iPhone in Business

Deployment Scenarios

June 2010

Learn how iPhone integrates seamlessly into enterprise environments with these deployment scenarios.

- Microsoft Exchange ActiveSync
- Standards-based Servers
- Virtual Private Networks
- Wi-Fi
- Digital Certificates
- Security Overview
- Mobile Device Management
- Deploying iTunes

iPhone in Business
Exchange ActiveSync

Supported Exchange ActiveSync security policies

- Remote wipe
- Enforce password on device
- Minimum password length
- Maximum failed password attempts (before local wipe)
- Require both numbers and letters
- Inactivity time in minutes (1 to 60 minutes)

Additional Exchange ActiveSync policies (for Exchange 2007 and 2010 only)

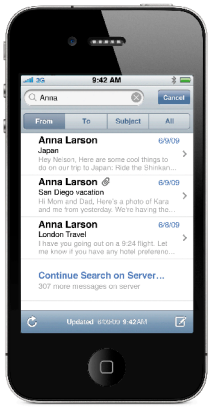
- Allow or prohibit simple password
- Password expiration
- Password history
- Policy refresh interval
- Minimum number of complex characters in password
- Require manual syncing while roaming
- Allow camera
- Allow web browsing

iPhone communicates directly with your Microsoft Exchange Server via Microsoft Exchange ActiveSync (EAS), enabling push email, calendar, and contacts. Exchange ActiveSync also provides users with access to the Global Address List (GAL), and provides administrators with passcode policy enforcement and remote wipe capabilities. iPhone supports both basic and certificate-based authentication for Exchange ActiveSync. If your company currently enables Exchange ActiveSync, you have the necessary services in place to support iPhone—no additional configuration is required. If you have Exchange Server 2003, 2007, or 2010 but your company is new to Exchange ActiveSync, review the following steps.

Exchange ActiveSync Setup

Network configuration overview

- Check to ensure port 443 is open on the firewall. If your company allows Outlook Web Access, port 443 is most likely already open.
- On the Front-End Server, verify that a server certificate is installed and enable SSL for the Exchange ActiveSync virtual directory in IIS.
- If you're using a Microsoft Internet Security and Acceleration (ISA) Server, verify that a server certificate is installed and update the public DNS to resolve incoming connections.
- Make sure the DNS for your network returns a single, externally routable address to the Exchange ActiveSync server for both intranet and Internet clients. This is required so the device can use the same IP address for communicating with the server when both types of connections are active.
- If you're using a Microsoft ISA Server, create a web listener as well as an Exchange web client access publishing rule. See Microsoft's documentation for details.
- For all firewalls and network appliances, set the Idle Session Timeout to 30 minutes. For information about heartbeat and timeout intervals, refer to the Microsoft Exchange documentation at http://technet.microsoft.com/en-us/library/cc182270.aspx.
- Configure mobile features, policies, and device security settings using the Exchange System Manager. For Exchange Server 2007 and 2010, this is done in the Exchange Management Console.
- Download and install the Microsoft Exchange ActiveSync Mobile Administration Web Tool, which is necessary to initiate a remote wipe. For Exchange Server 2007 and 2010, remote wipe can also be initiated using Outlook Web Access or the Exchange Management Console.



Other Exchange ActiveSync services

- Global Address List lookup
- Accept and create calendar invitations
- Sync Reply and Forward flags with Exchange Server 2010
- Mail search on Exchange Server 2007 and 2010
- Support for multiple Exchange ActiveSync accounts
- Certificate-based authentication
- Email push to selected folders
- Autodiscover

Basic authentication (username and password)

- Enable Exchange ActiveSync for specific users or groups using the Active Directory service. These are enabled by default for all mobile devices at the organizational level in Exchange Server 2003, 2007, and 2010. For Exchange Server 2007 and 2010, see Recipient Configuration in the Exchange Management Console.
- By default, Exchange ActiveSync is configured for basic user authentication. It's recommended that you enable SSL for basic authentication to ensure credentials are encrypted during authentication.

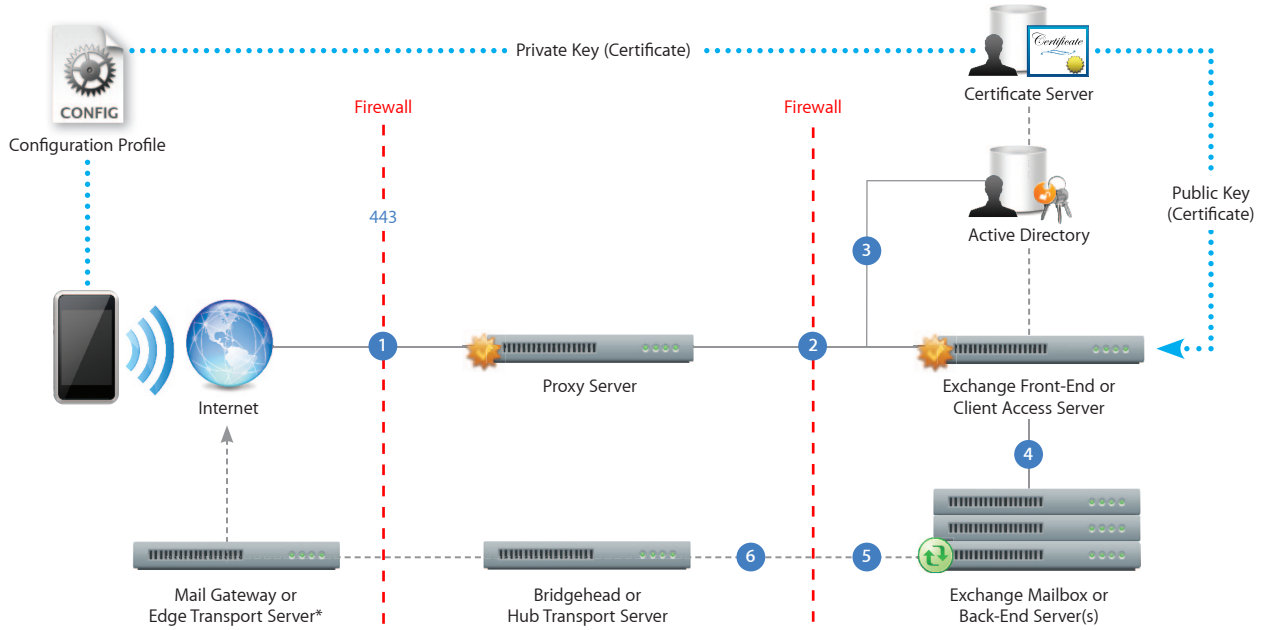
Certificate-based authentication

- Install enterprise certificate services on a member server or domain controller in your domain (this will be your certificate authority server).
- Configure IIS on your Exchange front-end server or Client Access Server to accept certificate-based authentication for the Exchange ActiveSync virtual directory.
- To allow or require certificates for all users, turn off "Basic authentication" and select either "Accept client certificates" or "Require client certificates."
- Generate client certificates using your certificate authority server. Export the public key and configure IIS to use this key. Export the private key and use a Configuration Profile to deliver this key to iPhone. Certificate-based authentication can only be configured using a Configuration Profile.

