Deploying iPhone and iPad
Security Overview

iOS, the operating system at the core of iPhone and iPad, is built upon layers of security. This enables iPhone and iPad to securely access corporate services and protect important data. iOS provides strong encryption for data in transmission, proven authentication methods for access to corporate services, and hardware encryption for all data at rest. iOS also provides secure protection through the use of passcode policies that can be delivered and enforced over the air. And if the device falls into the wrong hands, users and IT administrators can initiate a remote wipe command to erase private information.

When considering the security of iOS for enterprise use, it's helpful to understand the following:

- **Device security:** Methods that prevent unauthorized use of the device
- **Data security:** Protecting data at rest, even when a device is lost or stolen
- **Network security:** Networking protocols and the encryption of data in transmission
- **App security:** The secure platform foundation of iOS

These capabilities work in concert to provide a secure mobile computing platform.

Device security

- Strong passcodes
- Passcode expiration
- Passcode reuse history
- Maximum failed attempts
- Over-the-air passcode enforcement
- Progressive passcode timeout

Device Security

Establishing strong policies for access to iPhone and iPad is critical to protecting corporate information. Device passcodes are the front line of defense against unauthorized access and can be configured and enforced over the air. iOS devices use the unique passcode established by each user to generate a strong encryption key to further protect mail and sensitive application data on the device. Additionally, iOS provides secure methods to configure the device in an enterprise environment, where specific settings, policies, and restrictions must be in place. These methods provide flexible options for establishing a standard level of protection for authorized users.

Passcode policies

A device passcode prevents unauthorized users from accessing data or otherwise gaining access to the device. iOS allows you to select from an extensive set of passcode requirements to meet your security needs, including timeout periods, passcode strength, and how often the passcode must be changed.

The following passcode policies are supported:

- Require passcode on device
- Allow simple value
- Require alphanumeric value
- Minimum passcode length
- Minimum number of complex characters
- Maximum passcode age
- Time before auto-lock
- Passcode history
- Grace period for device lock
- Maximum number of failed attempts

Supported configurable policies and restrictions:

Device functionality
- Allow installing apps
- Allow Siri
- Allow Siri while locked
- Allow use of camera
- Allow FaceTime
- Allow screen capture
- Allow automatic syncing while roaming
- Allow voice dialing
- Allow In-App Purchase
- Require store password for all purchases
- Allow multiplayer gaming
- Allow adding Game Center friends

Applications
- Allow use of YouTube
- Allow use of iTunes Store
- Allow use of Safari
- Set Safari security preferences

iCloud
- Allow backup
- Allow document sync and key-value sync
- Allow Photo Stream

Security and privacy
- Allow diagnostic data to be sent to Apple
- Allow user to accept untrusted certificates
- Force encrypted backups

Content ratings
- Allow explicit music and podcasts
- Set ratings region
- Set allowed content ratings

Policy enforcement

The policies described previously can be set on iPhone and iPad in a number of ways. Policies can be distributed as part of a Configuration Profile for users to install. A profile can be defined so that deleting the profile is only possible with an administrative password, or you can define the profile so that it is locked to the device and cannot be removed without completely erasing all of the device contents. Additionally, passcode settings can be configured remotely using Mobile Device Management (MDM) solutions that can push policies directly to the device. This enables policies to be enforced and updated without any action by the user.

Alternatively, if the device is configured to access a Microsoft Exchange account, Exchange ActiveSync policies are pushed to the device over the air. Keep in mind that the available set of policies will vary depending on the version of Exchange (2003, 2007, or 2010). Refer to *Exchange ActiveSync and iOS Devices* for a breakdown of which policies are supported for your specific configuration.

Secure device configuration

Configuration Profiles are XML files that contain device security policies and restrictions, VPN configuration information, Wi-Fi settings, email and calendar accounts, and authentication credentials that permit iPhone and iPad to work with your enterprise systems. The ability to establish passcode policies along with device settings in a Configuration Profile ensures that devices within your enterprise are configured correctly and according to security standards set by your organization. And, because Configuration Profiles can be encrypted and locked, the settings cannot be removed, altered, or shared with others.

