Guidance

End User Devices Security Guidance: Apple iOS 7

Updated 10 June 2014

Contents

This guidance is applicable to devices running iOS 7.0 and 7.1. This guidance was developed following testing performed on iPhone 5S and iPhone 5 devices running iOS 7.0.4.

1. Changes since previous guidance

This document is an update of the previous iOS 6 guidance to cover iOS 7. Some changes to the recommended configuration have been made to take account of new features and changed behaviours in the platform. The risk information given below is the same as in previous guidance.

Deployments which followed the previous iOS 6 guidance will need to update the configuration of those devices to ensure that the VPN will automatically connect when the devices are updated to iOS 7.

2. Usage Scenario

iOS devices will be used remotely over 3G, 4G and non-captive Wi-Fi networks to enable a variety of remote working approaches such as:

- accessing OFFICIAL email
- reviewing and commenting on OFFICIAL documents

- accessing the OFFICIAL intranet resources, the Internet and other web-resources

To support these scenarios, the following architectural choices are recommended:

- All data should be routed over a secure enterprise VPN to ensure the Confidentiality and Integrity of the traffic, and to allow the devices and data on them to be protected by enterprise protective monitoring solutions
- Arbitrary third-party application installation by users is not permitted on the device. An enterprise application catalogue should be used to distribute in-house applications and trusted third-party applications

3. Summary of Platform Security

This platform has been assessed against each of the twelve security recommendations, and that assessment is shown in the table below. Explanatory text indicates that there is something related to that recommendation that the risk owners should be aware of. Rows marked [!] represent a more significant risk. See How the Platform Can Best Satisfy the Security Recommendations for more details about how each of the security recommendations is met.

Recommendation	Rationale
1. Assured data-in-transit protection	The VPN can be disabled by the user. The built-in VPN has not been independently assured to Foundation Grade, and no suitable third-party products exist.
2. Assured data-at-rest protection	iOS data protection has not been independently assured to Foundation Grade. Only applications which opt to use the relevant Data Protection APIs on iOS have their sensitive information protected when locked (rather than powered off).
3. Authentication	
4. Secure boot	
5. Platform integrity and application sandboxing	
6. Application whitelisting	
7. Malicious code detection and prevention	
8. Security policy enforcement	Whilst Configurator settings cannot be overridden, the MDM profiles can be removed by the user. The MDM APIs only offer a limited set of controls. Significant overhead per-device is required to provision each device.
9. External interface protection	Radio interfaces such as Wi-Fi and Bluetooth cannot be controlled by policy.
10. Device update policy	
11. Event collection for enterprise analysis	[!] There is no facility for collecting logs remotely from a device, and collecting forensic log information from a device is very difficult.

3.1 Significant Risks

The following key risks should be read and understood before the platform is deployed.

- CESG have performed a due-diligence risk assessment of the VPN component and found that the VPN currently does not support some of the mandatory requirements expected from assured VPNs. Without assurance in the VPN there is a risk that data transiting from the device could be compromised. In addition, there is no guarantee that data from applications on the device will use the VPN, leading to potential for data leakage onto untrusted networks. A private APN can be used to help treat this risk
- iOS data protection has not been independently assured to Foundation Grade. However, CESG has previously determined that the level of protection is commensurate with Foundation Grade for applications that use Data Protection APIs to protect data when the device is locked
- Applications can choose classes of data encryption on a per-file basis, and the only default application which opts-in to encryption whilst locked is the Mail application. Files other than e-mail and attachments will not be encrypted when the device is locked, and could be extracted without knowledge of the password using a vulnerability in the platform. Third-party applications are automatically opted in to the encryption class which is protected when the device is in a powered off state (but not when locked). Developers can then choose whether to opt-out of this encryption, or opt-in to the highest encryption class (i.e. encrypted when locked)
- Collection of events for enterprise analysis is limited, meaning protective monitoring and forensic analysis following any compromise may be much harder than on other platforms
- There are no policy controls available to restrict the external interfaces a user can enable, meaning that external interfaces may be accidentally or deliberately enabled by the end-user. Enabling external interfaces means additional attack surface could be exposed and data could be inadvertently or maliciously leaked without enterprise visibility
- Procedural controls are used to achieve some of the requirements where no technical controls could be used, which means that users have to be trusted not to alter certain settings on the device, or perform actions which may impact the security of the device. These controls are discussed in later sections

4. How the Platform Can Best Satisfy the Security Recommendations

This section details the platform security mechanisms which best address each of the security recommendations.