  For more information on certificate services, please refer to resources available from Microsoft.

Exchange ActiveSync Deployment Scenario

This example shows how iPhone connects to a typical Microsoft Exchange Server 2003, 2007, or 2010 deployment.



*Depending on your network configuration, the Mail Gateway or Edge Transport Server may reside within the perimeter network (DMZ).

1. iPhone requests access to Exchange ActiveSync services over port 443 (HTTPS). (This is the same port used for Outlook Web Access and other secure web services, so in many deployments this port is already open and configured to allow SSL encrypted HTTPS traffic.)
2. ISA provides access to the Exchange Front-End or Client Access Server. ISA is configured as a proxy, or in many cases a reverse proxy, to route traffic to the Exchange Server.
3. Exchange Server authenticates the incoming user via the Active Directory service and the certificate server (if using certificate-based authentication).
4. If the user provides the proper credentials and has access to Exchange ActiveSync services, the Front-End Server establishes a connection to the appropriate mailbox on the Back-End Server (via the Active Directory Global Catalog).
5. The Exchange ActiveSync connection is established. Updates/changes are pushed to iPhone over the air, and any changes made on iPhone are reflected on the Exchange Server.
6. Sent mail items on iPhone are also synchronized with the Exchange Server via Exchange ActiveSync (step 5). To route outbound email to external recipients, mail is typically sent through a Bridgehead (or Hub Transport) Server to an external Mail Gateway (or Edge Transport Server) via SMTP. Depending on your network configuration, the external Mail Gateway or Edge Transport Server could reside within the perimeter network or outside the firewall.

© 2010 Apple Inc. All rights reserved. Apple, the Apple logo, and iPhone are trademarks of Apple Inc., registered in the U.S. and other countries. Other product and company names mentioned herein may be trademarks of their respective companies. Product specifications are subject to change without notice. This material is provided for information purposes only; Apple assumes no liability related to its use. June 2010 L419822A

iPhone in Business
Standards-Based Services

Common ports

- IMAP/SSL: 993
- SMTP/SSL: 587
- LDAP/SSL: 636
- CalDAV/SSL: 8443, 443
- CardDAV/SSL: 8843, 443

IMAP or POP-enabled mail solutions
iPhone supports industry-standard IMAP4- and POP3-enabled mail servers on a range of server platforms, including Windows, UNIX, Linux, and Mac OS X.

CalDAV and CardDAV standards
iPhone supports the CalDAV calendaring and CardDAV contacts protocols. Both protocols have been standardized by the IETF. More information can be found through the CalConnect consortium at http://caldav.calconnect.org/ and http://carddav.calconnect.org/.

With support for the IMAP mail protocol, LDAP directory services, and CalDAV calendaring and CardDAV contacts protocols, iPhone can integrate with just about any standards-based mail, calendar, and contacts environment. And if your network environment is configured to require user authentication and SSL, iPhone provides a secure approach to accessing standards-based corporate email, calendar, and contacts.

In a typical deployment, iPhone establishes direct access to IMAP and SMTP mail servers to receive and send email over the air, and can also wirelessly sync notes with IMAP-based servers. iPhone can connect to your company's LDAPv3 corporate directories, giving users access to corporate contacts in the Mail, Contacts, and SMS applications. Synchronization with your CalDAV server allows iPhone users to wirelessly create and accept calendar invitations and receive calendar updates. And CardDAV support allows your users to maintain a set of contacts synced with your CardDAV server using the vCard format. All network servers can be located within a DMZ subnetwork, behind a corporate firewall, or both. With SSL, iPhone supports 128-bit encryption and X.509 root certificates issued by the major certificate authorities.

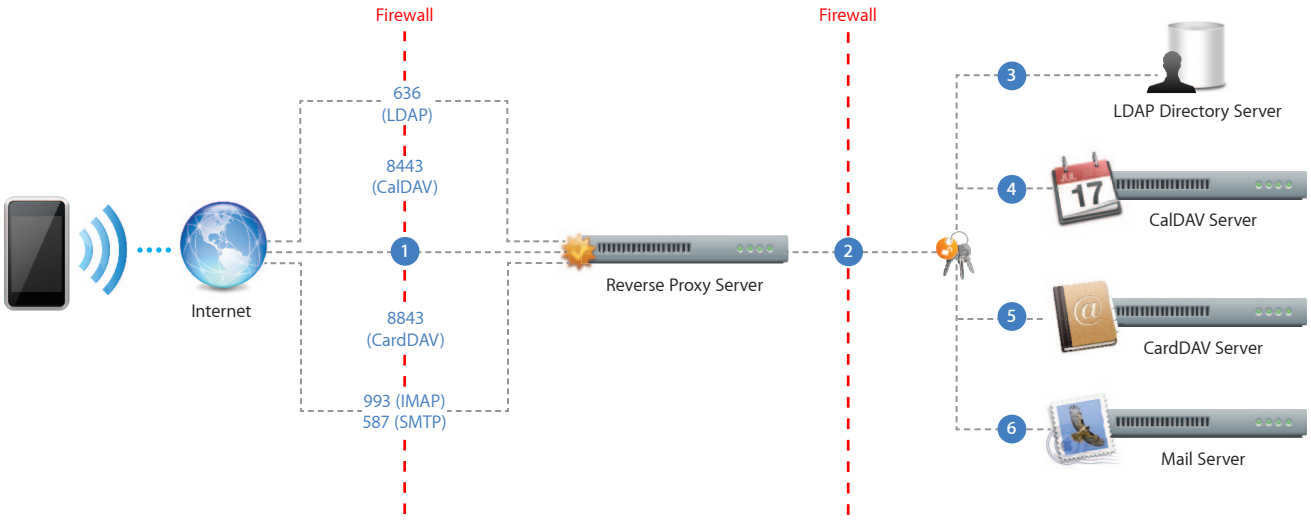
Network Setup

Your IT or network administrator will need to complete these key steps to enable access from iPhone to IMAP, LDAP, CalDAV, and CardDAV services:

- Open the appropriate ports on the firewall. Common ports include 993 for IMAP mail, 587 for SMTP mail, 636 for LDAP directory services, 8443 for CalDAV calendaring, and 8843 for CardDAV contacts. It's also recommended that communication between your proxy server and your back-end IMAP, LDAP, CalDAV and CardDAV servers be set to use SSL and that digital certificates on your network servers be signed by a trusted certificate authority (CA) such as VeriSign. This important step ensures that iPhone recognizes your proxy server as a trusted entity within your corporate infrastructure.
- For outbound SMTP email, port 587, 465, or 25 must be opened to allow email to be sent from iPhone. iPhone automatically checks for port 587, then 465, and then 25. Port 587 is the most reliable, secure port because it requires user authentication. Port 25 does not require authentication, and some ISPs block this port by default to prevent spam.

