



iPad in Business

Deployment Scenarios and
Device Configuration Overview

April 2010

Learn how iPad integrates seamlessly into enterprise environments with these deployment scenarios and the device configuration overview.

- Microsoft Exchange
- IMAP, CalDAV, and LDAP
- Virtual Private Network (VPN)
- WPA2 Enterprise/802.1X
- Digital Certificates
- Device Configuration Overview
- Over-the-Air Enrollment and Configuration

iPad in Business

Microsoft Exchange



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 Server 2007 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

iPad communicates directly with 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 Lookup (GAL) and administrators with passcode policy enforcement and remote wipe capabilities. iPad 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 iPad—no additional configuration is required. If you have Exchange Server 2003 or 2007 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 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 Microsoft ISA Server, create a web listener as well as an Exchange web client access publishing rule. See Microsoft 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, this is done in the Exchange Management Console.
- Download and install the Exchange ActiveSync Mobile Administration Web tool, which is necessary to initiate a remote wipe. For Exchange Server 2007, remote wipe can also be initiated using Outlook Web Access or the Exchange Management Console.



Other Exchange ActiveSync services

- Mail search on Exchange Server 2007
- Accept and create calendar invitations
- Global Address List lookup
- Certificate-based authentication
- Email push to selected folders
- Autodiscovery

Basic authentication (user name and password)

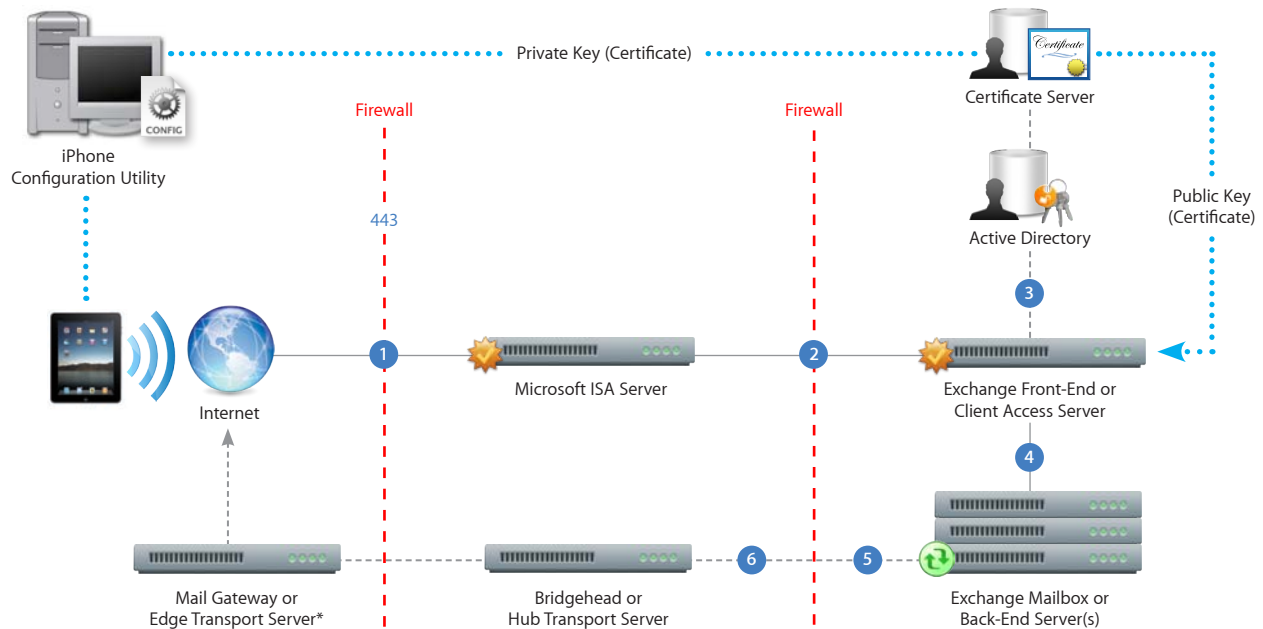
- Enable Exchange ActiveSync for specific users or groups using the Active Directory service. These are enabled by default for all mobile devices at the organizational level in Exchange Server 2003 and 2007. For Exchange Server 2007, see Recipient Configuration in the Exchange Management Console.
- By 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). For more information on certificate services, refer to resources available from Microsoft.
- 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 the iPhone Configuration Utility or over-the-air enrollment and configuration to deliver this key to iPad.

