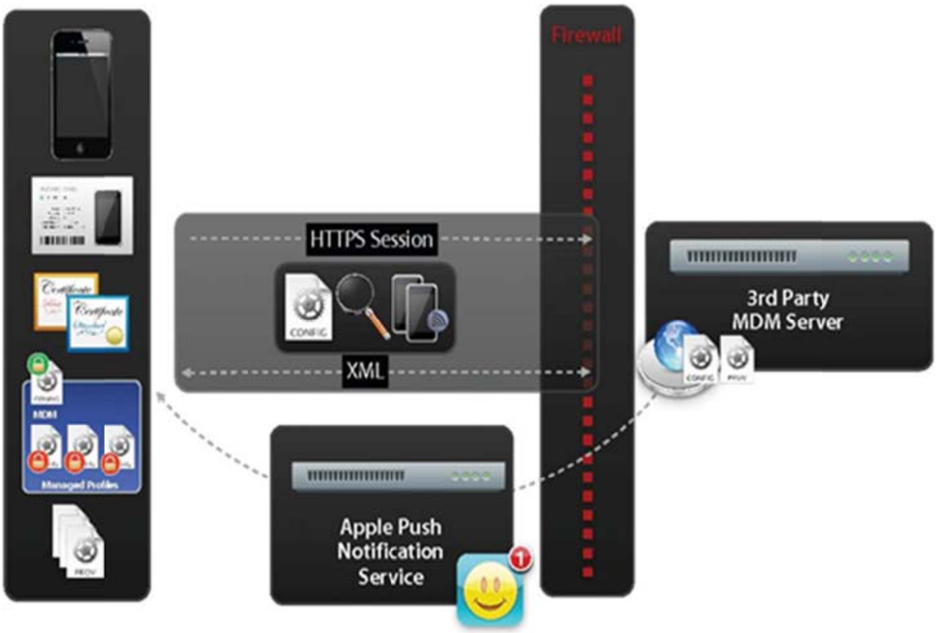
Apple Push Notification Service

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

Examples of apps that may use APNS include push email notification, Mobile Device Management (MDM) servers, and iOS client/server applications that are able to execute in the background (e.g. VOIP apps, streaming audio apps, or apps that need to be location aware). When APNS is used by an MDM server, it is a simple ping to the MDM agent on the device to "phone home" to its parent MDM server instance, and exchange XML queries and responses inside an SSL tunnel.

[2] Access Point Name (APN) See your carrier for more detail.

The firewall rules applied to the devices, APN subnet, and VPN subnet, as well as the EAS, MDM server in the DMZ, should allow access to the APNS for these services to work.



Data Roaming

Data roaming generally refers to a process by which a device from a specific carrier's network can take advantage of the data service on a different carrier. For example a device with a SIM from an Australian carrier, being used in the US on a US carrier's network and taking advantage of the carrier's data infrastructure. Note that roaming need not be international; in some countries carriers with different coverage areas may allow some data roaming to avoid infrastructure duplication.

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 often not subject to privacy and consumer protection requirements in the same way as purely domestic communications in the host country. It is incorrect to assume that 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 consoles, or MobileMe's "Find My iPhone". In some cases, private data APN can be preserved across international boundaries because of commercial arrangements between carriers - note that data costs can still be high.

Apps

One of the major attractions of the iOS platform is the availability of a wide range of Apps, and ease of App development. As outlined in DSD's *Strategies to Mitigate Targeted Cyber Intrusions*, DSD recommends that only applications that are required should be installed. There are four main 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. These Apps are loaded to a device either over-the-air (OTA) from the App Store itself, or the via the iTunes application on the host computer for the iOS device. Apple maintains discretionary control of curating App Store content, and can remove applications for a variety of reasons. It may be appropriate to restrict the use of Apps to only ones that have been tested and approved for use within an agency. Although App store applications come from a curated environment, and the runtime environment the Apps execute in is a relatively hardened one, agencies should assess the risk in allowing unrestricted user initiated installation of applications. Approaches to managing risks around these considerations are covered later in this document.
- **Ad Hoc**. Limited deployment (up to 100) instances of Apps can be installed on devices via USB tether, iTunes on the host computer, or iPhone Configuration Utility, using an Ad Hoc provisioning profile and a compiled, signed application binary. 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.
- **Enterprise In-House Apps**. Agencies with a Dun and Bradstreet Data Universal Numbering System (DUNS)[3] 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, which are for distribution only to their employees and contractors (i.e. not to the general public). Applications can be installed over-the-air via a web site, or over USB tether via the iTunes application instance on a host computer, or iPhone Configuration utility. These Apps are digitally signed, and the expiration of the provisioning profile controls the App "use-by date". Enterprise In-House Apps should include a method to authenticate the App, for use on the device.
- **Web Apps**. Safari Mobile has extensive support for HTML5, CSS3 and JavaScript features for Web Apps, including ones that run full screen and offline. The Product Guides for iPod Touch, iPhone and iPad are all examples of these. Web Apps are 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.

GSM Voice and SMS/MMS Communication

As noted above, GSM voice and SMS networks have a number of security weaknesses, where the security or authenticity of a voice or SMS communication cannot always be

[3] DUNS is a unique nine digit number assigned to business by Dun and Bradstreet. See www.dnb.com for more information.

ensured, due to both ‘Man-in-the-Middle’ attacks and the variation in the security features implemented by carriers. As such, voice and SMS communication should generally be considered less secure than methods that implement a chain of trust back into a user’s own agency such as SSL tunnelled email.

iTunes

iTunes is the cornerstone application required for management of iOS devices. It is not possible to deploy iOS devices within an agency without considering how iTunes will be used as part of the device management workflow. iTunes can be locked down for use in agency Standard Operating Environments (SOE)s via registry keys or XML property lists as detailed here:

http://developer.apple.com/library/ios/#featuredarticles/FA_Deploying_iTunes/Introduction/Introduction.html

One of the strategic decisions around iOS management is how access to iTunes is provisioned as part of the device lifecycle. There are three common options:

- use of iTunes in a locked down mode inside the Agency’s desktop SOE;
- provision of iTunes Kiosks for device activation and OS updates; and
- users sync and backup devices to personal computer, outside of the desktop SOE.

iTunes Accounts

One of the organisational risks that some users express concern about is a perceived need to associate a credit card with every iTunes account. 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 iTunes credentials as part of the process of submitting to the agency Acceptable Use Policy (AUP). If users then purchase approved applications, using their own credit card, they can be reimbursed. This provides one method to control expenditure of agency funds. A Mobile Device Management (MDM) console can be used to monitor what applications have been installed.
- For an agency device model, where users are not allowed to install their own Apps, per device iTunes accounts 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: the end user requires the iTunes account password in order to enable application updates.
- iTunes accounts can be optionally used to create free MobileMe accounts to facilitate user initiated device location and remote wipe.
- The most restrictive approach is to not reveal the iTunes account password to the end users, and install App Store Apps prior to issue of the device to the end user. A

configuration profile would be used to lock out any further updates. However, to update these devices, there is an additional support load, as updates must be done by IT staff. This approach is recommended for small controlled deployments only.

- In-House developed applications can be deployed either by iTunes, or over-the-air to devices, using a secure web site. In all the above cases, an MDM console allows monitoring of what App versions are installed on a device, allowing a management decision as to when updates are required. An MDM console can push a webclip to allow downloading of Enterprise In-House Apps out to a fleet of devices.

Planning Questions

The questions below offer a guide for considerations in implementing policy on the device.

Question	Comments/Selection
How sensitive is the data I am intending to view or store on a mobile device?	If there is any degree of sensitivity, then a strong passcode should be set on the device in order to enable data protection. If the data is coming over a network, then the data should be secured by some combination of encryption, typically SSL or VPN. If the data is classified refer to the ISM section Cryptography.
Is it appropriate that data gets to the device over a 3G data or wireless network?	If you have data that is within your control and must get to the device in a secure way, then USB tethering to a trusted computer may be an acceptable alternative.
Do I want users to collaborate using that data in a networked fashion?	If users need to share or collaborate with the data over the network, then a secure connection should be in place between the users collaborating.
Does my agency want to allow individually owned devices to access some agency data?	Allowing personally owned devices usually has a significant reduction in costs to do with both procurement and management of mobile device fleets, but introduces a different set of expectations about the level of control an agency can exert over the devices. The balance point between control and flexibility is usually different, and is more consultative in process, than for agency owned devices. An important point to remember is that classified information should not be retained on personally owned devices.
Does my agency want to allow a mixture of personal and agency owned devices?	If mixed device ownership is allowed, then consideration needs to be given as to what the differences in access to information and services are appropriate, if any. In some cases this could involve use of sandboxed applications to separate agency data from personal data.