Deployment Scenario

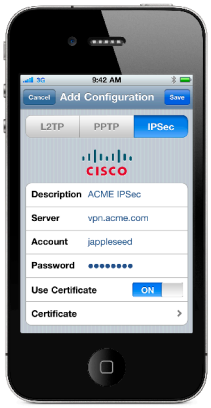
This example shows how iPhone connects to a typical IMAP, LDAP, CalDAV and CardDAV deployment.



1. iPhone requests access to network services over the designated ports.
2. Depending on the service, iPhone users must authenticate either with the reverse proxy or directly with the server to obtain access to corporate data. In all cases, connections are relayed by the reverse proxy, which functions as a secure gateway, typically behind the company's Internet firewall. Once authenticated, users can access their corporate data on the back-end servers.
3. iPhone provides lookup services on LDAP directories, giving users the ability to search for contacts and other address book information on the LDAP server.
4. For CalDAV calendars, users can access and update calendars on iPhone.
5. CardDAV contacts are stored on the server and can also be accessed locally on iPhone. Changes to fields in CardDAV contacts are synced back to the CardDAV server.
6. For IMAP mail services, existing and new messages can be read on iPhone through the proxy connection with the mail server. Outgoing mail on iPhone is sent to the SMTP server, with copies placed in the user's Sent folder.

© 2010 Apple Inc. All rights reserved. Apple, the Apple logo, iPhone, and Mac OS are trademarks of Apple Inc., registered in the U.S. and other countries. UNIX is a registered trademark of The Open Group. Other product and company names mentioned herein may be trademarks of their respective companies. Product specifications are subject to change without notice. This material is provided for information purposes only; Apple assumes no liability related to its use. June 2010 L419827A

iPhone in Business
Virtual Private Networks (VPN)



Secure access to private corporate networks is available on iPhone using established industry-standard VPN protocols. Users can easily connect to enterprise systems via the built-in VPN client or through third-party applications from Juniper and Cisco.

Out of the box, iPhone supports Cisco IPSec, L2TP over IPSec, and PPTP. If your organization supports one of these protocols, no additional network configuration or third-party applications are required to connect iPhone to your VPN.

Additionally, iPhone supports SSL VPN, enabling access to Juniper SA Series and Cisco ASA SSL VPN servers. Users simply download a VPN client application developed by Juniper or Cisco from the App Store to get started. Like other VPN protocols supported on iPhone, SSL VPN can be configured manually on iPhone or via Configuration Profile.

iPhone supports industry-standard technologies such as IPv6, proxy servers, and split-tunneling, providing a rich VPN experience when connecting to corporate networks. And iPhone works with a variety of authentication methods including password, two-factor token, and digital certificates. To streamline the connection in environments where certificate-based authentication is used, iPhone features VPN On Demand, which dynamically initiates a VPN session when connecting to specified domains.

Supported Protocols and Authentication Methods

SSL VPN
Supports user authentication by password, two-factor token, and certificates.

Cisco IPSec
Supports user authentication by password, two-factor token, and machine authentication by shared secret and certificates.

L2TP over IPSec
Supports user authentication by MS-CHAP v2 Password, two-factor token, and machine authentication by shared secret.

PPTP
Supports user authentication by MS-CHAP v2 Password and two-factor token.

VPN On Demand

For configurations using certificate-based authentication, iPhone supports VPN On Demand. VPN On Demand will establish a connection automatically when accessing predefined domains, providing a seamless VPN connectivity experience for iPhone users.

This is a feature of iOS that does not require additional server configuration. The configuration of VPN On Demand takes place via a Configuration Profile or can be configured manually on the device.

The VPN On Demand options are:

Always
Initiates a VPN connection for any address that matches the specified domain.

Never
Does not initiate a VPN connection for addresses that match the specified domain, but if VPN is already active, it may be used.

Establish if needed
Initiates a VPN connection for addresses that match the specified domain only after a DNS look-up has failed.

VPN Setup

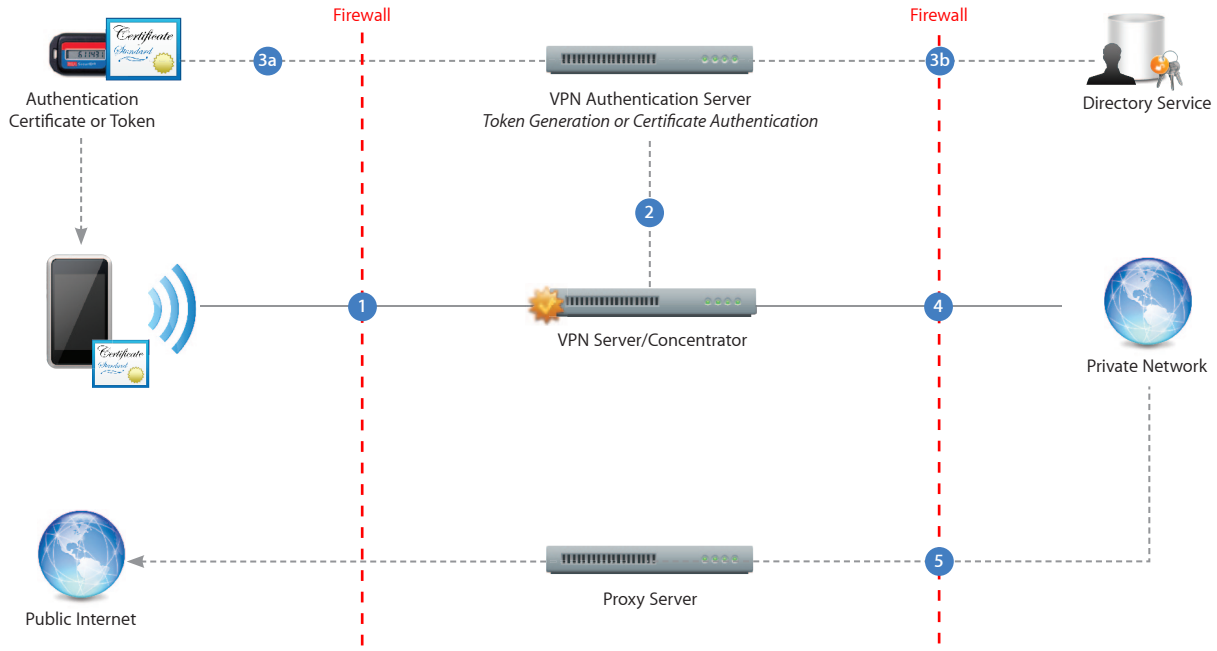
- iPhone integrates with many existing VPN networks, with minimal configuration necessary. The best way to prepare for deployment is to check whether iPhone supports your company's existing VPN protocols and authentication methods.
- It's recommended that you review the authentication path to your authentication server to make sure standards supported by iPhone are enabled within your implementation.
- If you plan to use certificate-based authentication, ensure you have your public key infrastructure configured to support device- and user-based certificates with the corresponding key distribution process.
- If you want to configure URL-specific proxy settings, place a PAC file on a web server that is accessible with the basic VPN settings and ensure that it is hosted with the application/x-ns-proxy-autoconfig MIME type.