Exchange ActiveSync Deployment Scenario

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



*Depending on your network configuration, the mail gateway or Edge Transport server may reside within the perimeter network (DMZ).

- 1 iPad 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 Exchange Server.
- 3 Exchange Server authenticates the incoming user via the Active Directory service and the certificate authority 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 and changes are pushed to iPad over the air, and any changes made on iPad are reflected on Exchange Server.
- 6 Sent mail items on iPad are also synchronized with 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.

iPad in Business

IMAP, CalDAV, and LDAP



Recommended ports

- IMAP/SSL: 993
- SMTP/SSL: 587
- LDAP/SSL: 636
- CalDAV/SSL: 8443

IMAP or POP-enabled mail solutions

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

Additional information regarding the IMAP4rev1 standard can be found at www.imap.org.

CalDAV calendar standard

iPad supports the CalDAV calendaring protocol. The CalDAV protocol has been standardized by the IETF. More information can be found through the CalConnect consortium at <http://caldav.calconnect.org>.

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

In a typical deployment, iPad establishes direct access to IMAP and SMTP mail servers to receive and send email over the air. Synchronization with your CalDAV server allows iPad users to wirelessly receive updates to their calendars. And iPad can connect to your company's LDAPv3 corporate directories, giving users access to corporate contacts in the Mail and Contacts applications. All network servers can be located within a DMZ subnetwork, behind a corporate firewall, or both. With SSL, iPad supports 128-bit encryption and X.509 root certificates issued by the major certificate authorities.

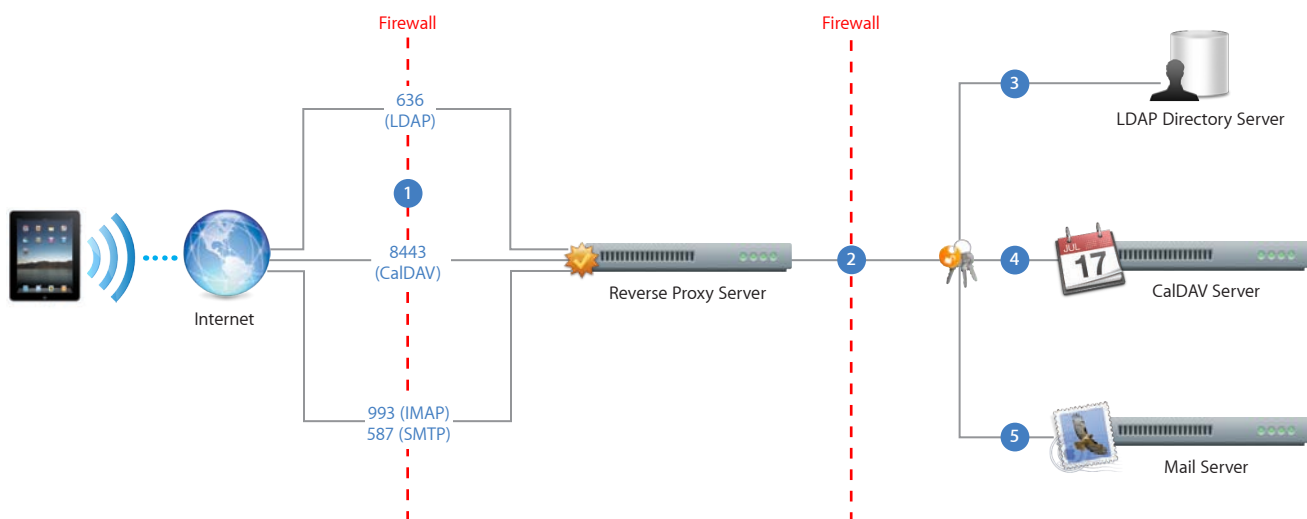
Network Setup

The IT or network administrator will need to complete these key steps to enable direct access from iPad to IMAP, CalDAV, and LDAP services:

- Open the following ports on the firewall: 993 for IMAP mail, 587 for SMTP mail, 636 for LDAP directory services, and 8443 for CalDAV calendaring. These are the standard ports for communications over SSL, which ensures that calls made to your servers are securely encrypted during wireless transmission. It's also recommended that communication between your proxy server and your back-end IMAP, CalDAV, and LDAP 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 is an important step to ensure that iPad 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 iPad. iPad 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 iPad connects to a typical IMAP, CalDAV, and LDAP deployment.



- 1 iPad requests access to network services over the designated ports.
- 2 Depending on the service, iPad 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 iPad 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 iPad.
- 5 For IMAP mail services, existing and new messages can be read on iPad through the proxy connection with the mail server. Outgoing mail on iPad is sent to the SMTP server, with copies placed in the user's Sent folder.

iPad in Business

Virtual Private Network (VPN)



VPN protocols

- Cisco IPSec
- L2TP/IPSec
- PPTP

Authentication methods

- Password (MS-CHAPv2)
- RSA SecurID
- CRYPTOCARD
- X.509 digital certificates
- Shared secret

Secure access to private corporate networks is available on iPad using established industry-standard VPN protocols. iPad 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 iPad to your VPN.

Cisco IPSec deployments can take advantage of certificate-based authentication via industry-standard X.509 digital certificates. With certificate-based authentication, iPad supports VPN On Demand. VPN On Demand can establish a connection automatically when accessing predefined domains, providing a seamless VPN connectivity experience for iPad users.

For two-factor token-based authentication, iPad supports RSA SecurID as well as CRYPTOCARD. Users enter a PIN and a token-generated, one-time password directly on iPad when establishing a VPN connection.

iPad supports shared secret authentication for Cisco IPSec and L2TP/IPSec deployments. And for basic user name and password authentication, iPad supports MS-CHAPv2.

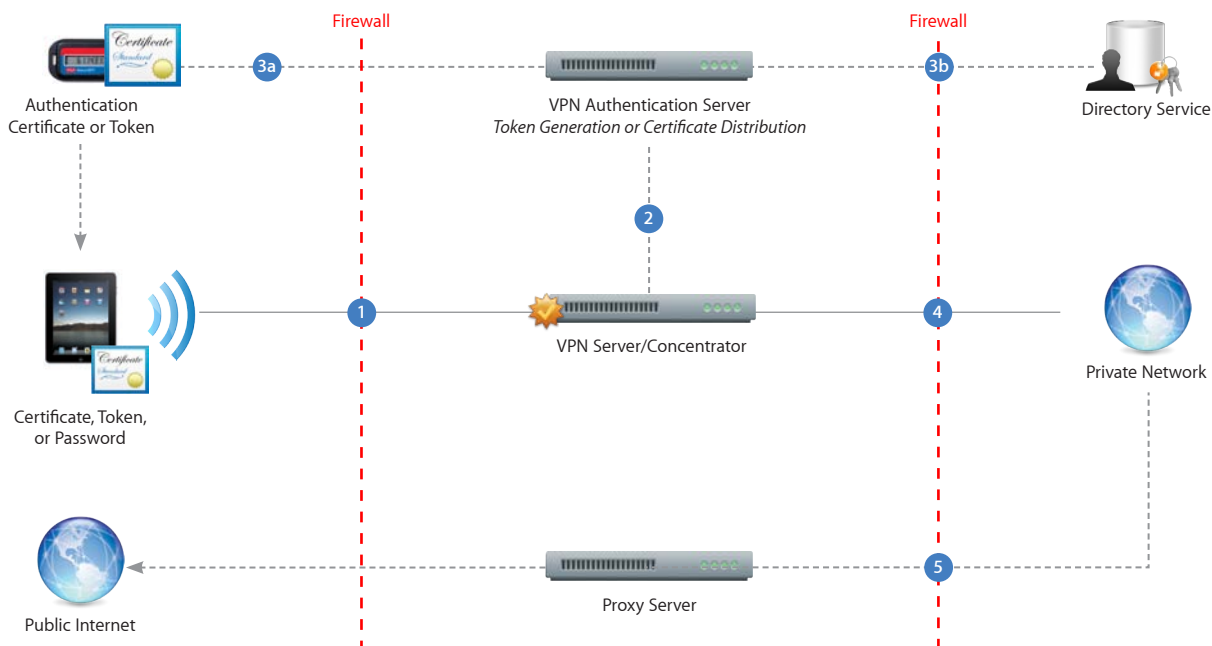
VPN Proxy Auto-Configuration (PAC) is also supported, which allows you to specify proxy server settings for accessing specific URLs.