Question	Comments/Selection
Does my agency need different policy applied to a device depending on if it is personally or agency owned?	This is a complex issue that requires a mixture of user initiated opt-in Configuration Profiles, MDM managed profiles and pre-installed profiles on a per device basis, appropriate to its context. In some cases this could involve use of sandboxed applications to risk manage the separation of agency data from personal data.
What balance does my agency need to set between the advantages of users being able to install App Store apps themselves, versus the overhead of managing this centrally?	The more sensitive the data being accessed by a device, the risk is increased. Typically a combination of an approved whitelist and monitoring via MDM will mitigate the risks. At high levels of sensitivity, applications may need to be pre-screened, and pre-loaded by IT prior to device issue, or developed in-house and deployed to devices.
Do my agency's acceptable usage policies require explicit education and enforcement?	AUP compliance prior to devices being deployed is critical. AUP education content can be provided as a Web App and Web Clip on the devices for user reference. Other policy controls via EAS, MDM and Configuration profile may be required.
Are all of my devices with one carrier, and agency owned?	If you have single billing arrangement with a carrier, then use of a custom, secured APN, with a proxy, can assist in enforcing tighter policy controls for devices on the 3G data network. In many cases, a custom APN with an EAS and an authenticated, SSL encrypted reverse proxy may be sufficient security for low level sensitivity data.
Do I need to support devices from multiple carriers and a mix of personal and agency ownership?	A VPN solution may be more appropriate than a custom APN.
How can an agency remote wipe devices or secure containers whenever they are reachable on the network?	Remote wipe is usually best managed by a combination of EAS or an MDM console. If your agency does not have a 24/7 service desk capability, then use of OWA or MobileMe can allow user-initiated remote wipes.
To what level does the agency care about its data being monitored and recorded by a third party?	Use of SSL,Wi-Fi encryption, and VPN needs to be considered as per ISM guidelines.

Question	Comments/Selection
How does an agency develop applications that are customised to its environment and needs to make the users more productive and better informed when they are mobile, away from their desks?	In-house application development needs to be done in either HTML5/CSS3/Javascript, or native applications code signed with an Enterprise Developer Agreement. Native apps, and Web Clips to web applications can be pushed OTA to devices that are under the control of an MDM server.
Does access to my agency information need to be pervasive?	If access to agency data is primarily appropriate on a site or campus, then potentially, focus on Wi-fi security, and limit agency data access, such as EAS PIM, or limited web site access via a reverse SSL proxy.
Do I need to be able to locate devices remotely?	Use of Mobile Me or an MDM that provides this in its on-device App.
Do I need to digitally sign email (e.g. S/MIME or PGP) ?	In iOS 4.3.3 Mail app does not support PGP or S/MIME, however third party solutions that support S/MIME are available as Apps e.g. Good for Enterprise.

Chapter Two
Installing iOS 4

This chapter is provided to help agencies ensure that their iOS 4 devices are configured in a way that enables the full set of data protection capabilities in iOS.

Data Protection

iOS 4 introduces a new system for data protection at rest, that takes advantage of the hardware cryptographic module in recent iOS devices. This minimises the impact of encryption on CPU load and battery life. Data protection is enabled by setting a passcode on the device.

If a device is new and shipped from the factory with iOS 4 pre-installed, then no action other than setting a passcode needs to be taken from this chapter.

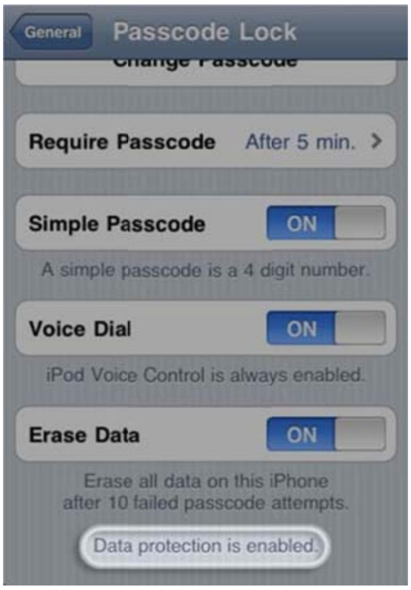
If there is no requirement for data to be retained on a device, then simply performing a restore of iOS 4, and then setting it up as a new device with a passcode will enable data protection.

If there is data on a device, then the procedure in the Apple Knowledge Base articlehttp://support.apple.com/kb/HT4175 should be followed in order to ensure that data protection is enabled.

Note: *iPhone 3, and iPod Touch (Second Generation) are capable of running iOS 4, but do not have the hardware cryptographic module. These older devices should be used in less sensitive roles, or third party solutions that put an encrypted container on the device independent of iOS features, such as Good Enterprise or Sybase Afaria.*

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. A Mobile Device Management console can query and report centrally as to if data protection is enabled on a device. The user of a device can also validate if data protection is enabled by going to Settings -> General, -> Passcode Lock and scroll to the bottom on the screen. If data protection is enabled, “Data protection is enabled” will be displayed at the bottom of the screen.



Passcode Lock

Change Passcode

Require Passcode After 5 min. >

Simple Passcode ON

A simple passcode is a 4 digit number.

Voice Dial ON

iPod Voice Control is always enabled.

Erase Data ON

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

Data protection is enabled.

iOS device with data protection enabled

Setting a Passcode

The last step in activating data protection is to set a passcode. In most environments enabling a passcode will form part of agency policy, and this will be enforced either over Exchange ActiveSync, or via a configuration profile installed on the device. For ISM password policies see Access Controls.

Data Protection Classes

Agencies should consult with App developers as to what data protection classes their application selects for data and authentication credentials. Apple provides extensive documentation on the data protection APIs on its developer web site, and in WWDC Session videos on 'iTunes U'. WWDC 2010 Sessions 204 and 209 are the most relevant in this area. In addition, WWDC 2009 Session 625 will be of interest.

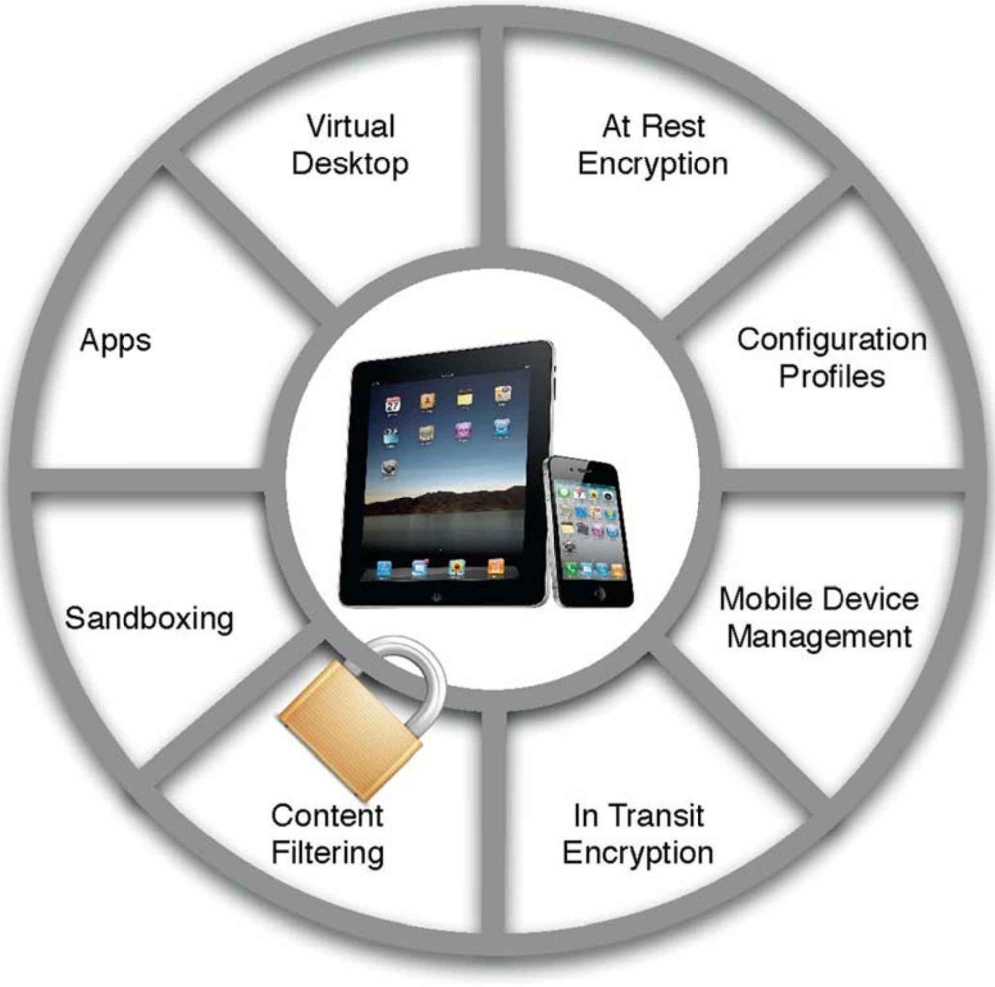
Chapter Three

Security Features and Capabilities

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

Mobile Device Security Toolbox

When setting up a secure system that uses mobile devices, the security tools and solutions are not on a linear scale, where a solution to a higher security environment is provided by one product alone. Rather, the security posture of the devices can be progressively improved by combinations of capabilities shown below.