Proxy Setup

For all configurations you can also specify a VPN proxy. To configure a single proxy for all connections, use the Manual setting and provide the address, port, and authentication if necessary. To provide the device with an auto-proxy configuration file using PAC or WPAD, use the Auto setting. For PACS, specify the URL of the PACS file. For WPAD, iPhone will query DHCP and DNS for the appropriate settings.

Deployment Scenario

The example depicts a typical deployment with a VPN server/concentrator as well as an authentication server controlling access to enterprise network services.

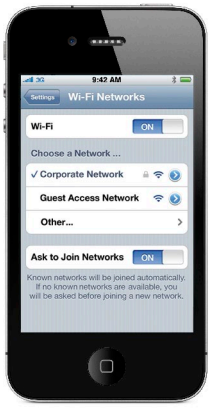


1. iPhone requests access to network services.
2. The VPN server/concentrator receives the request and then passes it to the authentication server.
3. In a two-factor token environment, the authentication server would then manage a time-synchronized token key generation with the key server. If a certificate authentication method is deployed, an identity certificate needs to be distributed to iPhone prior to authentication. If a password method is deployed, the authentication process proceeds with user validation.
4. Once a user is authenticated, the authentication server validates user and group policies.
5. After user and group policies are validated, the VPN server provides tunneled and encrypted access to network services.
6. If a proxy server is in use, iPhone connects through the proxy server for access to information outside the firewall.

For more information regarding VPN on iPhone, visit www.apple.com/iphone/business/integration

© 2010 Apple Inc. All rights reserved. Apple, the Apple logo, and iPhone are trademarks of Apple Inc., registered in the U.S. and other countries. App Store is a service mark of Apple Inc. Other product and company names mentioned herein may be trademarks of their respective companies. Product specifications are subject to change without notice. This material is provided for information purposes only; Apple assumes no liability related to its use. June 2010 L419828A

iPhone in Business
Wi-Fi



Wireless security protocols

- WEP
- WPA Personal
- WPA Enterprise
- WPA2 Personal
- WPA2 Enterprise

802.1X authentication methods

- EAP-TLS
- EAP-TTLS
- EAP-FAST
- EAP-SIM
- PEAPv0 (EAP-MS-CHAP v2)
- PEAPv1 (EAP-GTC)
- LEAP

Out of the box, iPhone can securely connect to corporate or guest Wi-Fi networks, making it quick and simple to join available wireless networks whether you're on campus or on the road.

iPhone supports industry standard wireless network protocols, including WPA2 Enterprise, ensuring corporate wireless networks can be configured quickly and accessed securely. WPA2 Enterprise uses 128-bit AES encryption, a proven, block-based encryption method, providing users with the highest level of assurance that their data will remain protected.

With support for 802.1X, iPhone can be integrated into a broad range of RADIUS authentication environments. 802.1X wireless authentication methods supported on iPhone include EAP-TLS, EAP-TTLS, EAP-FAST, EAP-SIM, PEAPv0, PEAPv1, and LEAP.

Users can set iPhone to join available Wi-Fi networks automatically. Wi-Fi networks that require login credentials or other information can be quickly accessed without opening a separate browser session, from Wi-Fi settings or within applications such as Mail. And low-power, persistent Wi-Fi connectivity allows iPhone applications to use Wi-Fi networks to deliver push notifications.

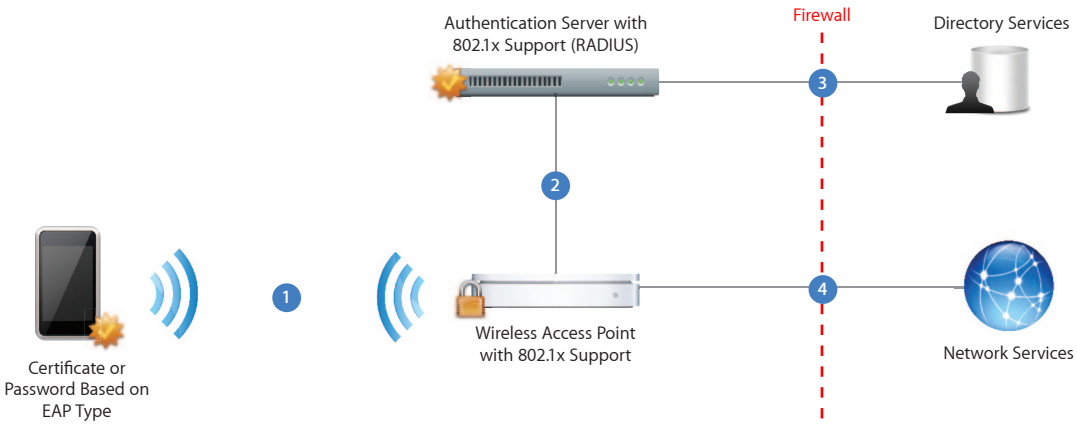
For quick setup and deployment, wireless network, security, and authentication settings can be configured using Configuration Profiles.

WPA2 Enterprise Setup

- Verify network appliances for compatibility and select an authentication type (EAP type) supported by iPhone.
- Check that 802.1X is enabled on the authentication server and, if necessary, install a server certificate and assign network access permissions to users and groups.
- Configure wireless access points for 802.1X authentication and enter the corresponding RADIUS server information.
- If you plan to use certificate-based authentication, configure your public key infrastructure to support device- and user-based certificates with the corresponding key distribution process.
- Verify certificate format and authentication server compatibility. iPhone supports PKCS#1 (.cer, .crt, .der) and PKCS#12.
- For additional documentation regarding wireless networking standards and Wi-Fi Protected Access (WPA), visit www.wi-fi.org.

WPA2 Enterprise/802.1X Deployment Scenario

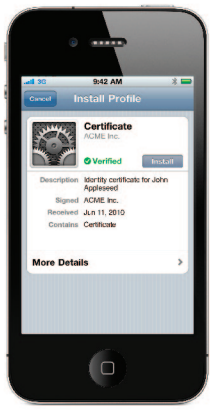
This example depicts a typical secure wireless deployment that takes advantage of RADIUS-based authentication.



