Guidance

End User Devices Security Guidance: Apple iOS 9

Published

Contents

This guidance is applicable to devices running iOS 9.0. This guidance was developed following testing performed on iPad Air device running iOS 9.0.

1. Changes since previous guidance

This document is an update of the previous iOS 8 guidance and covers the security relevant changes to iOS 9. Some changes to the recommended configuration have been made to take account of new features and changed behaviours in the platform. iOS 9 introduces a number of updates which have particular security considerations as well as providing improvements to many of the security features introduced in earlier versions, such as VPN. Always-on support in the IKEv2 VPN has also been improved to provide a more robust tunnel.

Other security benefits from the introduction of IKEv2 are unchanged from the iOS 8 security guidance document. These benefits are:

- Users cannot disable the device VPN, lowering the risk of data being transmitted outside the VPN.
- The VPN does not disconnect when the screen is locked, permitting push notifications

for email and incoming Voice over IP calls to work.
- Local Wi-Fi traffic cannot transit outside the VPN (unless explicitly permitted), lowering the risk of compromise on a hostile Wi-Fi network.
- If you have previously decided a carrier-provided Access Point Name (APN) is required to mitigate certain risks then nearly all of those risks will be mitigated by using the always-on VPN, allowing the APN to be removed from the architecture.

The previous iOS 7 (and below) approach to the VPN can still be used in iOS 8 and iOS 9, though the risks associated with the previous approach must be considered if this option is taken.

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 the native IKEv2 always-on 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 suitable assessed third-party applications. CESG guidance on third-party application development for iOS can be used to assist with this process.
- Unless the organisation decides to use a particular third-party VPN, third party VPN extensions should not be installed by users. Although VPN extension providers require entitlements to be granted by Apple when developing the extension, it may be possible that a malicious or poorly-written VPN extension could be used to capture and log network traffic.

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 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 will have their sensitive information protected when locked (rather than powered off).
3. Authentication	
4. Secure boot	
5. Platform integrity and application sandboxing	Developers can allow their applications signed by the same key to access to a shared storage container, shared preferences and shared keychain. Sensitive data generated within one application may potentially be accessible to another if those applications are part of an app group. Application whitelisting can help mitigate this.
6. Application whitelisting	Not all classes of application extension respect managed to unmanaged application restrictions (e.g. a sharing extension may sensitive data to be shared to a social network). Administrators should pay particular attention to the extensions installed by whitelisted applications, to ensure that managed documents are not able to be trivially shared outside of managed applications.
7. Malicious code detection and prevention	
8. Security policy enforcement	Policy settings applied through Apple Configurator cannot be overridden (when using recommended security settings). However, MDM profiles can be removed by the user (unless DEP is used). Device Enrollment Program (DEP) can allow devices to be enrolled over-the-air during the device setup process. This can be used to limit the time a device is in a potentially hostile environment or configuration, and prevent removal of the MDM profile.
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.
12. Incident response	iOS devices can be remotely locked, wiped, and reconfigured by their MDM.

3.1 Significant risks

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

- The VPN has not been independently assured to Foundation Grade. Without assurance in the VPN there is a risk that data transiting from the device could be compromised.
- 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. By default, only a limited number of files remain encrypted whilst the device is locked, including e-mail and attachments (within the mail app), managed books and location data. Files belonging to other applications may 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 protects their data when the device is in a powered off state (but not when locked). Developers can then choose whether to opt-out of this encryption entirely, or opt-in to the highest encryption class (encrypted when locked).
- Custom keyboards should not be deployed via MDM. Keyboards deployed via MDM are considered managed and can then be used within other managed applications such as the mail app. If the user allows “full access” to the keyboard extension (which may be required for its correct operation), it is then not restricted from logging and sending keystrokes to external servers.
- Collection of events for enterprise analysis is limited, meaning protective monitoring and forensic analysis following any compromise may be much more difficult 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 increasing the exposed attack surface, and data could be inadvertently or maliciously leaked without enterprise visibility.
- Procedural controls must be 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