Configuration Profiles can be both signed and encrypted. Signing a Configuration Profile ensures that the settings it enforces cannot be altered in any way. Encrypting a Configuration Profile protects the profile's contents and permits installation only on the device for which it was created. Configuration Profiles are encrypted using CMS (Cryptographic Message Syntax, RFC 3852), supporting 3DES and AES 128.

The first time you distribute an encrypted Configuration Profile, you can install it via USB using the Configuration Utility or wirelessly via Over-the-Air Enrollment. In addition to these methods, subsequent encrypted Configuration Profiles can be delivered via email attachment, hosted on a website accessible to your users, or pushed to the device using MDM solutions.

Device restrictions

Device restrictions determine which features your users can access on the device. Typically, these involve network-enabled applications such as Safari, YouTube, or the iTunes Music Store, but restrictions can also control device functionality such as application installation or use of camera. Restrictions let you configure the device to meet your requirements, while permitting users to utilize the device in ways that are consistent with your business practices. Restrictions can be manually configured on each device, enforced using a Configuration Profile, or established remotely with MDM solutions. Additionally, like passcode policies, camera or web-browsing restrictions can be enforced over the air via Microsoft Exchange Server 2007 and 2010.

In addition to setting restrictions and policies on the device, the iTunes desktop application can be configured and controlled by IT. This includes disabling access to explicit content, defining which network services users can access within iTunes, and determining whether new software updates are available for users to install. For more information, refer to *Deploying iTunes for iOS Devices*.

Data Security

Data security
- Hardware encryption
- Data protection
- Remote wipe
- Local wipe
- Encrypted Configuration Profiles
- Encrypted iTunes backups

Protecting data stored on iPhone and iPad is important for any environment with sensitive corporate or customer information. In addition to encrypting data in transmission, iPhone and iPad provide hardware encryption for all data stored on the device, and additional encryption of email and application data with enhanced data protection.

If a device is lost or stolen, it's important to deactivate and erase the device. It's also a good idea to have a policy in place that will wipe the device after a defined number of failed passcode attempts, a key deterrent against attempts to gain unauthorized access to the device.

Encryption

iPhone and iPad offer hardware-based encryption. Hardware encryption uses 256-bit AES to protect all data on the device. Encryption is always enabled, and cannot be disabled by users.

Additionally, data backed up in iTunes to a user's computer can be encrypted. This can be enabled by the user, or enforced by using device restriction settings in Configuration Profiles.

iOS supports S/MIME in mail, enabling iPhone and iPad to view and send encrypted email messages. Restrictions can also be used to prevent mail messages from being moved between accounts or messages received in one account being forwarded from another.

Data protection

Building on the hardware encryption capabilities of iPhone and iPad, email messages and attachments stored on the device can be further secured by using data protection features built into iOS. Data protection leverages each user's unique device passcode in concert with the hardware encryption on iPhone and iPad to generate a strong encryption key. This key prevents data from being accessed when the device is locked, ensuring that critical information is secured even if the device is compromised.

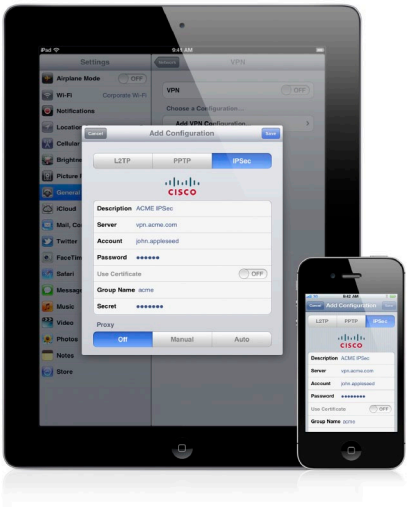
To turn on the data protection feature, simply establish a passcode on the device. The effectiveness of data protection is dependent on a strong passcode, so it is important to require and enforce a passcode stronger than four digits when establishing your corporate passcode policies. Users can verify that data protection is enabled on their device by looking at the passcode settings screen. Mobile Device Management solutions are able to query the device for this information as well.