1. iPhone requests access to the network. iPhone initiates the connection in response to a user selecting an available wireless network, or automatically initiates a connection after detecting a previously configured network.
2. After the request is received by the access point, the request is passed to the RADIUS server for authentication.
3. The RADIUS server validates the user account utilizing the directory service.
4. Once the user is authenticated, the access point provides network access with policies and permissions as instructed by the RADIUS server.

© 2010 Apple Inc. All rights reserved. Apple, the Apple logo, and iPhone are trademarks of Apple Inc., registered in the U.S. and other countries. Other product and company names mentioned herein may be trademarks of their respective companies. Product specifications are subject to change without notice. This material is provided for information purposes only; Apple assumes no liability related to its use. June 2010 L419830A

iPhone in Business
Digital Certificates



Supported certificate and identity formats:

- iPhone supports X.509 certificates with RSA keys.
- The file extensions .cer, .crt, .der, .p12 and .pfx are recognized.

Root certificates

Out of the box, iPhone includes a number of preinstalled root certificates. To view a list of the preinstalled system roots, see the Apple Support article at http://support.apple.com/kb/HT3580. If you are using a root certificate that is not preinstalled, such as a self-signed root certificate created by your company, you can distribute it to iPhone using one of the methods listed in the "Distributing and Installing Certificates" section of this document.

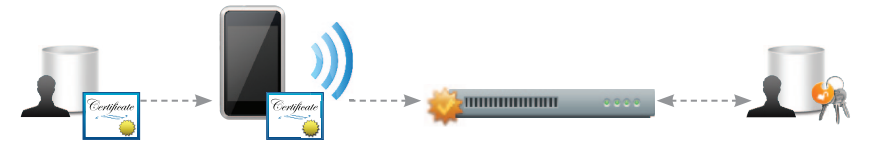
iPhone supports digital certificates, giving business users secure, streamlined access to corporate services. A digital certificate is composed of a public key, information about the user, and the certificate authority that issued the certificate. Digital certificates are a form of identification that enables streamlined authentication, data integrity, and encryption.

On iPhone, certificates can be used in a variety of ways. Signing data with a digital certificate helps to ensure that information cannot be altered. Certificates can also be used to guarantee the identity of the author or "signer." Additionally, they can be used to encrypt configuration profiles and network communications to further protect confidential or private information.

Using Certificates on iPhone

Digital certificates

Digital certificates can be used to securely authenticate users to corporate services without the need for user names, passwords or soft tokens. On iPhone, certificate-based authentication is supported for access to Microsoft Exchange ActiveSync, VPN, and Wi-Fi networks.



Server certificates

Digital certificates can also be used to validate and encrypt network communications. This provides secure communication to both internal and external websites. The Safari browser can check the validity of an X.509 digital certificate and set up a secure session with up to 256-bit AES encryption. This verifies that the site's identity is legitimate and that communication with the website is protected to help prevent interception of personal or confidential data.

Distributing and Installing Certificates

Distributing certificates to iPhone is simple. When a certificate is received, users simply tap to review the contents, then tap to add the certificate to their device. When an identity certificate is installed, users are prompted for the passphrase that protects it. If a certificate's authenticity cannot be verified, users will be presented with a warning before it is added to their device.

Installing certificates via Configuration Profiles

If Configuration Profiles are being used to distribute settings for corporate services such as Exchange, VPN, or Wi-Fi, certificates can be added to the profile to streamline deployment.

Installing certificates via Mail or Safari

If a certificate is sent in an email, it will appear as an attachment. Safari can be used to download certificates from a web page. You can host a certificate on a secured website and provide users with the URL where they can download the certificate onto their devices.

Installation via the Simple Certificate Enrollment Protocol (SCEP)

SCEP is designed to provide a simplified process to handle certificate distribution for large-scale deployments. This enables Over-the-Air Enrollment of digital certificates on iPhone that can then be used for authentication to corporate services, as well as enrollment with a mobile device management server.

For more information on SCEP and Over-the-Air Enrollment, visit www.apple.com/iphone/business/integration.

Certificate removal and revocation

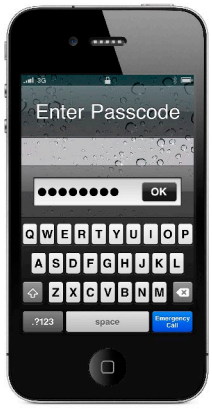
To manually remove a certificate that has been installed, choose Settings > General > Profiles. If you remove a certificate that is required for accessing an account or network, the device will no longer be able to connect to those services.

To remove certificates over the air, a mobile device management server can be used. This server can view all certificates on a device and remove ones it has installed.

Additionally, the Online Certificate Status Protocol (OCSP) is supported to check the status of certificates. When an OSCP-enabled certificate is used, iPhone validates it to make sure that it has not been revoked before completing the requested task.

© 2010 Apple Inc. All rights reserved. Apple, the Apple logo, Safari, and iPhone are trademarks of Apple Inc., registered in the U.S. and other countries. Other product and company names mentioned herein may be trademarks of their respective companies. Product specifications are subject to change without notice. This material is provided for information purposes only; Apple assumes no liability related to its use. June 2010 L419821A

iPhone in Business
Security Overview



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

Data security
- Remote wipe
- Local wipe
- Encrypted configuration profiles
- Encrypted iTunes backups
- Hardware encryption
- Data protection

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

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

iPhone can securely access corporate services and protect data on the device. iPhone provides strong encryption for data in transmission, proven authentication methods for access to corporate services, and hardware encryption for all data stored on the device. iPhone 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 iPhone 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
- Application Security: The secure platform foundation of iOS

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

Device Security

Establishing strong policies for access to iPhone 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. iPhone uses 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, 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. iOS 4 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
- Auto-lock
- Passcode history

- Grace period for device lock
- Maximum number of failed attempts

Policy Enforcement

The policies described above can be set on iPhone 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 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 the Enterprise Deployment Guide for a breakdown of what 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 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.

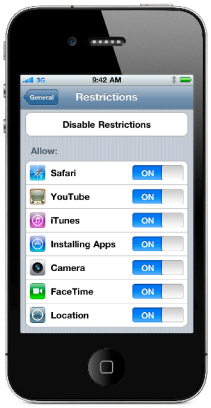
Configuration profiles can be both signed and encrypted. Signing a configuration profile ensures that the settings it enforces cannot be altered in any way. Encrypting a configuration profile protects the profile's contents and permits installation only on the device for which it was created. Configuration 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 install them via USB sync using the iPhone Configuration Utility or wirelessly via Over-the-Air Enrollment. In addition to these methods, subsequent distribution of encrypted configuration profiles can be delivered via email attachment, hosted on a website accessible to your users, or pushed to the device using Mobile Device Management solutions.

