iPhone in Business
Security Overview

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

Data protection
- Remote wipe
- Local wipe
- Encrypted configuration profiles
- Encrypted iTunes backups
- Hardware encryption (iPhone 3GS)

Network security
- Cisco IPSec, L2TP, PPTP VPN protocols
- SSL/TLS with X.509 certificates
- WPA/WPA2 Enterprise with 802.1X
- Certificate-based authentication
- RSASecurID, CRYPTOCard

Platform security
- Runtime protection
- Mandatory code signing
- Keychain services
- Common Crypto APIs

iPhone can securely access corporate services and protect data on the device. It provides strong encryption for data in transmission, proven authentication methods for access to corporate services, and for iPhone 3GS, hardware encryption for all data stored on the device. iPhone also provides secure protection through the use of passcode policies that can be enforced and delivered over-the-air. And if the device falls into the wrong hands, users and IT administrators can initiate a remote wipe command to help ensure that private information is erased.

When considering the security of iPhone for enterprise use, it is helpful to understand the following:

- Methods that prevent unauthorized use of the device
- Protecting data at rest, including when a device is lost or stolen
- Networking protocols and the encryption of data in transmission
- Secure platform foundation of iPhone OS

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

Device Control and Protection

Establishing strong policies for access to iPhone is critical to protecting corporate information. Passcode enforcement is the front line of defense against unauthorized access and can be configured and enforced over-the-air. Additionally, iPhone 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 stored on iPhone or otherwise gaining access to the device. iPhone OS 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 Microsoft Exchange ActiveSync passcode policies are supported:

- Enforce password on device
- Minimum password length
- Maximum failed password attempts
- Require both numbers and letters
- Inactivity time in minutes

With Microsoft Exchange Server 2007, these additional passcode policies are supported:

- Allow or prohibit simple password
- Password expiration
- Password history
- Policy refresh interval
- Minimum number of complex characters in a password

Policy Enforcement

The policies described above can be set on iPhone in two ways. If the device is configured to access a Microsoft Exchange account, the Exchange ActiveSync policies are pushed to the device over-the-air. This enables policies to be enforced and updated without any action by the user.

Policies can also 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.

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 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 both 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.

For the first-time distribution of encrypted configuration profiles, you'll need to install them via USB sync using the iPhone Configuration Utility or via Over-the-Air Enrollment and Distribution. In addition to these methods, subsequent distribution of encrypted configuration profiles can be delivered via email attachment or hosted on a website accessible to your users.

Device Restrictions

Device restrictions determine which iPhone features your users can access on the device. Typically, these involve network-enabled applications such as Safari, YouTube, or the iTunes Store, but restrictions can also control things such as application installation, or use of the camera. Device restrictions let you configure the device to meet your requirements, as well as permit users to utilize the device in ways that are consistent with your business practices. Restrictions are enforced using a configuration profile, or they can be manually configured on each device. Additionally, camera restrictions can be enforced over-the-air via Microsoft Exchange Server 2007.

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 whether new software updates are available for them to install.

Available restrictions

- Access to explicit media in iTunes Store
- Use of Safari
- Use of YouTube
- Access to iTunes Store
- Use of App Store and iTunes to install applications
- Use of the camera (can also be controlled with an Exchange policy)

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

Data Protection

Protecting data stored on iPhone is important for any environment with a high level of sensitive corporate or customer information. In addition to encrypting data in transmission, iPhone 3GS provides hardware encryption for data stored on the device.

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 3GS offers hardware-based encryption. iPhone 3GS hardware encryption uses AES 256 bit encoding 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. When an encrypted configuration profile is stored on the user's device, this capability is enforced automatically. And to further protect application data, developers have access to APIs that enable them to encrypt data within their own application data stores.

Remote Wipe

iPhone 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.

Local Wipe

Devices can also be configured to automatically initiate a local wipe after several failed passcode attempts. This is a key deterrent against brute force attempts to gain access to the device. By default, iPhone will automatically wipe the device after 10 failed pass-code attempts. As with other passcode policies, the maximum number of failed attempts can be established via a configuration profile or enforced over-the-air via Microsoft Exchange ActiveSync policies.

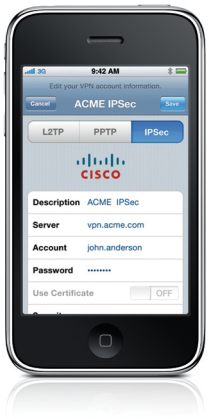
Secure Network Communication

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. iPhone provides proven technologies to accomplish these security objectives for both Wi-Fi and cellular data network connections.

VPN

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

iPhone integrates with a broad range of commonly used VPN technologies through support for Cisco IPSec, L2TP, and PPTP. Support for these protocols ensures the highest level of IP-based encryption for transmission of sensitive information. iPhone 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.



VPN protocols
- Cisco IPSec
- L2TP/IPSec
- PPTP

Authentication methods
- Password (MSCHAPv2)
- RSA SecureID
- 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
iPhone supports X.509 certificates with RSA keys. The file extensions .cer, .crt, and .der are recognized.

In addition to enabling secure access to existing VPN environments, iPhone 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 iPhone 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, iPhone integrates with RSA SecureID and CRYPTOCard.

SSL/TLS
iPhone supports SSL v3 as well as Transport Layer Security (TLS v1), 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 iPhone and corporate services.

WPA/WPA2
iPhone 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 can be integrated into a broad range of RADIUS authentication environments.

Secure Platform Foundation

iPhone OS is a platform designed with security at its core. It includes a "sandboxed" approach to application runtime protection and requires mandatory application signing to ensure that applications cannot be tampered with. iPhone OS 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 iPhone OS. Code generation is also prevented.

Mandatory Code Signing
All iPhone 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. Administrators can also restrict the use of an application to specific devices.

Secure Authentication Framework
iPhone 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 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 provides hardware acceleration for AES and SHA1 encryption, maximizing application performance.

Revolutionary Phone, Secure Throughout

iPhone 3GS provides encrypted protection of data in transit, at rest, or backed up to iTunes. Whether a user is accessing corporate email, visiting a private website, or authenticating to the corporate network, iPhone provides assurance that only authorized users can access sensitive corporate information. And, with support for enterprise-grade networking and comprehensive methods to prevent data loss, iPhone can be deployed with confidence that you are implementing proven mobile device security and data protection methods.

Additional Resources

Enterprise Deployment Guide
http://manuals.info.apple.com/en_US/Enterprise_Deployment_Guide.pdf

Enterprise Deployment Resource and Scenarios
http://www.apple.com/iphone/enterprise/integration.html