These data protection APIs are also available to developers, and can be used to secure enterprise in-house or commercial application data.

Progressive passcode timeout
iPhone and iPad can be configured to automatically initiate a wipe after several failed passcode attempts. If a user repeatedly enters the wrong passcode, iOS will be disabled for increasingly longer intervals. After too many unsuccessful attempts, all data and settings on the device will be erased.

Remote wipe

iOS supports remote wipe. If a device is lost or stolen, the administrator or device owner can issue a remote wipe command that removes all data and deactivates the device. If the device is configured with an Exchange account, the administrator can initiate a remote wipe command using the Exchange Management Console (Exchange Server 2007) or Exchange ActiveSync Mobile Administration Web Tool (Exchange Server 2003 or 2007). Users of Exchange Server 2007 can also initiate remote wipe commands directly using Outlook Web Access. Remote wipe commands can also be initiated by MDM solutions even if Exchange corporate services are not in use.



Local wipe
Devices can also be configured to automatically initiate a local wipe after several failed passcode attempts. This protects against brute force attempts to gain access to the device. When a passcode is established, users have the ability to enable local wipe directly within the settings. By default, iOS will automatically wipe the device after 10 failed passcode attempts. As with other passcode policies, the maximum number of failed attempts can be established via a Configuration Profile, set by an MDM server, or enforced over the air via Microsoft Exchange ActiveSync policies.

iCloud
iCloud stores music, photos, apps, calendars, documents, and more, and automatically pushes them to all of a user's devices. iCloud also backs up information, including device settings, app data, and text and MMS messages, daily over Wi-Fi. iCloud secures your content by encrypting it when sent over the Internet, storing it in an encrypted format, and using secure tokens for authentication. Additionally, iCloud features, including Photo Stream, Document Sync, and Backup, can be disabled via a Configuration Profile. For more information on iCloud security and privacy, visit http://support.apple.com/kb/HT4865.

Network Security

Mobile users must be able to access corporate information networks from anywhere in the world, yet it's also important to ensure that users are authorized and that their data is protected during transmission. iOS provides proven technologies to accomplish these security objectives for both Wi-Fi and cellular data network connections.

In addition to your existing infrastructure, each FaceTime session and iMessage conversation is encrypted end to end. iOS creates a unique ID for each user, ensuring communications are encrypted, routed, and connected properly.

VPN
Many enterprise environments have some form of virtual private network (VPN) established. These secure network services are already deployed and typically require minimal setup and configuration to work with iPhone and iPad.

Out of the box, iOS integrates with a broad range of commonly used VPN technologies through support for Cisco IPSec, L2TP, and PPTP. iOS supports SSL VPN through applications from Juniper Networks, Cisco, SonicWALL, Check Point, Aruba Networks, and F5 Networks. Support for these protocols ensures the highest level of IP-based encryption for transmission of sensitive information.

In addition to enabling secure access to existing VPN environments, iOS offers proven methods for user authentication. Authentication via standard X.509 digital certificates provides users with streamlined access to company resources and a viable alternative to using hardware-based tokens. Additionally, certificate authentication enables iOS to take advantage of VPN On Demand, making the VPN authentication process transparent while still providing strong, credentialed access to network services. For enterprise environments in which a two-factor token is a requirement, iOS integrates with RSA SecurID and CRYPTOCard.

iOS supports network proxy configuration as well as split IP tunneling so that traffic to public or private network domains is relayed according to your specific company policies.

Network security
- Built-in Cisco IPSec, L2TP, PPTP VPN
- SSL VPN via App Store apps
- SSL/TLS with X.509 certificates
- WPA/WPA2 Enterprise with 802.1X
- Certificate-based authentication
- RSA SecurID, CRYPTOCard

VPN protocols
- Cisco IPSec
- L2TP/IPSec
- PPTP
- SSL VPN

Authentication methods
- Password (MSCHAPv2)
- RSA SecurID
- CRYPTOCard
- X.509 digital certificates
- Shared secret

802.1X authentication protocols
- EAP-TLS
- EAP-TTLS
- EAP-FAST
- EAP-SIM
- PEAP v0, v1
- LEAP

Supported certificate formats
iOS supports X.509 certificates with RSA keys. The file extensions .cer, .crt, and .der are recognized.