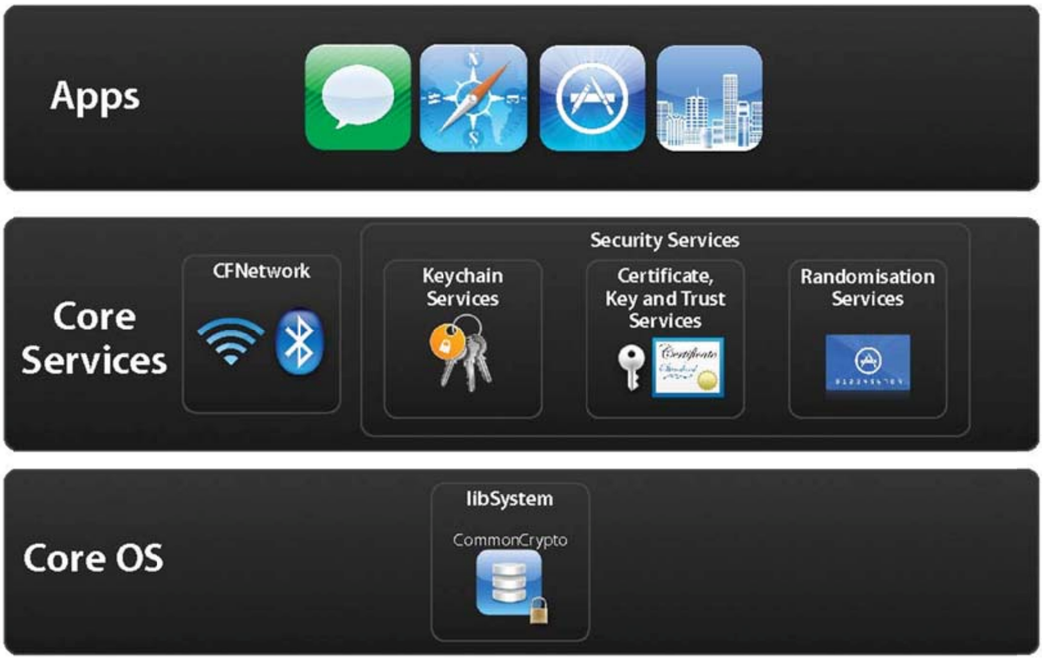
Security Features and Capabilities

Security features in iOS

iOS provides a number of features that enable:

- management of credentials and passwords with Keychain;
- encryption of data in transit (using DACA[4] and DACP[5]);
- encryption of data at rest and in transit (using DACA and DACP);
- digital signatures, certificates and trust services;
- randomisation services; and
- Code Signing Applications can leverage these services providing capabilities beyond the baseline implemented in iOS. Any Enterprise In-House Applications developed for an agency should generally take advantage of these services, rather than re-inventing the same capabilities. More information is available in detail from the Apple Developer web site:

http://developer.apple.com/library/ios/#documentation/Security/Conceptual/Security_Overview/Introduction/Introduction.html



Security Services in iOS

iOS 4.2.1 introduced no-cost “Find My iPhone” functionality for iOS devices. This allows a MobileMe account to use the “Find my iPhone/iPad” functionality, with a free MobileMe account, rather than full MobileMe subscription. User level setup information is included in the URL below:

http://www.apple.com/iphone/find-my-iphone-setup/

[4] DSD Approved Cryptographic Algorithm

[5] DSD Approved Cryptographic Protocol

Find My iPhone user interface

Generally, when agency devices are used, this MobileMe account would be the same as the iTunes account used to install agency owned apps, and set up prior to issuing the device. Note that this requires a network connection, location services to be active, and the device to have opted in to the "Find my iPhone" service.

Virtualisation

Some agencies may opt to present some agency applications to iOS devices over a network via a Virtual Desktop Infrastructure (VDI), such as Citrix Receiver (e.g. http://www.citrix.com/ipad) or VMWare View.

This works particularly well for users who are "micromobile" i.e. they move about a building or a campus during their work day, and able to take advantage of the relatively high bandwidth of a secure Wi-Fi network, but are not strictly away from the office location. Solutions in this space (such as Citrix XenApp version 6) provide an ability to tune the application UI for a small screen suitable for presenting to mobile devices, rather than merely presenting a remote session to the standard agency desktop resolution. Due to dependency on network performance and differences in screen sizes and input device sizes, VDI based solutions should be thoroughly tested from a usability perspective. This approach also has the advantage that minimal agency data is stored on the device.

Note *most major authentication token vendors have a soft token available for iOS.*

Note *that in some cases use of VDI is a classic usability/productivity trade off against security, as the absence of locally cached data means users are not able to be productive when the device is off the network, there is no integration with native applications running locally on the end point device.*

Sandboxing

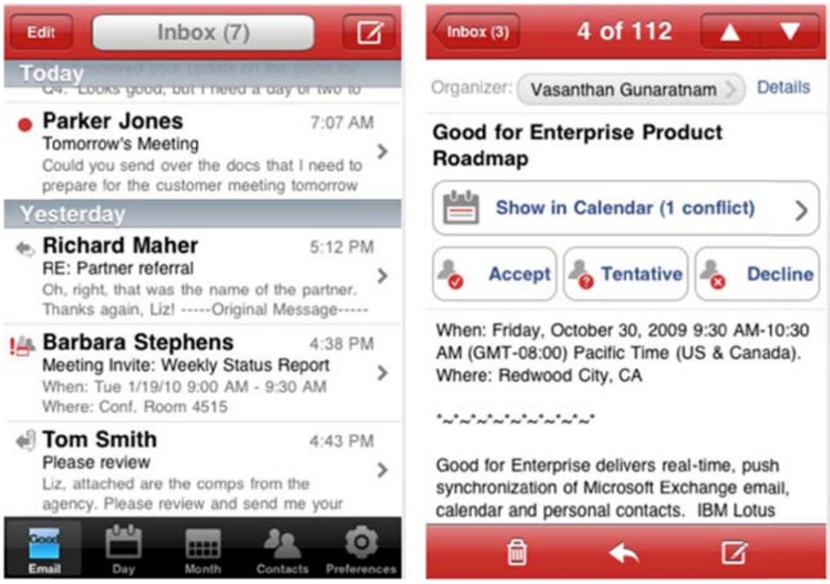
In iOS, all applications are sandboxed, with the kernel enforcing mandatory access controls, and applications being highly restricted in how they can share data.

Apple ships iOS 4 with the Mail App configured to store mail messages and attachments in the strongest data protection –class – where each file is encrypted with a unique key, and is only able to be decrypted when the device is unlocked. Address book and calendar information is currently allowed to be decrypted when the device is locked (to support caller ID and event notifications).

If a security posture is required where this level of sandboxing is insufficient, then in-house Apps, or third party solutions such as Sybase Afaria (http://www.sybase.com/afaria), Good for Enterprise (http://www.good.com) or LRW Pinecone (http://www.lrwtechnologies.com/pinecone.html) can be used to provide additional levels of sandboxing and policy enforcement for email, calendar and contact data, managed by dedicated servers.

There is usually a usability/security trade off in the configuration, with custom sandboxed solutions having a lower level of integration with other apps on the device (e.g. it may not be possible to take a photo with the device's camera, and then send via email is using the third party sandboxed email client).

***Note** that currently no third party sandboxed solution has been evaluated by DSD.*



Q4. Looks good, but I need a day or two to

Parker Jones 7:07 AM
Tomorrow's Meeting
Could you send over the docs that I need to prepare for the customer meeting tomorrow

Richard Maher 5:12 PM
RE: Partner referral
Oh, right, that was the name of the partner. Thanks again, Liz! -----Original Message-----

Barbara Stephens 4:38 PM
Meeting Invite: Weekly Status Report
When: Tue 1/19/10 9:00 AM - 9:30 AM
Where: Conf. Room 4515

Tom Smith 4:43 PM
Please review
Liz, attached are the comps from the agency. Please review and send me your

Organizer: Vasanthan Gunaratnam

Good for Enterprise Product Roadmap

When: Friday, October 30, 2009 9:30 AM-10:30 AM (GMT-08:00) Pacific Time (US & Canada).
Where: Redwood City, CA

~~*~*~*~*~*~*~*

Good for Enterprise delivers real-time, push synchronization of Microsoft Exchange email, calendar and personal contacts. IBM Lotus

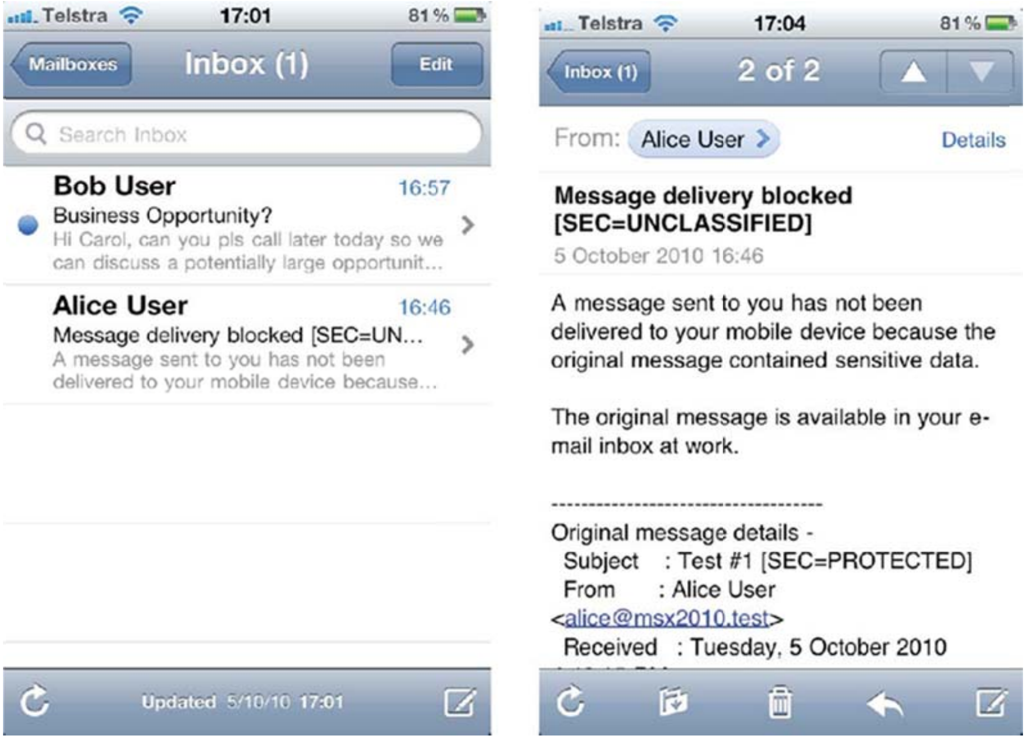
Good Enterprise App User Interface

Content Filtering

Access to intranet sites, and some mail, contact or calendaring data can be achieved via reverse proxies and content filters. There are multiple solutions in this space such as IIS from Microsoft, Mobile Access Server from Apple, and a wide variety of other solutions (e.g. from Cisco or F5 networks).