iOS 9 improves the IKEv2 VPN client which can be configured in an ‘Always On’ mode to guarantee all traffic is routed through the organisational infrastructure for inspection. This can protect data-in-transit and quickly switch between cellular and Wi-Fi networks. The native IKEv2 VPN client should be used until a Foundation Grade VPN client for this platform becomes available. Organisations also have the option to use a third-party VPN supporting the VPN Extension Point API. These extensions should be installed in a whitelisted fashion if required by an organisation, minimising the risk of installing a malicious or poorly-configured VPN extension.

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. By default, this level of protection also extends to location data and app launch images. Third-party developers can also request this protection class to gain the benefit of the technology.

4.3 Authentication

The user should use 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. TouchID permits biometric unlock of devices but the strength of its security is difficult to measure. In cases where there is a requirement to use biometric authentication, and the risks of using biometrics as the sole authentication mechanism are understood, TouchID can be enabled.

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, the MDM can be used to monitor which applications a user has installed.

Extensions are installed along with a containing application, and cannot be installed alone. It is therefore possible to apply application whitelisting rules that target these applications in order to restrict extensions. Administrators must be fully aware of the extensions installed by their whitelisted applications, to ensure that they do not introduce unexpected methods for sharing data outside of managed applications. It is not currently possible to define granular rules that block extensions, but permit the containing application (beyond implementation of managed / unmanaged application boundaries).

4.7 Malicious code detection and prevention

The enterprise app catalogue should only contain in-house applications and third-party applications which have been approved by an administrator. Content-based attacks can be filtered by scanning on the email server.

4.8 Security policy enforcement

Settings applied through Apple Configurator can be configured such that they cannot be removed by the user.

Policy applied through an MDM can be removed completely by an end user through removal of the Remote Management profile (unless DEP is used). However, this will also remove any data stored as part of accounts configured through MDM (e.g. e-mail and credentials). When configuring an MDM, it should be configured such that (i) arbitary devices cannot be enrolled, (ii) end users are prevented from re-enrolling.

Users should not be allowed to directly re-enrol, as it may be possible for the user to affect the security of the device by: (i) removing the MDM profile, (ii) modifying the on-device configuration options, (iii) re-enrolling the device through a self service portal. Apple’s Device Enrollment Programs should be considered to enable devices to register the Management Server during the setup process, decreasing the risk of a malicious device enrolling. iOS 9 allows administrators to use their MDM to completely configure the device whilst still inside the Setup Assistant.

It is recommended that email accounts are provisioned via MDM, as only email accounts provisioned via MDM will operate correctly with restrictions to disallow opening documents in unmanaged applications (“Managed Open In”).

4.9 External interface protection

The USB interface is only used by Configurator to put the device into supervised mode after which the user is only able to use it for charging their device. 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, though the enterprise can block this at the proxy server if desired. In addition, an MDM can be used to monitor the iOS versions currently installed and access could be revoked if necessary.