Device Restrictions

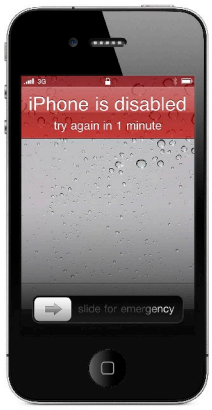
Device restrictions determine which iPhone features your users can access on the device. Typically, these involve network-enabled applications such as Safari, YouTube, or the iTunes Store, but restrictions can also control device functionality such as application installation, or use of the camera. Device 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 Mobile Device Management solutions. Additionally, camera and 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 whether new software updates are available for them to install.



Available restrictions

- Access to iTunes Music Store
- Access to explicit media and content ratings in iTunes Store
- Use of Safari and security preferences
- Use of YouTube
- Use of App Store and in-app purchase
- Installing apps
- Ability to screen capture
- Automatic sync while roaming
- Use of voice dialing
- Enforce encrypted iTunes backups
- Use of the camera



Progressive passcode timeout
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 Security

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 provides hardware encryption for 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 3GS and new devices offer hardware-based encryption. iPhone 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. This can be enabled by the user, or enforced by using device restriction settings in configuration profiles.

Data Protection

Building on the hardware encryption capabilities of iPhone 3GS and newer devices, email messages and attachments stored on the device can be further secured by using data protection features built into iOS 4. Data protection leverages each user's unique device passcode in concert with the hardware encryption on iPhone 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.

Enabling data protection requires that existing devices be fully restored from backup when upgrading to iOS 4. New devices that ship with iOS 4 will already have this capability. 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 Mangement solutions are able to query the device for this information as well.

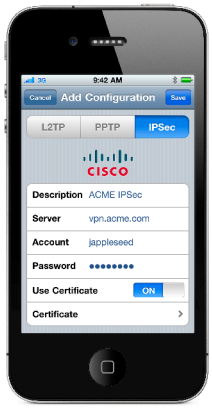
These data protection APIs are also available to developers, and can be used to secure enterprise in-house or commercial application data.

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. Remote wipe commands can also be initiated by Mobile Device Management 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 on iPhone. By default, iPhone 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 a Mobile Device Management server, or enforced over the air via Microsoft Exchange ActiveSync policies.



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
iPhone supports X.509 certificates with RSA keys. The file extensions .cer, .crt, and .der are recognized.

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. 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.

Out of the box, iPhone integrates with a broad range of commonly used VPN technologies through support for Cisco IPSec, L2TP, and PPTP. Additionally, iPhone supports SSL VPN through applications from Juniper and Cisco. 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, 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 SecurID and CRYPTOCard.

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.

SSL/TLS

iPhone supports SSL v3 as well as Transport Layer Security (TLS v1.0), 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.

Application Security

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 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. Provisioning profiles can be installed or revoked over the air using Mobile Device Management solutions. 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 encryption and SHA1 hashing, maximizing application performance.

Application Data Protection
Applications can also take advantage of the built-in hardware encryption on iPhone 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 to any potential intruders when the device is locked.

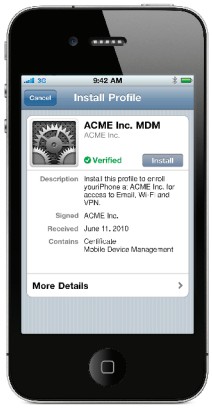
Revolutionary Phone, Secure Throughout

iPhone provides encrypted protection of data in transit, at rest, and when 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 its support for enterprise-grade networking and comprehensive methods to prevent data loss, you can deploy iPhone with confidence that you are implementing proven mobile device security and data protection.

For additional information and deployment resources for iPhone visit:
www.apple.com/iphone/business/integration/

© 2010 Apple Inc. All rights reserved. Apple, the Apple logo, iPhone, iTunes, and Safari are trademarks of Apple Inc., registered in the U.S. and other countries. App Store is a service mark of Apple Inc. iTunes Music Store is a service mark of Apple Inc., registered in the U.S. and other countries. Other product and company names mentioned herein may be trademarks of their respective companies. Product specifications are subject to change without notice. This material is provided for information purposes only; Apple assumes no liability related to its use. June 2010 L419826A

iPhone in Business
Mobile Device Management



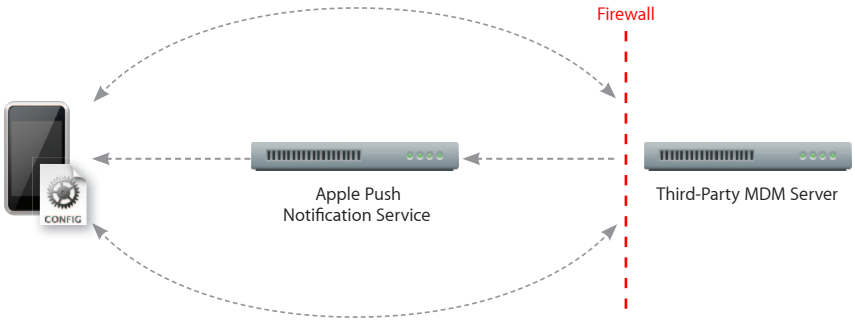
iPhone supports Mobile Device Management, giving businesses the ability to manage scaled deployments of iPhone across their organizations. These Mobile Device Management capabilities are built upon existing iOS technologies like Configuration Profiles, Over-the-Air Enrollment, and the Apple Push Notification service and can be integrated with in-house or third-party server solutions. This gives IT departments the ability to securely enroll iPhone in an enterprise environment, wirelessly configure and update settings, monitor compliance with corporate policies, and even remotely wipe or lock managed iPhone devices.

Managing iPhone

Management of iPhone takes place via a connection to a mobile device management server. As noted, this server can be built in-house by IT or purchased from a third-party solution provider. When a mobile device management server wants to communicate with iPhone, a silent notification is sent to the device prompting it to check in with the server. The device communicates with the server to see if there are tasks pending and responds with the appropriate actions. These tasks can include updating policies, providing requested device or network information, or removing settings and data.

Management functions are completed behind the scenes with no user interaction required. For example, if an IT department updates its VPN infrastructure, the mobile device management server can configure iPhone with new account information over the air. The next time VPN is used by the employee, the appropriate configuration is already in place, so the employee doesn't need to call the help desk or manually modify settings.

To illustrate the capabilities of Mobile Device Management, this document is organized into four categories of deployment: Enroll, Configure, Query, and Manage.



Enroll

The first step in managing iPhone is to enroll a device with a mobile device management server. This creates a relationship between the device and the server, allowing the device to be managed on demand without further user interaction. This can be done wirelessly or by connecting iPhone to a computer via USB.