Filtering Exchange Active Sync data products such as JanusGATE Mobile (http://www.janus.net.au/janusGATE/Mobile) can be used to ensure email sent to Exchange ActiveSync devices has appropriate privacy markings for the classification the device is approved to by an agency. This approach can allow for an asymmetric strategy – mobile devices only receive email content at a classification appropriate to the device, as well as have 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, e.g. 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.



Bob User 16:57
Business Opportunity?
Hi Carol, can you pls call later today so we can discuss a potentially large opportunit...

Alice User 16:46
Message delivery blocked [SEC=UN...
A message sent to you has not been delivered to your mobile device because...

Message delivery blocked [SEC=UNCLASSIFIED]
5 October 2010 16:46

A message sent to you has not been delivered to your mobile device because the original message contained sensitive data.

The original message is available in your e-mail inbox at work.

Original message details -
Subject : Test #1 [SEC=PROTECTED]
From : Alice User <alice@msx2010.test>
Received : Tuesday, 5 October 2010

Example of Mail App interface when JanusGATE Mobile blocks email

Capability	Enablers	Comment
Remote Wipe	MDM, EAS, Apple Push Notification Service (APNS)	
Proxy	Custom APN, VPN	iOS 4.3.3 does not implement a global proxy setting. A proxy can be set on a custom APN and a VPN session.
Firewall	Firewall on Custom APN, Firewall on Wireless network.	iOS 4.3.3 does not implement a local firewall. This is significantly mitigated by the runtime environment.
Force Device Settings	iPCU 3.x, MDM	Enterprise Deployment Guide lists XML schema, this can be used to generate and sign profiles from custom scripts. iPCU is an easy to use GUI tool to generate the XML, but CA integration requires signing with OpenSSL tools.
Multi-factor Authentication	SSL CA infrastructure, DNS, RSA or CryptoCard (VPN Only), Smartcard (Requires Good Enterprise and Good Mobility Server)	Depending on the agency's security posture device certificates or soft tokens may be considered as a second factor of authentication.
OTA Configuration Profile (pull)	SSL CA infrastructure, DNS, Web Service, Directory Service	Externally sign & encrypt profiles, do not sign with iPCU.
OTA Configuration and Provisioning Profiles (push)	Enterprise Developer Agreement, 3rd Party MDM appliance, SSL CA infrastructure, DNS, Directory Service, APNS	MDM should be tied into CA and Directory Service.
Mobile Device Monitoring	Enterprise Developer Agreement, 3rd Party MDM appliance, CA infrastructure, DNS, Directory Service, APNS	MDM should be tied into CA and Directory Service.
Mobile Device Management	Enterprise Developer Agreement, 3rd Party MDM appliance, CA infrastructure, DNS, Directory Service, APNS	MDM should be tied into CA and Directory Service.
Remote Application Deployment	Enterprise Developer Agreement, Web Server, 3rd Party MDM appliance (optional), APNS (optional).	Only Enterprise In-House Apps can be deployed OTA.
Home screen		Set Home screen to "If found return to PO BOX XXXX". This could also be done with a Picture Frame Album.

Chapter Four

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.

> ***Note**: at the time of writing, iOS devices implement DSD Approved Cryptographic Algorithms and Protocols (and the implementations have been submitted for FIPS-140-2 certification), but have not yet completed a DSD Cryptographic Evaluation (DCE) conducted by DSD.*

In the absence of a DCE, use with PROTECTED and/or RESTRICTED content would require the agency head and accreditation authority, (typically an SES level staff member tasked with CISO responsibilities) to provide a dispensation for use. The ISM and agency security policy should be consulted directly for risk assessment and mitigation procedures in such use-cases.

If iOS devices are being considered for use at classifications above RESTRICTED/ 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 any dispensations as required by the ISM.

Feature	Unclassified	XX-in-Confidence	Restricted/Protected
Hardware Crypto iOS Devices	Agency's Decision	Recommended	Must
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	Must	Must	Must
iTunes Account	Personal or Agency	Personal or Agency	Personal or Agency
Sync to Content/Sync to iTunes Account.	Yes, if Personal iTunes	Generally no	Generally no

Feature	Unclassified	XX-in-Confidence	Restricted/Protected
Home Computer backup enforcement	Stated in agency usage policy.	Stated in agency usage policy.	Stated in agency usage policy.
MobileMe	Agencies need to assess the risk in their own situation.	Agencies need to assess the risk in their own situation.	Generally no, but “Find My iPhone” with free account may be possible.
User ability to install applications	Agencies need to assess the risk in their own situation.	Agency approved applications only. Recommend agency iTunes account. Consider MDM enforced Agency Store Apps whitelist.	Agency approved applications only. Recommend agency iTunes account. MDM enforced Agency Store Apps whitelist.
EAS	Recommended if Exchange or Lotus is used for agency email.	Recommended if Exchange or Lotus is used for agency email. Second factor of authentication using a certificate is preferred.	Possible, with 2 factor authentication. For some agencies a dedicated mail container may be preferable (e.g. Good for Enterprise or Sybase Afaria),or VDI could be used for email access.
EAS Filtering	Should be used if mobile device security domain is lower classification than intranet security domain.	Should be used if mobile device security domain is lower classification than intranet security domain.	Should be used if mobile device security domain is lower classification than intranet security domain.
Email secured independently of device passcode	Use a dedicated third party mail container.	Use a dedicated third party mail container.	Use a dedicated third party mail container.
MDM	Optional depending on role of device/scale of deployment.	Optional depending on role of device/ scale of deployment. Recommended if BYOD model used.	Recommended.
Custom APN for 3G data	Optional.	Recommended.	Recommended.

Feature	Unclassified	XX-in-Confidence	Restricted/Protected
VPN-on-Demand	Optional depending on role.	Recommended.	Recommended.
SSL Reverse Proxy	Optional depending on role.	Optional depending on role of device/ scale of deployment.	VPN-On-Demand recommended.
CA Infrastructure	Optional depending on role.	Recommended.	Required.

Chapter Five

Recommended Device Profile Settings

This chapter lists the profile settings that would typically be used when an iOS device is used on an Australian government network.

***Note** that if profiles are not being pushed by an MDM solution, the correct technique with Configuration Profiles is bundling the payloads in a way that:*

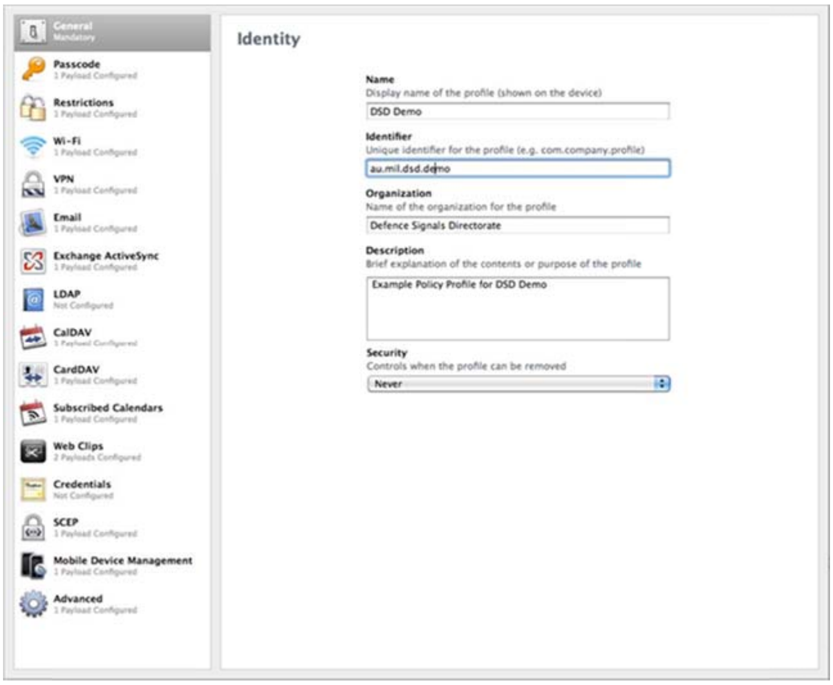
Profiles pulled to the device, bundle restrictions with authentication, so if the profile is removed, all access to agency resources is removed.

If MDM is used, the MDM master profile is always removable, but if it is removed all managed profiles are lost as well.

Pre-loaded Configuration Profiles and MDM managed profiles can be mixed on devices, but the MDM server cannot remove the profiles manually pulled to the device.