VPN Setup

- iPad integrates with most existing VPN networks, so minimal configuration should be necessary to enable iPad access to your network. The best way to prepare for deployment is to determine whether iPad supports your company's existing VPN protocols and authentication methods.
- It's a good idea to review the authentication path to your authentication server to make sure standards supported by iPad are enabled within your implementation.
- If you plan to use certificate-based authentication, ensure you have your public key infrastructure (PKI) configured to support device- and user-based certificates with the corresponding key distribution process. For additional documentation regarding digital certificates for IPSec VPNs, visit: <https://cisco.hosted.jivesoftware.com/docs/DOC-3592>.
- If you want to configure URL-specific proxy settings, place a PAC file on a web server that's accessible with the basic VPN settings and ensure that it's hosted with the application/x-ns-proxy-autoconfig MIME type.
- Check with your solution providers to confirm that your software and equipment are up to date with the latest security patches and firmware.

VPN 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 iPad requests access to network services (typically over a PPP connection).
- 2 The VPN server/concentrator receives the request and then passes it to the authentication server.
- 3a 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 iPad prior to authentication. If a password method is deployed, the authentication process proceeds with user validation.
- 3b Once a user is authenticated, the authentication server validates user and group policies.
- 4 After user and group policies are validated, the VPN server provides tunneled and encrypted access to network services (typically via IPSec).
- 5 If a proxy server is in use, iPad connects through the proxy server for access to information outside the firewall.

iPad in Business

WPA2 Enterprise/802.1X



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-CHAPv2)
- PEAPv1 (EAP-GTC)
- LEAP

iPad supports WPA2 Enterprise, ensuring corporate wireless networks are 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, iPad can be integrated into a broad range of RADIUS authentication environments. 802.1X wireless authentication methods supported on iPad include EAP-TLS, EAP-TTLS, EAP-FAST, EAP-SIM, PEAPv0, PEAPv1, and LEAP.

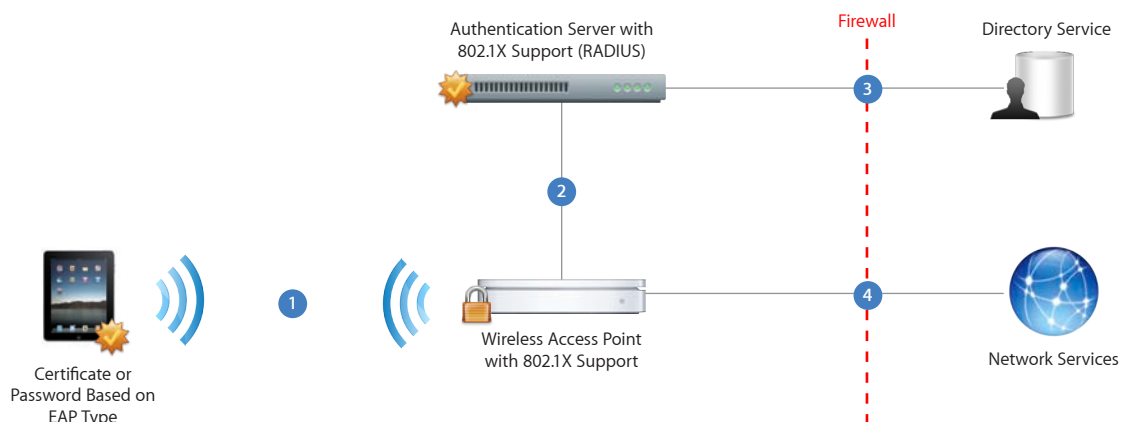
For quick setup and deployment, wireless network, security, and authentication settings can be configured using configuration profiles. For more information, see the “Device Configuration Overview” section of this document.