As a scalable way to securely enroll devices in an enterprise environment, iPhone supports a process called Over-the-Air Enrollment.

Using Over-the-Air Enrollment, your enterprise can provide a secure web portal through which users can enroll their devices for management. The server can then configure managed devices with the appropriate restrictions and account access.

iPhone and SCEP
iPhone supports the Simple Certificate Enrollment Protocol (SCEP). SCEP is an Internet draft in the IETF, and is designed to provide a simplified way of handling certificate distribution for large-scale deployments. This enables over-the-air enrollment of identity certificates to iPhone that can be used for authentication to corporate services.

Process Overview

The process of Over-the-Air Enrollment involves three phases that, when combined in an automated workflow, provide a secure way to provision devices within the enterprise. These phases include:

1. User authentication
User authentication ensures that incoming enrollment requests are from authorized users and that the user's device information is captured prior to proceeding with certificate enrollment. Administrators can prompt the user to begin the process of enrollment by providing a URL via email or SMS notification.

2. Certificate enrollment
After the user is authenticated, iPhone generates a certificate enrollment request using the Simple Certificate Enrollment Protocol (SCEP). This enrollment request communicates directly to the enterprise Certificate Authority (CA), and enables iPhone to receive the identity certificate from the CA in response.

3. Device configuration
Once an identity certificate is installed, iPhone can receive encrypted configuration information over the air. This information can only be installed on the device it is intended for and contains settings for iPhone to connect to the mobile device management server.

At the end of the enrollment process, the user will be presented with an installation screen that describes what access rights the mobile device management server will have on the device. By agreeing to the profile installation, the user's device is automatically enrolled without further interaction.

Configure

Once a device is enrolled as a managed device, it can be dynamically configured with settings and policies by the mobile device management server. The server sends configurations, known as Configuration Profiles, to the device that are installed automatically.

Configuration Profiles are XML files that contain configuration information and settings that permit iPhone to work with your enterprise systems, including account information, passcode policies, restrictions, and other device settings.

When combined with the previously discussed process of enrollment, device configuration provides IT with assurance that only trusted users are accessing corporate services, and that their devices are properly configured with established policies.

And because Configuration Profiles can be signed, encrypted, and locked, the settings cannot be altered or shared with others.

Supported configurable settings

Accounts

- Exchange ActiveSync
- IMAP/ POP email
- VPN
- Wi-Fi
- LDAP
- CalDAV
- CardDAV
- Subscribed calendars

Policies

- Require passcode
- Allow simple value
- Require alphanumeric value
- Passcode length
- Number of complex characters
- Maximum passcode age
- Time before auto-lock
- Number of unique passcodes before reuse
- Grace period for device lock
- Number of failed attempts before wipe
- Control Configuration Profile removal by user

Restrictions

- App installation
- Camera
- Screen capture
- Automatic sync of mail accounts while roaming
- Voice dialing when locked
- In-application purchasing
- Require encrypted backups to iTunes
- Explicit music & podcasts in iTunes
- Allowed content ratings for movies, TV shows, apps
- Safari security preferences
- YouTube
- iTunes Store
- App Store
- Safari

Other settings

- Certificates and identities
- Web Clips
- APN settings

Query

In addition to configuring devices, a mobile device management server has the ability to query devices for a variety of information. This information can be used to ensure that devices continue to comply with required policies.

The mobile device management server determines the frequency at which it gathers information.

Supported queries

Device information

- Unique Device Identifier (UDID)
- Device name
- iOS and build version
- Model name and number
- Serial number
- Capacity and space available
- IMEI
- Modem firmware

Network information

- ICCID
- Bluetooth® and Wi-Fi MAC addresses
- Current carrier network
- SIM carrier network
- Carrier settings version
- Phone number
- Data roaming setting (on/off)

Compliance and security information

- Configuration Profiles installed
- Certificates installed with expiry dates
- List of all restrictions enforced
- Hardware encryption capability
- Passcode present

Applications

- Applications installed (app ID, name, version, size, and app data size)
- Provisioning Profiles installed with expiry dates

Manage

When a device is managed, it can be administered by the mobile device management server through a set of specific actions.

Remote wipe

A mobile device management server can remotely wipe an iPhone. This will permanently delete all media and data on the iPhone, restoring it to factory settings.

Remote lock

The server locks the iPhone and requires the device passcode to unlock it.

Clear passcode

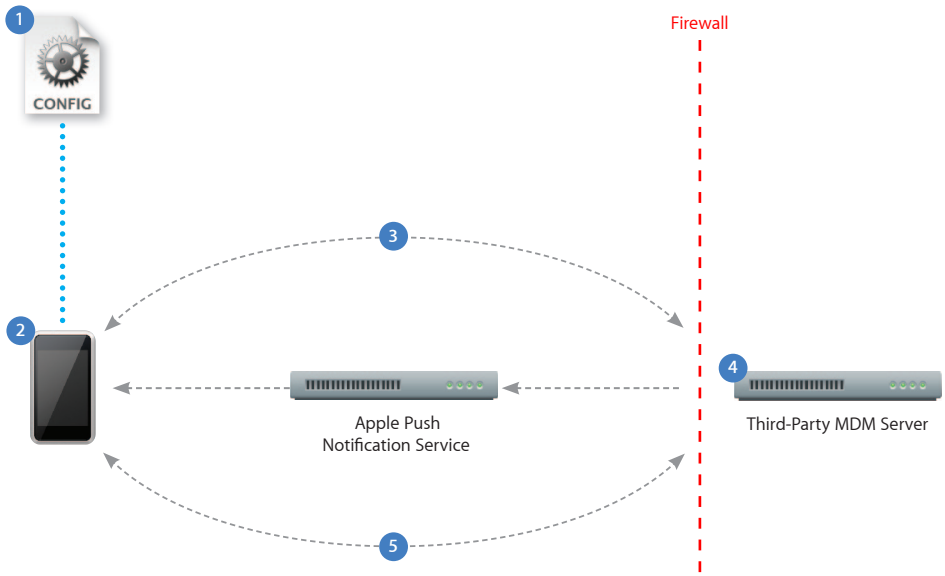
This action temporarily removes the device passcode for users who have forgotten it. If the device has a policy requiring a passcode, the user will be required to create a new one.

Configuration and Provisioning Profiles

To configure devices and provision in-house applications, mobile device management servers can add and remove Configuration Profiles and Application Provisioning Profiles remotely.

Process Overview

This example depicts a basic deployment of a mobile device management server.



1. A Configuration Profile containing mobile device management server information is sent to the device. The user is presented with information about what will be managed and/or queried by the server.
2. The user installs the profile to opt in to the device being managed.
3. Device enrollment takes place as the profile is installed. The server validates the device and allows access.
4. The server sends a push notification prompting the device to check in for tasks or queries.
5. The device connects directly to the server over HTTPS. The server sends commands or requests information.