The following settings are a baseline for use on Restricted/Protected networks. Agency discretion can be used to vary to be more restrictive if required by local 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. iPhone Configuration Utility can be used to view the full range of profile setting that can be deployed.

General (non-Managed Profiles only):



Identity

Name
Display name of the profile (shown on the device)
DSD Demo

Identifier
Unique identifier for the profile (e.g. com.company.profile)
au.mil.dsd.demo

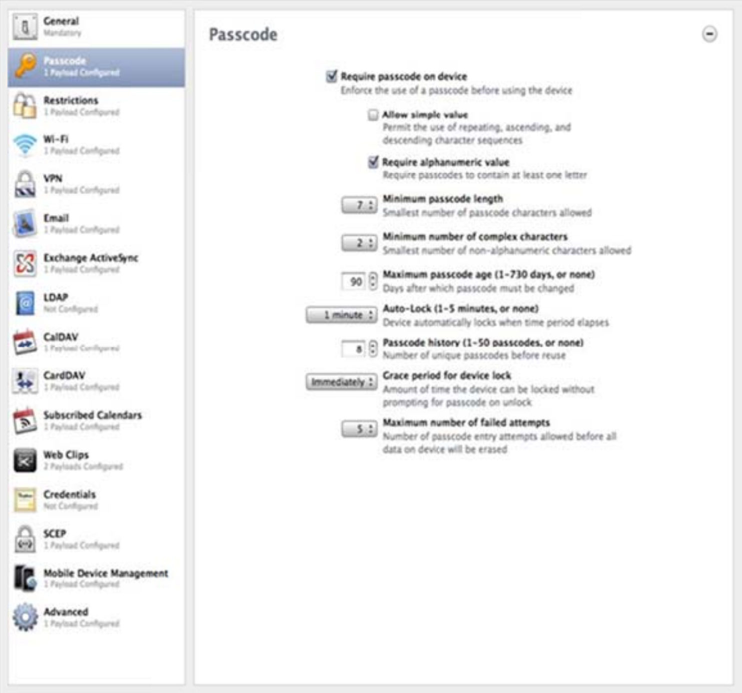
Organization
Name of the organization for the profile
Defence Signals Directorate

Description
Brief explanation of the contents or purpose of the profile
Example Policy Profile for DSD Demo

Security
Controls when the profile can be removed
Never

- Profile Security should be “Remove Always” if setting is for convenience for users that does not contain any 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 would usually be “Remove with Passcode” for profiles that you may want IT staff to remove temporarily. Generally users would not get the passcode to such profiles.
- Most profiles that are not MDM managed would be set to “Never”. The Passcode policy profile, if used, should be set to “Never”.

Passcode (can be set via EAS depending on version, OR Configuration Profile):



Passcode

☑ Require passcode on device
Enforce the use of a passcode before using the device

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

☑ Require alphanumeric value
Require passcodes to contain at least one letter

7 Minimum passcode length
Smallest number of passcode characters allowed

2 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

1 minute Auto-Lock (1-5 minutes, or none)
Device automatically locks when time period elapses

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

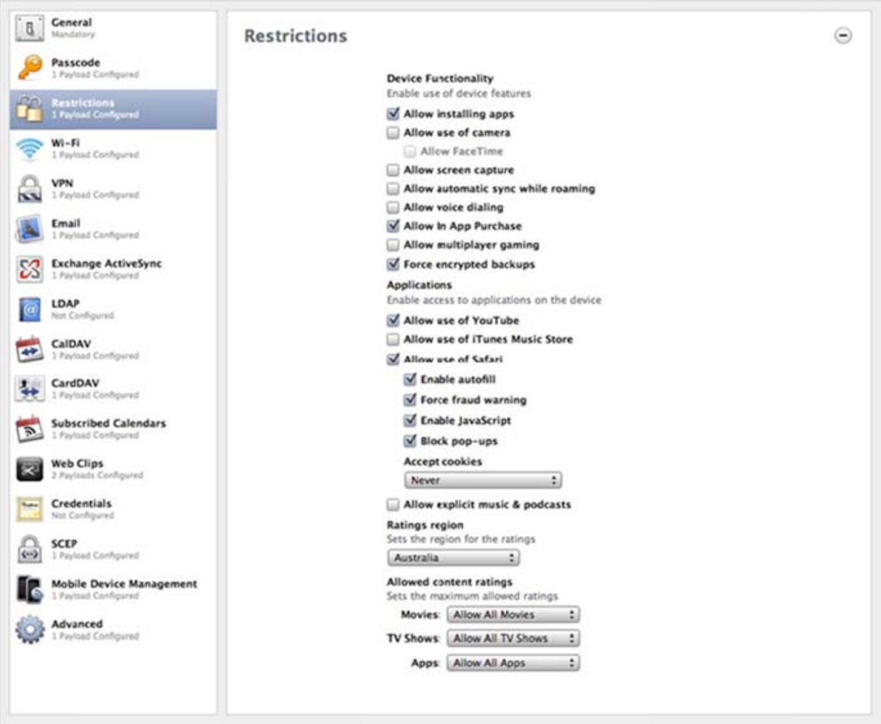
Immediately Grace period for device lock
Amount of time the device can be locked without prompting for passcode on unlock

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

- a maximum passcode length of 90 days;
- require passcode on device;
- do NOT allow simple value (i.e. PIN);
- require alphanumeric;
- minimum of 8 characters;
- auto-lock of 5 minutes (Note: Current maximum allowed time on iOS);
- history of 8 passwords;
- immediate device lock; and
- auto-wipe on 5 failed attempts.

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



Restrictions

Device Functionality
Enable use of device features
☑ Allow installing apps
☐ Allow use of camera
☐ Allow FaceTime
☐ Allow screen capture
☐ Allow automatic sync while roaming
☐ Allow voice dialing
☑ Allow In App Purchase
☐ Allow multiplayer gaming
☑ Force encrypted backups

Applications
Enable access to applications on the device
☑ Allow use of YouTube
☐ Allow use of iTunes Music Store
☑ Allow use of Safari
☑ Enable autofill
☑ Force fraud warning
☑ Enable JavaScript
☑ Block pop-ups
Accept cookies
Never
☐ Allow explicit music & podcasts

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 installing apps - Off at Restricted/Protected, and to fully comply with ISM. Potentially On as an exception at lower levels, as per discussion and mitigation measure noted previously.
- Allow use of Camera - up to agency
- Allow screen capture - up to agency
- Allow automatic sync while roaming - usually off
- Allow voice dialling - on
- Allow in-app purchase - Off if app installation off, potentially on if user-installed apps allowed
- Force encrypted backups
- Allow use of You-tube - as per agency policy
- Allow use of iTunes Music Store - as per agency policy
- Allow use of Safari – enable autofill, force fraud warning, enable JavaScript, block popups
- Allow use of explicit music and podcasts - usually off, as per agency policy
- Ratings Region - Australia
- Allowed content ratings - up to agency policy

Wi-Fi

- SSID of network as appropriate
- Hidden SSID as per agency policy
- WPA2 Authentication with EAP-TLS and a pre-shared key as a minimum, but per user RADIUS or 802.1X is recommended
- Protocols, Authentication and Trust to match network requirements. 802.1X with device identity certificate and username/password is the preferred authentication mechanism for in-Confidence and higher.

VPN

- IPSec and SSL are DSD Approved Cryptographic Protocols, please refer to the Evaluated Products List (EPL) for more information – http://www.dsd.gov.au/infosec/epl/
- “VPN Server Configuration for iOS 4 Devices” on http://developer.apple.com should be consulted for server side settings that iOS supports.
- Certificate based Machine Authentication. Full trust chain needs to be included.
- Split tunnel VPN should be off (set VPN concentrator side)
- VPN on Demand should be enabled with a whitelist of agency URLs or domains that device is allowed to access
- Proxy should be configured - ideally a PAC file.

Email

- Not typically needed if EAS (e.g. Exchange ActiveSync Gateway, Lotus Notes Traveller) is in use. Otherwise appropriate to IMAP server, and can co-exist with Exchange.
- If set, SSL only, with authentication

Exchange ActiveSync

- Settings as per EAS server details, SSL authentication credentials required to control both which device and which users have access to EAS.
- Note if a profile with an EAS payload is removed, all EAS synced email and attachments are deleted from the device.

LDAP

- As per agency requirements if desired. Not typically needed if Exchange GAL is used, but can co-exist.
- SSL recommended

CalDAV

- As per agency requirements if required. May not be needed if Exchange used, but can co-exist.
- SSL recommended

CardDAV

- As per agency requirements if required. May not be needed if Exchange is used, but can co-exist.
- SSL recommended

Subscribed Calendars

- As per agency requirements
- SSL should be used if there is any sensitivity to the calendar data

Web Clips

- As per agency requirements. These are “aliases” or links to URLs with a custom icon on the home screen.
- 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.

Credentials

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

SCEP

- Used when pre-configuring SCEP enrolment prior to device issue - rather than OTA opt-in. OTA opt-in is the normal method used.

MDM

- Used when pre-configuring MDM enrolment prior to device issue - rather than OTA opt-in. OTA opt-in is the normal method used.
- Usually, credentials should be added, all messages signed, and all access rights enabled for remote administrators
- The Development APNS should generally not be used for production systems

Advanced (Used when a custom APN for 3G data is used)

- Authentication should be set,
- Proxy should be set appropriately.

All details here are worked out with the telephony carrier.