4.1 Assured data-in-transit protection

Use the native IPsec VPN client until a Foundation Grade VPN client for this platform becomes available.

4.2 Assured data-at-rest protection

iOS data protection is enabled by default. The Mail application uses Data Protection APIs to encrypt emails and attachments when the device is locked. Third-party developers can also use this protection class to gain the

benefit of the technology.

4.3 Authentication

The user has a strong 7 character password to authenticate themselves to the device. This password unlocks a key which encrypts certificates and other credentials, giving access to enterprise services.

4.4 Secure boot

This requirement is met by the platform without additional configuration.

4.5 Platform integrity and application sandboxing

This requirement is met by the platform without additional configuration.

4.6 Application whitelisting

An enterprise application catalogue can be established to permit users access to an approved list of in-house applications. If the App Store is enabled, MDM can be used to monitor which applications a user has installed.

4.7 Malicious code detection and prevention

The enterprise app catalogue should only contain approved in-house applications which have been checked for malicious code. iOS does not support side-loading of applications. Content-based attacks can be filtered by scanning on the email server.

4.8 Security policy enforcement

Settings applied through Configurator cannot be removed by the user.

Settings applied through MDM can be removed completely, but that also removes any data stored as part of accounts configured through MDM (eg e-mail and credentials).

4.9 External interface protection

The USB interface is configured by using Configurator to put the device into supervised mode. No technical controls exist to prevent users from enabling Wi-Fi and Bluetooth.

4.10 Device update policy

Users are free to update applications and firmware when they wish. The enterprise has no control over this.

4.11 Event collection for enterprise analysis

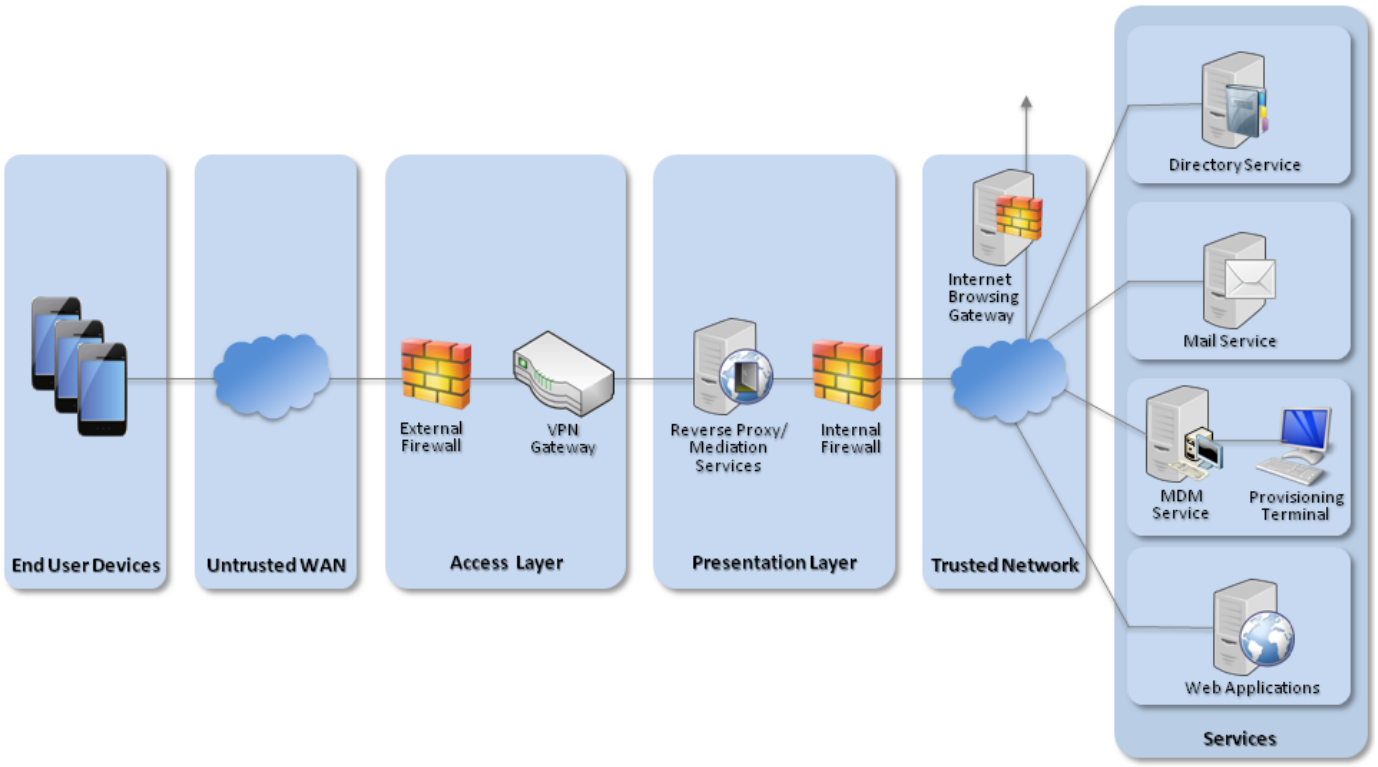
iOS does not support remote or local historic event collection.