4.11 Event collection for enterprise analysis

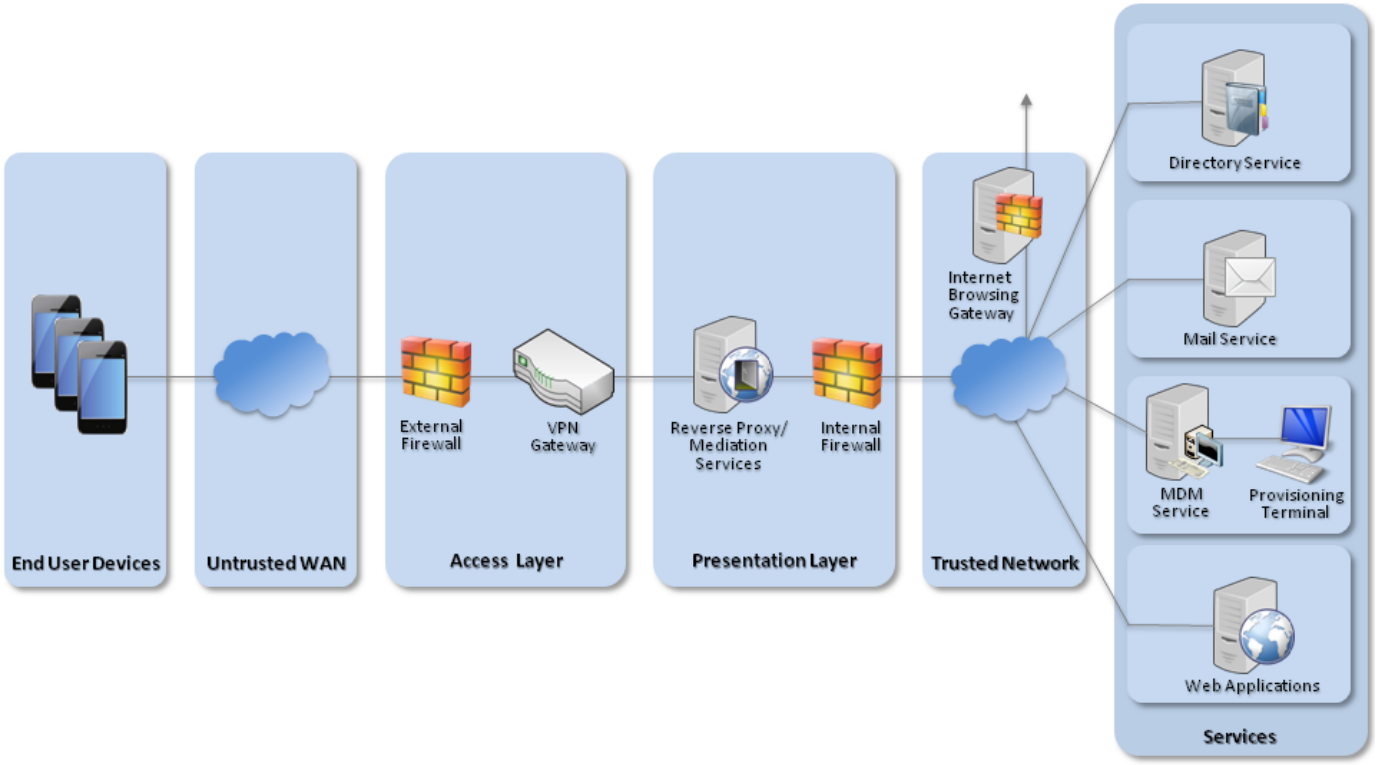
iOS does not support remote or local historic event collection. Limited information regarding device state can be retrieved from the device. The features may depend on the MDM.

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 deployments of Apple iOS 9

A Mobile Device Management server is required. Apple's OS X Server with 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 10.11+ and Apple Configurator 2 onto a dedicated provisioning terminal.
2. Procure, deploy and configure other network components, including an approved IPsec VPN Gateway.
3. Set up the MDM 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 2 to supervise the iOS devices (this is necessary for the “supervised only” restrictions enforced via the MDM to be effective).
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.

Alternatively, devices can be purchased through the Device Enrolment Program which means that the devices will automatically be supervised out of the box, and can be configured to automatically enrol with the MDM server when first activated.

8. Policy recommendations

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

It is important to remember that any guidance points given here are just recommendations; none of the suggestions are mandatory. Risk owners and administrators should agree a configuration which balances the business requirements, usability and security of the platform and use this guidance for advice where needed.