Other Settings not managed by Configuration Profile

GSM Voice and SMS/MMS

- GSM Voice and SMS/MMS should only be used for UNCLASSIFIED data at this time.
  Whilst a secure VOIP solution is technically possible, no Sectera compatible solutions are available on iOS at time of writing.

Cellular Data

- A SIM PIN should be set prior to issue.
  Data Roaming should generally be set to off.

Bluetooth

- Generally, Bluetooth should be set to off, unless there is a specific business reason for its use (e.g. Bluetooth headset with a phone, or Bluetooth Keyboard). See ISM section ”Mobile Devices" for further information.

Picture Frame (iPad Only)

- This feature is a similar to a screen saver on the login screen.
- It should either be set to point to a specific Photo Album that contains data of no sensitivity (under Settings -> Picture Frame), OR
  Picture frame can be turned off in Settings -> General -> Passcode

Wi-Fi

- “Ask to join networks” should be set to off. This requires the user to explicitly choose to join a network. iOS auto-joins previously known networks only.

Dock Connector

- Whilst unlocked, iOS could establish a trust relationship through the dock connector with devices or host computers. The dock connector cannot be managed by configuration profile, and therefore must be managed with agency policy. It is recommended that users be instructed to only connect their iOS device to their agency issued charger or computer.

Chapter Six

Mobile Device Management

iOS 3 devices can use web and SCEP servers to establish trust relationships, and pull policy to devices. iOS 4 devices establish initial trust via SCEP, and then can be monitored and managed by servers, services or appliances using Apple's MDM XML, and the Apple Push Notification Service.

Management without MDM

Policy on iOS devices and information security can be managed by a combination of:

- Configuration Profiles loaded on a device;
- Exchange ActiveSync policy;
- network security features (e.g. SCEP, 802.1X, firewalls, Ppoxies, custom APNs); and
- application specific behaviour (e.g. Good Enterprise App being managed by a Good Mobility Server).

Configuration Profiles can be loaded via the iPhone Configuration Utility over USB, pulled over-the-air from a web site, or piggybacked on an SCEP enrolment transaction. In addition, they can be emailed to a device, but this can present a "chicken-and-egg" problem. Sending an SMS containing a URL to a web site is possible, but as SMS are easily spoofed, it is generally not recommended. For small scale or limited scope deployments, a full iOS 4 MDM solution may not be needed, but it usually has significant advantages with larger fleets, or more complex usage scenarios.

MDM Vendors

At the time of writing this guide there are at least 25 vendors shipping MDM solutions that have full support for iOS 4 MDM XML and APNS integration, with others having an iOS 3 style solution of some form. In general an iOS 3 style solution will work on a device running iOS 4. Some of these MDM solutions focus purely on device policy and monitoring. Others enhance this functionality, providing enhanced features via an App, and event triggers for business rules that integrate with Exchange ActiveSync, Certificate Authorities and Directory Services. Many vendors can manage multi-platform client. In this chapter the discussion will be restricted to iOS features.

MDM functions

Once an iOS 4 device is enrolled with an MDM Server, an Apple MDM agent is activated on the client device. It can then perform a number of tasks without user interaction, including querying status of the device, and installing or removing Managed Profiles. The interaction between an MDM server and a device occurs in 2 or 3 main ways:

- The MDM server can send an Apple Push Notification Service notification to a device.

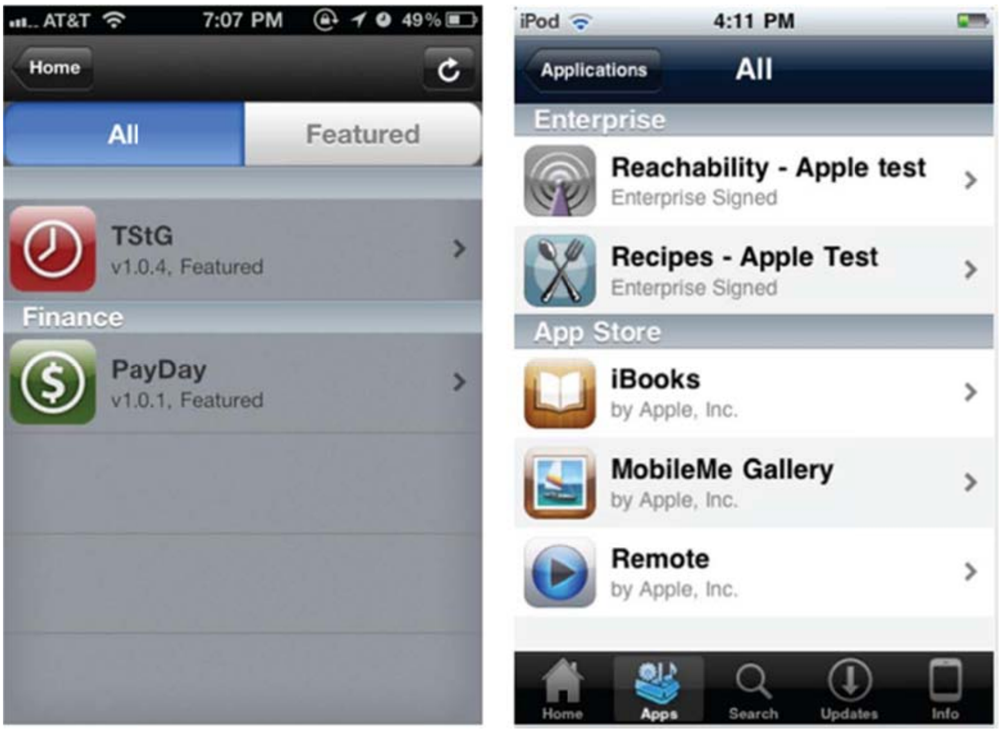
- A device, typically on receipt of a push notification, contacts the MDM server in an SSL encrypted session, and exchanges information using XML. This may be a simple query/response transaction, or it may lead to the device pulling content down from a location the MDM server told it to, such as a configuration profile or provisioning profiles.
- The MDM vendor may also have a client app that can interact with the MDM server. Such Apps can interact in proprietary ways beyond the functionality that the MDM XML interface allows for. Such Apps do not operate at any elevated level of privilege, and if available on the App store, are subject to normal App Store approval processes, but can enhance the functionality and the user experience.

Note that an MDM server cannot install native apps remotely without user intervention. Web apps can be deployed without user intervention by pushing a web clip to the device. Usually remote app installation occurs in one of 3 ways:

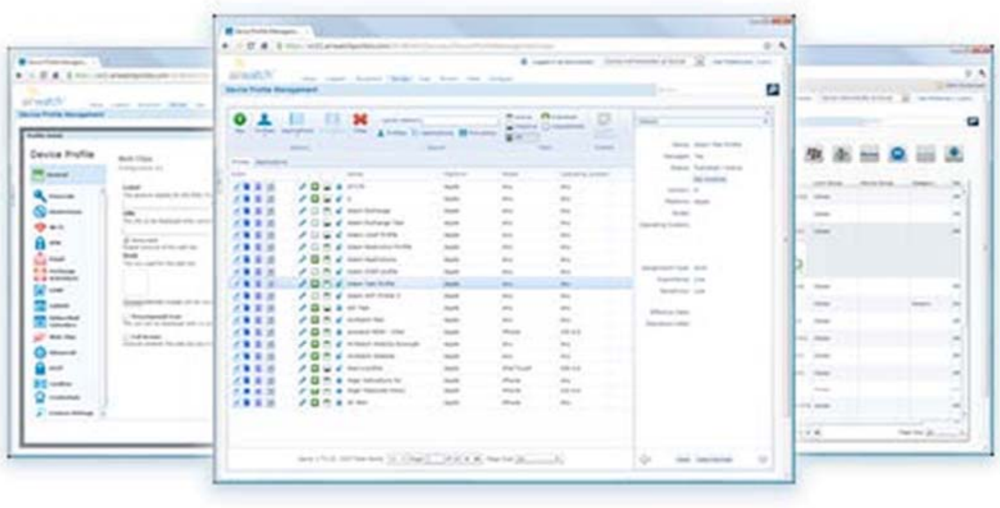
- *The MDM server can silently install or remove [6]provisioning profiles to enable or disable an application from running on a device. The application binary still needs to be downloaded to the device by some means. Enterprise Apps can either have a provisioning profile external to the App, so it can be installed/removed, typically via MDM, or have the provisioning profile embedded within the App itself, which means downloading the App bundle is sufficient for it to run (if present, the Provisioning Profile is copied from the App bundle, by the installer, and installed when the App is installed).*
- *The MDM server can silently install or remove [7]a configuration profile that contains a web clip. If the web clip points to an appropriately constructed web site, touching on it will download an Enterprise iOS application to the device. The Web clip can also be the URL for a Web app, in which case it is usable immediately.*
- *The MDM solution may also, either via a native app or a web app, provide a list of approved, or recommended App store apps, and Enterprise In-House Apps, that when touched by a user, will open the App Store or Web server on the device for the user to download or purchase.*

[6] MDM can only remove profiles that are installed via MDM.

[7] See above.



Example of approved or recommended applications lists. MobileIron shown on top left, Sybase Afaria shown on top right.



Airwatch Mobile Device Management Web Console

Appendix A

Security Checklist

The following checklist will assist an agency in ensuring that all key tasks in securely deploying iOS devices have been completed.