4.12 Incident response

iOS devices can be locked, wiped, and configured remotely by their MDM.

5. Network Architecture

All remote or mobile working scenarios should use a typical remote access architecture based on the Walled Garden Architectural Pattern. The following network diagram describes the recommended architecture for this platform.



Recommended network architecture for deployment of iOS 7

A Mobile Device Management server is required. Apple's OS X Server Profile Manager is sufficient for this purpose. Alternatively, third-party products exist which may offer additional functionality over and above Profile Manager.

6. Deployment Process

The steps below should be followed to prepare the enterprise infrastructure for hosting a deployment of these devices:

1. Deploy OS X 10.7.5+ and install iTunes 11.0.3+ and Apple Configurator 1.4+ onto a dedicated provisioning terminal.
2. Procure, deploy and configure other network components, including an approved IPsec VPN Gateway.
3. Set up the MDM with the Profile Manager component, and create policies for users and groups in accordance with the settings later in this section.

7. Provisioning Steps

The steps below should be followed to provision each end user device onto the enterprise network to prepare it for distribution to end users:

1. Use Configurator to supervise the iOS devices
2. Enrol the devices into the MDM deployed earlier and install the predefined configuration profile
3. Apply any additional required security controls by using the Restrictions menu locally on the device.

8. Policy Recommendations

This section details important security policy settings which are recommended for an iOS deployment. Other settings (eg server address) should be chosen according to the relevant network configuration.

8.1 Configurator Settings

These settings should be applied to the device by creating profiles in the Configurator utility.

Configuration Rule	Configuration Setting
General Group	
Security (user can remove profile)	Never
Automatically Remove Profile	Never
Supervision	On
Allow devices to connect to other Macs	No

The Global HTTP Proxy settings should also be set to match your particular network configuration for when the device is connected to the VPN.

8.2 MDM Settings

These settings should be applied to the device by creating profiles on the MDM server.

Passcode Group	
Allow Simple	No
Require alpha-numeric value	Yes
Minimum passcode length	7 (characters)
Minimum complex characters	1
Maximum passcode age	90 (days)
Maximum auto-lock	10 (minutes)
Passcode history	8
Maximum grace period for device lock	5 (minutes)
Maximum number of failed attempts	5
Restrictions Group	
Allow installing apps	No
Allow screen capture	No
Allow installation of Configuration Profiles (Supervised devices only)	No
Allow iCloud backup	No
Allow iCloud documents and data	No
Allow iCloud keychain	No
Allow iCloud photo sharing	No
Allow accepting untrusted TLS certificates	No
Allow Siri whilst device is locked	No
Allow modifying account settings	No
Allow AirDrop	No
Allow Touch ID to unlock device	No
Allow Control Center in lock screen	No
Show Today view in lock screen	No

If you are using Profile Manager, you should ensure that the option to sign configuration profiles is selected. Other MDMs may have a similar option which should be selected.