SSL/TLS
iOS supports SSL v3 as well as Transport Layer Security (TLS v1.0, 1.1, and 1.2), the next-generation security standard for the Internet. Safari, Calendar, Mail, and other Internet applications automatically start these mechanisms to enable an encrypted communication channel between iOS and corporate services.

WPA/WPA2
iOS supports WPA2 Enterprise to provide authenticated access to your enterprise wireless network. WPA2 Enterprise uses 128-bit AES encryption, giving users the highest level of assurance that their data will remain protected when they send and receive communications over a Wi-Fi network connection. And with support for 802.1X, iPhone and iPad can be integrated into a broad range of RADIUS authentication environments.

App Security

App security
- Runtime protection
- Mandatory code signing
- Keychain services
- CommonCrypto APIs
- Application data protection

iOS is designed with security at its core. It includes a "sandboxed" approach to application runtime protection and requires application signing to ensure that applications cannot be tampered with. iOS also has a secure framework that facilitates secure storage of application and network service credentials in an encrypted keychain. For developers, it offers a common crypto architecture that can be used to encrypt application data stores.

Runtime protection
Applications on the device are "sandboxed" so they cannot access data stored by other applications. In addition, system files, resources, and the kernel are shielded from the user's application space. If an application needs to access data from another application, it can only do so using the APIs and services provided by iOS. Code generation is also prevented.

Mandatory code signing
All iOS applications must be signed. The applications provided with the device are signed by Apple. Third-party applications are signed by the developer using an Apple-issued certificate. This ensures that applications haven't been tampered with or altered. Additionally, runtime checks are made to ensure that an application hasn't become untrusted since it was last used.

The use of custom or in-house applications can be controlled with a provisioning profile. Users must have the provisioning profile installed to execute the application. Provisioning profiles can be installed or revoked over the air using MDM solutions. Administrators can also restrict the use of an application to specific devices.

Secure authentication framework
iOS provides a secure, encrypted keychain for storing digital identities, user names, and passwords. Keychain data is partitioned so that credentials stored by third-party applications cannot be accessed by applications with a different identity. This provides the mechanism for securing authentication credentials on iPhone and iPad across a range of applications and services within the enterprise.

Common Crypto architecture
Application developers have access to encryption APIs that they can use to further protect their application data. Data can be symmetrically encrypted using proven methods such as AES, RC4, or 3DES. In addition, iPhone and iPad provide hardware acceleration for AES encryption and SHA1 hashing, maximizing application performance.

Application data protection
Applications can also take advantage of the built-in hardware encryption on iPhone and iPad to further protect sensitive application data. Developers can designate specific files for data protection, instructing the system to make the contents of the file cryptographically inaccessible to both the application and any potential intruders when the device is locked.

Managed apps
An MDM server can manage third-party apps from the App Store, as well as enterprise in-house applications. Designating an app as managed enables the server to specify whether the app and its data can be removed from the device by the MDM server. Additionally, the server can prevent managed app data from being backed up to iTunes and iCloud. This allows IT to manage apps that may contain sensitive business information with more control than apps downloaded directly by the user.

In order to install a managed app, the MDM server sends an installation command to the device. Managed apps require a user's acceptance before they are installed. For more information about managed apps, view the *Mobile Device Management Overview* at www.apple.com/business/mdm.

Revolutionary Devices, Security Throughout

iPhone and iPad provide encrypted protection of data in transit, at rest, and when backed up to iCloud or iTunes. Whether a user is accessing corporate email, visiting a private website, or authenticating to the corporate network, iOS provides assurance that only authorized users can access sensitive corporate information. And, with its support for enterprise-grade networking and comprehensive methods to prevent data loss, you can deploy iOS devices with confidence that you are implementing proven mobile device security and data protection.