WPA2 Enterprise Setup

- Verify network appliances for compatibility and select an authentication type (EAP type) supported by iPad.
- Check to ensure 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.
- Test your 802.1X deployment with a Mac or a PC to ensure RADIUS authentication is properly configured.
- If you plan to use certificate-based authentication, ensure that you have your public key infrastructure (PKI) configured to support device- and user-based certificates with the corresponding key distribution process.
- Verify certificate format and authentication server compatibility. iPad supports PKCS#1 (.cer, .crt, .der) and PKCS#12.
- Check with your solution providers to confirm that your software and equipment are up to date with the latest security patches and firmware.
- 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 iPad requests access to network services. By selecting a wireless network or configuring access to a specific SSID, iPad initiates the connection.
- 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.

iPad in Business

Digital Certificates



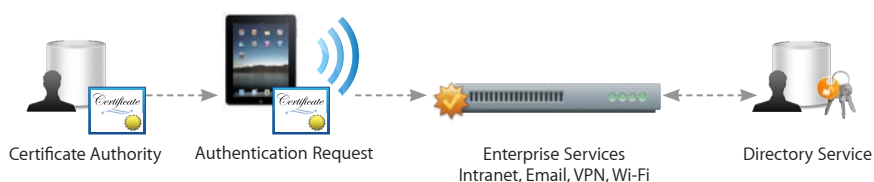
iPad supports digital certificates, giving business users secure, streamlined access to corporate services. A digital certificate is composed of a public and private key pair, along with other information about you and the certificate authority that issued the certificate. Digital certificates are a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

Certificates can be used to sign and encrypt many types of data. Signing data with a digital certificate helps to ensure that it hasn't been changed or altered and can also be used to guarantee the identity of the author or "signer." Additionally, certificates can be used to encrypt configuration profiles and network communications to help further protect confidential or private information.

Using Certificates on iPad

Identity certificates

Digital certificates can be used to securely authenticate users to corporate services without the need for user names, passwords, or even tokens. On iPad, certificate-based authentication is supported for access to Microsoft Exchange ActiveSync, Cisco IPsec VPN, and WPA2 Enterprise Wi-Fi networks.



Supported certificate and identity format:

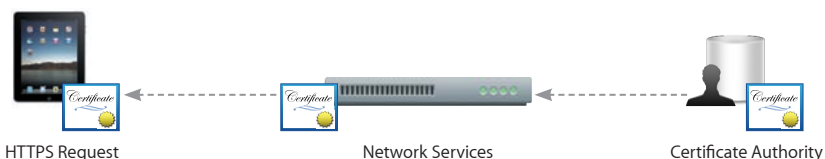
- iPad supports X.509 certificates with RSA keys.
- The file extensions .cer, .crt, .der, .p12, and .pfx are recognized.

Root certificates

Out of the box, iPad 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're using a root certificate that's preinstalled, such as a self-signed root certificate created by your company, you can distribute it to iPad using one of the methods listed in the "Distributing and Installing Certificates" section of this document.

Server certificates

Digital certificates can also be used to validate and encrypt network communications. This provides secure communication to both internal websites and websites on the public Internet. The Safari browser can check the validity of the X.509 digital certificate being presented and set up the secure session with 128-bit SSL encryption. This verifies that the site's identity is legitimate and that your communication with the website is protected to help prevent interception of personal or confidential data.



Distributing and Installing Certificates

Distributing certificates to iPad is simple. Whenever you receive a certificate, it can be imported into your keychain for later use. When an identity certificate is installed, the user is prompted for the passphrase that protects it. If a certificate's authenticity cannot be verified, you'll be presented with a warning before it's added to your keychain. Certificates can be distributed to iPad in four ways.