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

If not using the always-on IKEv2 VPN, 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 value	No
Require alphanumeric value	Yes
Minimum passcode length	7 (characters)
Minimum number of complex characters	1
Maximum passcode age	90 (days)
Maximum Auto-Lock	5 (minutes)
Passcode history	8
Maximum grace period for device lock	5 (minutes)
Maximum number of failed attempts	5
Security & Privacy	
Privacy: Allow sending diagnostic and usage data to Apple, and sharing crash data and statistics with app developers	No
Restrictions Group	
Allow installing apps	No
Allow screenshots	No
Allow installing configuration profiles (supervised devices only)	No
Allow iCloud backup	No
Allow iCloud documents & data	No
Allow iCloud keychain	No
Allow iCloud photo sharing	No
NEW: Allow backup of enterprise books	No

NEW: Allow managed apps to store data in iCloud	No
NEW: Allow Handoff	No
NEW: Allow notes and highlights sync for enterprise books	No
Force encrypted backups	Yes
Allow users to accept untrusted TLS certificates	No
Allow Siri whilst device is locked	No
Allow modifying account settings (supervised devices only)	No
Allow documents from managed sources in unmanaged destinations	No
Allow sending diagnostic and usage data to Apple	No
Allow AirDrop (supervised devices only)	No
Allow Touch ID to unlock device	No
Show Control Center in Lock screen	No
Show Today view in Lock screen	No
NEW: Allow Internet results in spotlight	No
Show notification center 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 notifications menu

To prevent sensitive data appearing on the lock screen, the following settings should be set on each device.

Configuration Rule	Recommended Setting
Messages - Show Previews	Disabled
Mail - Show Previews	Disabled

8.4 On-device restrictions menu

These settings should be set on each device.

Configuration Rule	Recommended Setting
Contacts - Don't allow changes	Enabled
Calendars - Don't allow changes	Enabled
Photos - Don't allow changes	As per organisational policy
Share My Location - Don't allow changes	Enabled
Bluetooth Sharing - Don't allow changes	Enabled

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.

To make the provisioning steps less onerous, the risks mitigated by these settings could also be met in other ways. Contacts, Calendars, Photos and Bluetooth permissions are only risky if third-party applications which use these permissions are installed on the device. Some users' locations may not be sensitive, in which case having Location Services enabled is not necessary. In these scenarios, the use of the above restrictions settings is not necessary.

8.5 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.

Module / Algorithm Type	Algorithm Details
ESP	
Encryption	AES-128
IKEv2	
Encryption	AES-128 in CBC
Psuedo-Random-Function	PRF_HMAC_SHA2_256

Diffie Hellman Group	14 (2048 bits)
Integrity	HMAC_SHA2_256_128

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. Further information on the supported server configurations can be found at http://help.apple.com/deployment/ios/

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 Catalogue to distribute applications to their employees if required.

9.2 Cloud integration

As with iOS 7 and 8 previously, 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 enterprise applications without associating to an account. In addition, in iOS 9 Apple have removed the need for an Apple ID when installing applications when using VPP, further reducing the requirement for each user to have a provisioned Apple ID.

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 who wish to prevent this should implement controls to prevent users from enabling unneeded iCloud services on their device, thereby preventing enterprise data from being synchronised with Apple servers.

9.3 App groups

Apps and extensions that are produced by the same developer can potentially share content when configured as part of an ‘app group’. Sensitive application data could

therefore be made available to another application on the device, potentially being shared from managed to unmanaged applications. Third party applications should be reviewed to identify membership of an app group, and appropriate whitelisting should be applied where necessary.

9.4 Unmarked email domains

As with iOS 8, “unmarked” email domains can now be configured. When a user is composing an email using the system email client, any email address entered which does not match the configured domains will be highlighted (marked) in red. Administrators should consider using this functionality, to warn users who may be inadvertently attempting to send sensitive information to untrusted email addresses.

9.5 Managed Safari web domains

In iOS 8+ a list of domains can now be configured that the device will treat as “managed” in the Safari web browser. Using Safari, documents downloaded from these domains are then subject to Managed Open In rules and should not be accessible to unmanaged applications. Configuring these domains can help to stop sensitive documents from being trivially shared to other applications.

Legal information