Task	Comments
Before Deploying iOS Devices	
Develop agency policy and procedures, including any restrictions, for the use of iOS devices that align with Australian government policies and standards, and that adhere to DSD information security requirements.	Effective policies and procedures help to ensure that an agency considers relevant issues and operates in accordance with whole-of-government guidelines. Documenting and making these available to staff will help ensure that users are aware of an agency's expectations of them when using mobile devices. On iOS devices making policy a 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.	Filtering solutions at the EAS Server such as JanusGATE can both 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 and 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. DSD can assist in ensuring that the necessary steps have been followed.
Manage Use of iOS Devices	

Task	Comments
Provide staff 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 in the appropriate use of devices can assist staff 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 staff 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 staff formally acknowledge their agreement to adhere to agency specific Acceptable Usage Policy and procedures.	Staff using a mobile device are responsible for its use. Staff must be aware of and agree in accordance with the agency's policy and procedures. The ramifications of failing to apply those policies and procedures must also be clear to staff.
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 Issues	
Server infrastructure for EAS, MDM ,CA, and Web that supports an iOS deployment must be controlled, either directly or under contract, by the Australian Government.	Use of EAS, MDM and CA infrastructure allows many risks to be mitigated. These servers should be situated in a controlled environment, and will permit the implementation of consistent policy and device settings. Software As A Service (SAAS) solutions may not be acceptable for production deployments.
Agencies must ensure that content is transferred between and iOS Device and an agency's ICT systems in accordance with DSD 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 *Implementation Guide for Email Protective Markings for Australian Government Agencies.*

Task	Comments
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 *Implementation Guide for Email Protective Markings for Australian Government Agencies.*

Task	Comments
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 Risk Management Plan (RMP), The System Security Plan (SSP), Standard Operating Procedures (SOP) and the implementation of email protective marking controls. This review must be completed within 12 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 an 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.

Appendix B
Configuration Profiles Format

This provides the references for the format of mobileconfig files for those wishing to create their own tools or custom configurations without deploying a commercial MDM solution.

Configuration Profiles use the Apple XML DTD and the general property list (plist) format. A general description of the Apple plist format is available at www.apple.com/DTDs/PropertyList-1.0.dtd.

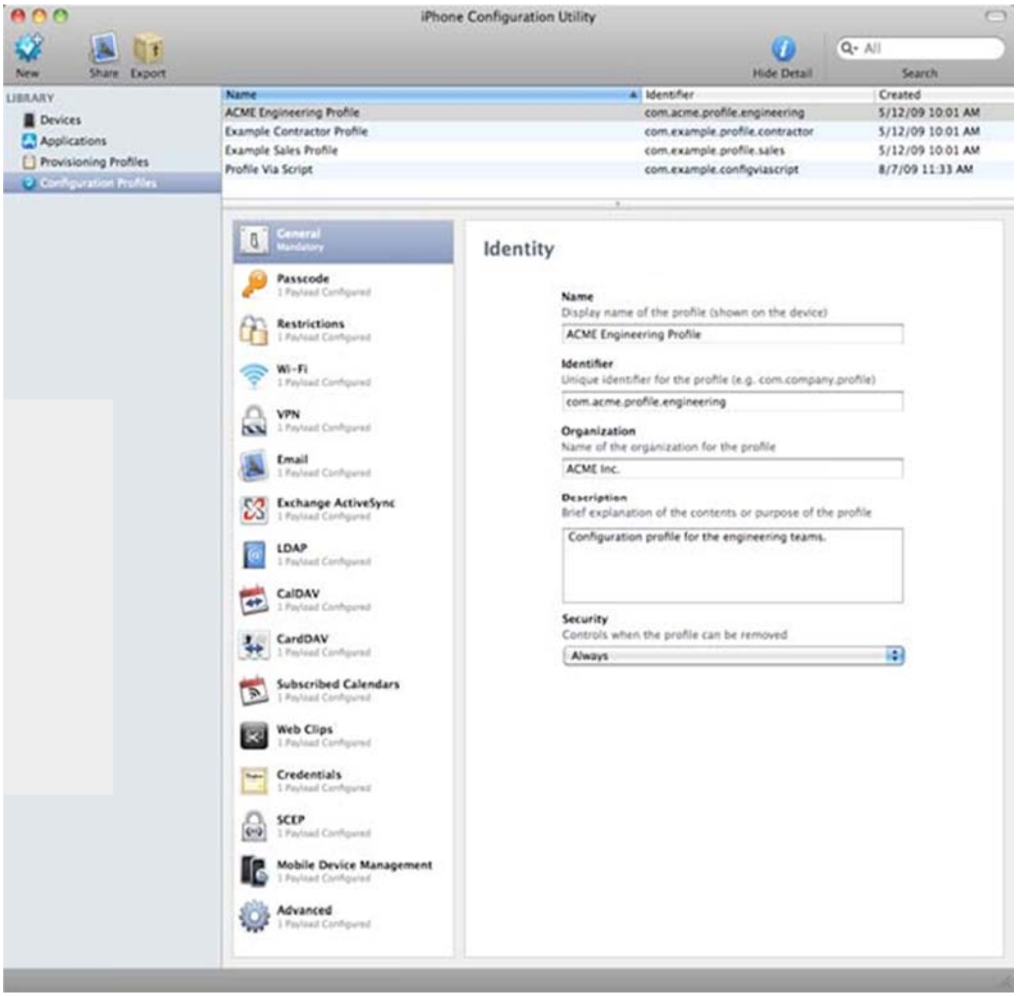
To get started with Configuration Profiles you can use iPhone Configuration Utility (iPCU) to create a skeleton file that you can modify using the information in this appendix, or you can use the examples at http://developer.apple.com.

iPhone Configuration Utility is documented in detail here:

http://developer.apple.com/library/ios/#featuredarticles/FA_iPhone_Configuration_Utility/Introduction/Introduction.html

A screen shot of the iPhone Configuration Utility is shown on the next page, showing the range of different profile payloads.

This document uses the terms payload and profile. A profile is the whole file that configures certain (single or multiple) settings on iPhone, iPod touch, or iPad. A payload is an individual component of the profile file.



Name	Identifier	Created
ACME Engineering Profile	com.acme.profile.engineering	5/12/09 10:01 AM
Example Contractor Profile	com.example.profile.contractor	5/12/09 10:01 AM
Example Sales Profile	com.example.profile.sales	5/12/09 10:01 AM
Profile Via Script	com.example.configviascript	8/7/09 11:33 AM

Identity

Name
Display name of the profile (shown on the device)
ACME Engineering Profile

Identifier
Unique identifier for the profile (e.g. com.company.profile)
com.acme.profile.engineering

Organization
Name of the organization for the profile
ACME Inc.

Description
Brief explanation of the contents or purpose of the profile
Configuration profile for the engineering teams.

Security
Controls when the profile can be removed
Always

iPhone Configuration Utility

For further information on configuration profile format, full documentation is available from:

http://developer.apple.com/library/ios/#featuredarticles/iPhoneConfigurationProfileRef/Introduction/Introduction.html

For further information on configuration profiles, including scripting of iPCU and sample Ruby code for building an SCEP server that generates profiles on demand, see:

http://developer.apple.com/library/ios/#documentation/NetworkingInternet/Conceptual/iPhoneOTAConfiguration/Introduction/Introduction.html

Appendix C
Sample Scripts

This appendix provides sample scripts for iPhone OS deployment tasks. The scripts in this section should be modified to fit your needs and configurations.

http://developer.apple.com/library/ios/#featuredarticles/FA_iPhone_Configuration_Utility/Introduction/Introduction.html

Sample C# Script for iPhone Configuration Utility

This sample script demonstrates creating configuration files using iPhone Configuration Utility for Windows.

```
using System;
using Com.Apple.iPCUScripting;
public class TestScript : IScript
  {
 private IApplication _host;
 public TestScript()
           {
           }
public void main (IApplication inHost)
{ _host = inHost;

string msg = string.Format("# of config profiles : {0}",
_host.ConfigurationProfiles.Count);
Console.WriteLine(msg);

IConfigurationProfile profile = _host.AddConfigurationProfile();
 profile.Name = "Profile Via Script";
profile.Identifier = "com.example.configviascript";
profile.Organization = "Example Org";
profile.Description = "This is a configuration profile created via the new scripting feature in
iPCU";

// passcode
IPasscodePayload passcodePayload = profile.AddPasscodePayload();
passcodePayload.PasscodeRequired = true;
passcodePayload.AllowSimple = true;

// restrictions
IRestrictionsPayload restrictionsPayload = profile.AddRestrictionsPayload();
restrictionsPayload.AllowYouTube = false;

// wi-fi IWiFiPayload
wifiPayload = profile.AddWiFiPayload();
wifiPayload.ServiceSetIdentifier = "Example Wi-Fi";
wifiPayload.EncryptionType = WirelessEncryptionType.WPA;
wifiPayload.Password = "password";
wifiPayload = profile.AddWiFiPayload();
profile.RemoveWiFiPayload(wifiPayload);
// vpn
IVPNPayload vpnPayload = profile.AddVPNPayload();
vpnPayload.ConnectionName = "Example VPN Connection";
vpnPayload = profile.AddVPNPayload();
profile.RemoveVPNPayload(vpnPayload);

// email
IEmailPayload emailPayload = profile.AddEmailPayload();
emailPayload.AccountDescription = "Email Account 1 Via Scripting";
emailPayload = profile.AddEmailPayload();
emailPayload.AccountDescription = "Email Account 2 Via Scripting";

// exchange
IExchangePayload exchangePayload = profile.AddExchangePayload();
exchangePayload.AccountName = "ExchangePayloadAccount";

// ldap
ILDAPPayload ldapPayload = profile.AddLDAPPayload();
ldapPayload.Description = "LDAP Account 1 Via Scripting";
ldapPayload = profile.AddLDAPPayload();
ldapPayload.Description = "LDAP Account 2 Via Scripting";

// webclip
IWebClipPayload wcPayload = profile.AddWebClipPayload();
wcPayload.Label = "Web Clip 1 Via Scripting";
wcPayload = profile.AddWebClipPayload();
wcPayload.Label = "Web Clip 2 Via Scripting";

        }
 }
```