Installing certificates via a configuration profile

If you're using configuration profiles to distribute settings to corporate services such as Exchange, VPN, or Wi-Fi, certificates can be added to the profile to streamline deployment. If you're using multiple configuration profiles, make sure certificates aren't duplicated. You cannot install multiple copies of the same certificate.

1. Under the Credentials tab in the iPhone Configuration Utility, click Configure.
2. In the file dialog that appears, select a PKCS#1 or PKCS#12 file, and then click Open.

To add multiple credentials to the configuration profile, click the Add (+) button.

Mac OS X

If the certificate or identity that you want to install is in your keychain, use Keychain Access to export the credential in .p12 format before creating your profile.

Windows

If the credential is not available in your personal certificate store, you must add it before creating your profile. In addition, the private key must be marked as exportable, which is one of the steps offered by the certificate import wizard. Note that adding root certificates requires administrative access to the computer, and the certificate must be added to the personal store.

Installing certificates via Mail

If a certificate is sent in an email, it appears as an attachment. The user simply taps on the attachment to review and taps install to add the certificate to the device.

Installing certificates via Safari

Safari can be used to download certificates from a web page. Host a certificate on a secured website and provide users with the URL where they can download the certificate onto their devices.

Installing certificates via the Simple Certificate Enrollment Protocol (SCEP)

SCEP is an Internet draft in the Internet Engineering Task Force (IETF) that's designed to simplify certificate distribution for large-scale deployments. This enables over-the-air distribution of identity certificates to iPad that can be used for authentication to corporate services.

Certificate removal and revocation

To remove an installed certificate, choose Settings > General > Profiles. If you remove a certificate that's required for accessing an account or network, your device cannot connect to those services.

Additionally, the Online Certificate Status Protocol (OCSP) is supported to check the status of certificates. OCSP-enabled certificates are validated before a task is completed to be sure the certificate hasn't been revoked.

iPad in Business

Device Configuration Overview



Supported passcode policies

- Require passcode
- Allow simple value
- Require alphanumeric value
- Passcode length
- Number of complex characters
- Passcode age
- "Time before" auto-lock
- Number of unique passcodes before reuse
- Grace period for device lock
- Number of failed attempts before wipe

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

Deploying iPad across your organization is easy with the use of configuration profiles. Configuration profiles are XML files that contain configuration information and settings that permit iPad to work with your enterprise systems.

iPhone Configuration Utility 2.2 lets you easily create, encrypt, and install configuration profiles. It can also track and install provisioning profiles and authorized applications. It can also capture device information, including console logs. The iPhone Configuration Utility is available for Windows and Mac OS X.

Configuration Profile Components



Passcode policies

Protect your enterprise data by configuring device passcode policies and requiring their use.



Restrictions

In addition to passcode policies, configuration profiles can be used to restrict certain device features.



Wi-Fi settings

Whether you're configuring iPad to connect to a private network or for RADIUS authentication to enterprise wireless access points, configuration profiles can be deployed to streamline access to Wi-Fi networks.



VPN settings

Configure VPN server settings, including accounts, proxies, and authentication settings for your corporate private networks.



Email settings

Configure IMAP or POP mail settings, including incoming and outgoing mail servers.



Exchange settings

Include server, domain, and account information in a configuration profile so that your users can connect via Microsoft Exchange ActiveSync.



LDAP

Configure access to LDAP directories for contact lookup in Mail and Address Book.



CalDAV

Provide these settings to synchronize calendar data with your company's CalDAV server wirelessly.



Web Clips

Place icons on your user's Home screen to provide quick access to internal or external websites.



Credentials

Ensure the identity of your users and control access to key enterprise services such as Exchange ActiveSync, VPN, and WPA2 Enterprise Wi-Fi networks on iPad.



Advanced

Edit these settings to modify the access point name (APN) on iPad. APN proxy settings can be specified using a configuration profile as well.