For more information on Mobile Device Management, visit www.apple.com/iphone/business/integration

© 2010 Apple Inc. All rights reserved. Apple, the Apple logo, iPhone, and Safari are trademarks of Apple Inc., registered in the U.S. and other countries. App Store is a service mark of Apple Inc. iTunes Music Store is a service mark of Apple Inc., registered in the U.S. and other countries. The Bluetooth word mark is a registered trademark owned by Bluetooth SIG, Inc., and any use of such marks by Apple is under license. Other product and company names mentioned herein may be trademarks of their respective companies. Product specifications are subject to change without notice. This material is provided for information purposes only; Apple assumes no liability related to its use. June 2010 L419825A

iPhone in Business
iTunes Deployment Overview

iTunes controls and restrictions
When deploying iTunes on your corporate network, you can restrict the following iTunes functionality using the registry in Windows or System Preferences in Mac OS X:

- Accessing the iTunes Store
- Library sharing with local network computers also running iTunes
- Playing explicit iTunes media content
- Playing movies
- Playing TV shows
- Playing Internet radio
- Entering a streaming media URL
- Subscribing to podcasts
- Displaying Genius suggestions while browsing or playing media
- Downloading album artwork
- Using Visualizer plug-ins
- Automatically discovering Apple TV systems
- Checking for new versions of iTunes
- Checking for device software updates
- Automatically syncing when devices are connected
- Registering new devices with Apple
- Access to iTunes (iTunes U)

Introduction

When deploying iPhone in your business, it's important to think about the role of iTunes. A few key functions require iTunes, starting with the activation of the device. After activation, iTunes isn't required to configure or use iPhone with your enterprise systems. It is, however, required for installing software updates and for creating a backup if user information ever needs to be restored or transferred to a new device. iTunes can also be used to synchronize music, video, applications, and other content. These synchronization capabilities are not required for general business use.

Whether you choose to install iTunes on your business computers or encourage your employees to do these functions from a home computer—corporate data can be encrypted and protected throughout the process. If you choose to support iTunes internally, you can tailor the application to meet the needs of your environment or business conduct policies. For example, you can customize iTunes by restricting or disabling network services such as the iTunes Store or shared media libraries, or controlling access to software updates. You can also deploy iTunes using centrally managed desktop software deployment tools.

For the end user, iTunes is simple to use. Users who are familiar with the iTunes interface for managing content and media at home will find it easy to manage their corporate content on an iPhone.

Using iTunes

Activation
Before you can make and receive calls, send text messages, or connect to the cellular data network, you must first activate your line of service with your wireless carrier. Additionally, iPhone must be connected to iTunes via USB to activate the device. Because iTunes is required to complete the activation process for iPhone, you'll need to decide whether you want to install iTunes on each user's Mac or PC, or whether you'll complete activation for each device with a centralized iTunes installation. Either way, the activation process is quick and easy.

Users simply connect an iPhone to a Mac or PC running iTunes, and within seconds, iPhone is activated and ready for use.

After activating a device, iTunes offers to sync the device with the computer. To avoid this when you're activating a device for your users, turn on activation-only mode within iTunes. This disables syncing and automatic backups and prompts you to disconnect the device as soon as activation is finished.

For instructions on how to enable activation-only mode, refer to the Enterprise Deployment Guide.

iTunes podcasts
iTunes can subscribe to and download audio and video podcasts. Podcasts are a great way to deliver everything from training and educational content to corporate communications and product information that's critical to your organization. Podcasts can be easily transferred to iPhone or iPad, so your employees can listen or watch—whenever and wherever they are. The iTunes Store also has thousands of free business-related podcasts available from providers such as Harvard Business Review, Wharton, Bloomberg, and more.

Syncing media
You can use iTunes to sync music, videos, photos, apps, and more. iTunes makes it easy to control exactly what to sync, and you can clearly see how much space is available for content. iPhone can sync each type of data to only one computer at a time. For example, you can sync music with a home computer and contacts with a work computer by setting iTunes sync options appropriately on both computers.

Software updates
iTunes is used to update or reinstall iPhone software and to restore default settings or restore from backup. When an update is performed, downloaded applications, settings, and data aren't affected. To update, users simply connect iPhone to their computer, and click "Check for Updates." iTunes informs the user if a newer version of iPhone software is available. If you turn off automated and user-initiated software update checking using iTunes restrictions, you'll need to distribute software updates for manual installation. This can be done by distributing the .ipsw file associated with each version of the software and instructing your users on how to manually install the update.

Backup
While the synchronization of data for business users will mostly take place over-the-air using corporate services such as Exchange ActiveSync, using iTunes to back up iPhone settings is important if users need to restore a device. When iPhone or iPod touch is synced with iTunes, device settings are automatically backed up to the computer. Applications purchased from the App Store are copied to the iTunes Library. Applications you've developed in-house and distributed to your users with enterprise provisioning profiles won't be backed up or transferred to the user's computer. However, the device backup will include any data files the enterprise application creates. Once iPhone has been configured to sync with a particular computer, iTunes automatically makes a backup of iPhone on that computer when synced. iTunes won't automatically back up an iPhone that isn't configured to sync with that computer.

iTunes backups can be encrypted on the host machine—preventing unwanted data loss from the host computer. Backup files are encrypted using AES 128 with a 256-bit key. The key is stored securely in the iPhone keychain. Users are prompted to create a strong passcode when backing up iPhone for the first time.

Deploying iTunes

Installation
iTunes uses standard Mac OS and Windows installers and can be deployed using many of the desktop management applications commonly used by IT professionals. iTunes can also be installed and updated without user interaction. Once settings and policies in the iTunes installer have been modified, iTunes can be deployed the same way other enterprise software is deployed.

When you install iTunes on Windows computers, by default you also install the latest versions of QuickTime, Bonjour, and Apple Software Update. You can omit the Bonjour and Software Update components by passing parameters to the iTunes installer or by pushing only the components you want to install on your users' computers. The QuickTime component, however, is required, and iTunes will not run without it. Mac computers come with iTunes installed. To push iTunes to Mac clients, you can use Workgroup Manager, an administrative tool included with Mac OS X Server.

© 2010 Apple Inc. All rights reserved. Apple, the Apple logo, Apple TV, Bonjour, iPad, iPhone, iPod, iPod touch, iTunes, Mac, Mac OS, and QuickTime are trademarks of Apple Inc., registered in the U.S. and other countries. App Store is a service mark of Apple, Inc. iTunes Store is a service mark of Apple Inc., registered in the U.S. and other countries. Other product and company names mentioned herein may be trademarks of their respective companies. Product specifications are subject to change without notice. This material is provided for information purposes only; Apple assumes no liability related to its use. June 2010 L419823A