Sample AppleScript for iPhone Configuration Utility

This sample script demonstrates creating configuration files using iPhone Configuration Utility for Mac OS X.

```
tell application "iPhone Configuration Utility"
        log (count of every configuration profile)

        set the Profile to make new configuration profile with properties{displayed name:
“Profile Via Script", profile identifier:"com.example.configviascript", organization:"Example
Org.", account description:"This is a configuration profile created via AppleScript"} with
properties {label:"Web Clip Account 1 with properties {label:"Web Clip Account 2”}

        tell theProfile
                make new passcode payload with properties {passcode required:true, simple
        value allowed:true}
                make new restrictions payload with properties {YouTube allowed:false}
                make new WiFi payload with properties {service set identifier:"Example Wi-
        Fi", security type:WPA, password:"password"}
                set theWiFiPayload to make new WiFi payload
                delete theWiFiPayload
```

```
    make new VPN payload with properties {connection name:"Example VPN Connection"}
    set theVPNPayload to make new VPN payload
    delete theVPNPayload
    make new email payload with properties {account description:"Email Account 1 Via Scripting"}
    make new email payload with properties {account description:"Email Account 2 Via Scripting"}
    make new Exchange ActiveSync payload with properties {account name:"ExchangePayloadAccount"}
    make new LDAP payload with properties {account description:"LDAP Account 1 Via Scripting"}
    make new LDAP payload with properties {account description:"LDAP Account 2 Via Scripting"}
    make new web clip payload Via Scripting"}
    make new web clip payload Via Scripting"}
        end tell
    end tell
```

Appendix D
Example Scenarios

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

Unclassified Example

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.

They set up a Wi-Fi network for the site, and use a Kiosk with a locked down instance of iTunes, and OTA app and profile provisioning from a secured web server to deploy, manage and reset devices during use with minimal effort.

In-Confidence Example

An agency wants to use iPad 3G's as a field based information gathering tool by its staff. Information will come from a mix of existing web sites, and with some data entry fed into an existing system with an XML interface, using an Enterprise In-House App the agency has developed. The devices will also allow staff to send and receive email in the field. The Agency's primary WAN is classified "Protected".

In this case the agency uses a combination of an MDM server, Exchange ActiveSync, and a 3rd party gateway filter to control policy on the devices, and control what email is sent to the devices, and implement protective markings on email sent from the devices. Access to the limited intranet sites with "in-confidence" data are controlled by a reverse proxy. The custom App and its supporting server infrastructure undergo a separate TRA. An "in-confidence" Wi-Fi network is provided at selected locations to support OTA provisioning and updating of devices.

Appendix E
Risk Management Guide

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

Australian Government Information Security Manual (ISM)

This appendix should be read in conjunction with the ISM, available from the DSD website: http://www.dsd.gov.au/infosec/ism.htm
iOS devices do not completely comply with all requirements described within the ISM.

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. These risks will require policy guidance and agencies will need to assess their residual risk:

- iOS devices implement DACA and DACP, but have not completed a DCE. This is a residual risk for data at the Restricted and Protected classifications. The submission of iOS devices for FIPS-140-2 certification is a partial mitigation, but not a substitution for a DCE. (Control 0453)
- iOS 4.3.3 does not have a local firewall. This is partially mitigated by firewalling at the network layer, and significantly mitigated by the sandboxed runtime environment in iOS.
- iOS 4.3.3 allows the user to deliberately connect to an untrusted Wi-Fi network. Note that iOS devices will not autoconnect to any unknown Wi-Fi network. The only mitigations available at this time are pre-configured settings, user education and AUP.
- iOS 4.3.3 allows the user to deliberately enable or disable the radios in the device - there is no method for a configuration profile to force a radio off. The only mitigations available at this time are user education, AUP or hardware modification (the latter being permanent and will void the warranty).
- iOS 4.3.3 has no “always-on” setting for VPN. It is either manually initiated, or on-demand based on a whitelist. Options to mitigate this for PIM data (if EAS and/or VPN on demand are assessed as insufficient mitigations) include using a 3rd party PIM solution such as Good Enterprise or Sybase Afaria, filtering at the EAS, or using approved VDI solution to access sensitive data. For web site access, a SSL reverse proxy may be more suitable than VPN in some scenarios.

Risk	Mitigations	Implied Preconditions
Device lost, still on Network	Strong Passcode, Data Protection Enabled, Remote Wipe, Find My iPhone/iPad.	Configuration Profiles, EAS or MDM Server in a network reachable location. MobileMe
Device Lost, off Network	Strong Passcode, Local Wipe, Data Protection Enabled.	Configuration Profiles, Device restored to iOS 4 prior to use in field.
Device lost, casual access attempt	Strong Passcode, Local Wipe, Data Protection Enabled.	Configuration Profiles, Device restored to iOS 4 prior to use in field.
Device lost, forensic access attempt without passcode knowledge	Strong Passcode, Local Wipe, Data Protection Enabled, App usage of appropriate data protection class[8].	Configuration Profiles, Device restored to iOS 4 prior to use in field.
Jailbreaking	Strong Passcode, Data Protection Enabled, Use of devices with Hardware Cryptographic Module, Use of MDM Console, use of VDI infrastructure. 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.
Malicious Runtime Code	Code signing, Memory and Filesystem Sandboxing, Use of VDI infrastructure, No-Execute Heap, Disable User Added Applications, Do not Jailbreak Operational Devices.	In-house application development capability, CA infrastructure. May mitigate on lower security levels by “approved” lists and MDM monitoring as mitigation.
Users cut and paste agency data into a public email account (e.g. Mobile Me, Yahoo or Gmail) and sent it from the device.	On iOS 4.3.3 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, Containing agency email to a sandboxed email App such as Good for Enterprise.	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 well for a mobile device.
Network Trust	Use of 802.1X NAC, IPSEC or SSL VPN, encrypted VDI.	Use of 802.1X with CA & NAC on Wireless, VPN on Demand with client certificates for agency network access, Use of SSL reverse proxy for low security data.

[8] Information for developers implementing data protection classes is available from: http://developer.apple.com/videos/wwdc/2010/?id=209

Risk	Mitigations	Implied Preconditions
Firewall	Use of Custom APN on 3G, 802.1X, SSL VPN.	A custom APN is an arrangement with your telephone carrier. This allows devices on 3G data to have a deterministic IP range that can be more easily firewalled or proxied.
Data compromise via host computer backup	Force encrypted profile onto device, User education, Physical security of backup host, iTunes in host SOE.	SSL CA infrastructure to sign and encrypt profiles into agency chain of trust. Potentially allow use of locked down iTunes configuration on agency computers so backup resides on agency assets.
Data compromise via Bluetooth	iOS 4.3.3 only includes 4 or 6 of the 26 Bluetooth profiles, depending on device, and specifically does not include file transfer related Bluetooth profiles. Included profiles are for microphone, speakers, and human input devices, as well as Apps that use a Bluetooth PAN. See http://support.apple.com/kb/HT3647	Apps that share information via Bluetooth PAN not approved for use on devices where this vector is a concern.

Appendix F

Firewall Rules

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

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 the following table below:

- http://support.apple.com/kb/TS1379
- http://support.apple.com/kb/TS1629

DNS name	Port(s)	Reason
ocsp.apple.com	443	Online Certificate Status for code signing certificates, checked periodically while online and after device reboot.
crl.apple.com	443	Certificate Revocation List for codesigning certificates, checked periodically while online and after device reboot.
gateway.push.apple.com	2195 (outbound push e.g. MDM) 2196 (for devices to receive)	Apple Push Notification Service (for a development environment only, gateway.sandbox.push.apple.com is used instead).
feedback.push.apple.com	2195 (outbound push - e.g. MDM) 2196 (for devices to receive)	Apple Push Notification Service (for a development environment only, feedback.sandbox.push.apple.com is used instead).
phobos.apple.com	80, 443	iTunes Store, Device Activation.
itunes.apple.com	80, 443	iTunes Store, Device Activation.
deimos.apple.com	80, 443	iTunes U.
deimos3.apple.com	80, 443	iTunes Music Store and album cover media servers.
ax.itunes.apple.com	80, 443	iTunes Store, Device Activation.
gs.apple.com	80, 443	iTunes Store, Device Activation.
albert.apple.com	80, 443	iTunes Store, Device Activation.
ax.init.itunes.apple.com	80, 443	Device Activation.
evintl-ocsp.verisign.com	80, 443	Verification of digital signatures of iTunes purchased content.
evsecure ocsp.verisign.com	80, 443	Verification of digital signatures of iTunes purchased content.
a1535.phobos.apple.com	80, 443	iTunes Music Store and album cover media servers.