8.3 On-device Restrictions Menu

In Settings → General → Restrictions, the following items should be set as described and protected using a unique 4-digit PIN which is not shared with the device user. These settings must be set on each device.

Configuration Rule	Recommended Setting
Contacts - Don't allow changes	Yes
Calendars - Don't allow changes	Yes
Photos - Don't allow changes	As per organisational policy
Bluetooth Sharing - Don't allow changes	Yes
Twitter - Don't allow changes	As per organisational policy
Facebook - Don't allow changes	As per organisational policy
Accounts - Don't allow changes	Yes

Allowing changes to these restrictions will allow applications on the device to request access to the named data store. Any that are not required should be disabled.

Allowing changes to the Facebook and Twitter settings will allow applications on the device to request access information from the user's Facebook and Twitter accounts, including identity, and make posts to that account.

8.4 VPN Profile

The deployed VPN solution should be configured to negotiate the following parameters. Not all of these settings can be configured on the device so the configuration needs to also be enforced from the VPN server.

Setting	Value
IKE DH Group	5 (1536-bit)
IKE Encryption Algorithm	AES-256
IKE Hash Algorithm	SHA-1
IKE Authentication Method	RSA X.509
IPsec Encryption	AES-256

IPsec Auth	SHA-1
SA Lifetime	24 hours
VPN On Demand	Always

In iOS 7, the mechanism for configuring the VPN on Demand settings has changed, and no tested tool (Configurator or MDM) currently exposes a GUI for this new mechanism. To configure the VPN on Demand to trigger for all outgoing connections, follow these steps:

- Configure the VPN settings using the MDM or Configurator and test the profile on the device to ensure it connects manually
- Export the VPN configuration profile (unsigned) from the MDM or Configurator as a .mobileconfig file. Convert this to text using `plutil` if required
- Using a text editor, modify the XML configuration inside the exported file. In the IPSec key, change:

```
<key>OnDemandEnabled</key>
<integer>1</integer>
```

to

```
<key>OnDemandEnabled</key>
<integer>1</integer>
<key>OnDemandRules</key>
<array>
<dict>
<key>Action</key>
<string>Connect</string>
</dict>
</array>
```

- Import the modified configuration to the MDM or Configurator and deploy to the device

Note that for an iOS device to verify the VPN server certificate, the certificate must have an alternate subject name entry that matches the common name. Information on the supported server configurations can be found at http://help.apple.com/iosdeployment-vpn/mac/1.2/

9. Enterprise Considerations

The following points are in addition to the common enterprise considerations, and contain specific issues for iOS deployments.

9.1 App Store Applications

The configuration given above prevents users from accessing the App Store to install applications, but an organisation can still host its own Enterprise App Catalogues to distribute in-house applications to their employees if required.

9.2 VPN

On iOS users can alter the configuration of the VPN which can adversely affect the security of the device. Procedural controls must be present in the user security procedures to prohibit the altering of any settings related to the VPN. Configuring the Global Proxy setting in Configurator means that the device will not be able to make successful outgoing connections if the user disables the VPN on Demand setting.

9.3 Cloud Integration

iOS devices do not need to be associated with an Apple ID to operate as required within an enterprise. For example, it is still possible to receive push notifications, and to install in-house applications without associating to an account. However, an Apple ID is required to obtain applications from the App Store, and to use certain other on-device services.

If an Apple ID is used to enable iCloud services on the device then documents and other sensitive data may be inadvertently synchronised with iCloud. As a mitigation, organisations should implement controls to prevent users from enabling unneeded iCloud services on their device, thereby preventing enterprise data from being synchronised with Apple servers.

Legal Information