Protecting Configuration Profiles

Security options

When preparing to deploy your configuration settings, you'll need to export your configuration profile from the iPhone Configuration Utility. The file that's created has a .mobileconfig extension. This file can be created with three different levels of security. With any of these methods, you should make sure that when the profile is distributed, it's accessible only to authorized users.

Unsigned—A plain text .mobileconfig file is created. It can be installed on any device. Some content in the file is obfuscated to prevent casual snooping if the file is examined. This profile will appear as unsigned and will prompt the user with a security message.

Signed—The .mobileconfig file is signed and will not be installed by a device if it is altered. Once installed, the profile can only be updated by a profile that has the same identifier and is signed by the same instance of the iPhone Configuration Utility. Like unsigned profiles, some of the information in the signed profile is obfuscated to prevent casual snooping if the file is examined.

Signed and encrypted—The profile is signed so it cannot be altered, and all of its contents are encrypted so the profile cannot be examined. Encrypted profiles can be distributed via desktop synchronization using the iPhone Configuration Utility or by over-the-air enrollment and configuration. An encrypted configuration profile can only be installed on the device for which it was created.

Controlling the removal of profiles

When creating a configuration profile, you have the option of controlling whether or not it can be removed by the user. You can lock the profile so that once it has been installed, its removal requires an administrative password or a full reset of the device.

Deploying Configuration Profiles

Configuration profiles can be distributed using four different deployment methods.



Desktop installation via USB

Configuration profiles can be installed through a USB connection with the iPhone Configuration Utility. When you install directly onto a device using USB, the configuration profile is automatically signed and encrypted.

1. Connect the device to your computer using a USB cable.
2. Select the iPad from the Devices list, and then click the Configuration Profiles tab.
3. Select a configuration profile from the list, and then click Install.
4. On the device, tap Install to install the profile.



Email

You can distribute configuration profiles using email. Users install the profile by receiving the message on their devices, then tapping the attachment to install it.

1. Export the profile from the iPhone Configuration Utility.
2. Attach the configuration profile (uncompressed) to an email and send to user(s).
3. Users install the profile by tapping the file directly from the message body in Mail on iPad.



Website

You can distribute configuration profiles using a website. Users install the profile by downloading it using Safari on their devices.

1. Export the profile from the iPhone Configuration Utility.
2. Host the configuration profile (uncompressed) on a secure site that's accessible to user(s).
3. Users navigate to the website using Safari on iPad and tap the file to initiate installation.



Over-the-air enrollment and distribution

You can distribute encrypted configuration profiles over the air using a secure enrollment and configuration process enabled by the Simple Certificate Enrollment Protocol (SCEP).

iPad in Business

Over-the-Air Enrollment and Configuration



iPad and SCEP

iPad supports the Simple Certificate Enrollment Protocol (SCEP). SCEP is an Internet draft in the IETF that 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 iPad that can be used for authentication to corporate services.

iPad supports over-the-air enrollment and configuration, providing an automated way to configure devices securely within the enterprise. Enrollment refers to the process of authenticating a device and user for the purposes of automated certificate distribution. While over-the-air enrollment facilitates the general deployment of device certificates within your company's public key infrastructure (PKI), it also can facilitate the distribution of signed and encrypted configuration profiles. The combined process of certificate enrollment and device configuration provides IT with assurance that only trusted users are accessing corporate services and that their devices are properly configured to comply with established policies. And because configuration profiles can be both encrypted and locked, the settings cannot be removed, altered, or shared with others.

Administrators can prompt users to begin the process of enrollment by providing them with a URL. By agreeing to the profile installation, the users' device is the automatically enrolled and configured in a single session.

Process Overview

The process of over-the-air enrollment and configuration involves three phases that when combined in an automated workflow provide a secure way to provision devices within the enterprise. These phases include:

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.

Certificate enrollment

After the user is authenticated, iPad generates a certificate enrollment request using the SCEP protocol. This SCEP enrollment request talks directly to the enterprise certificate authority and enables iPad to receive the identity certificate from the certificate authority in response.

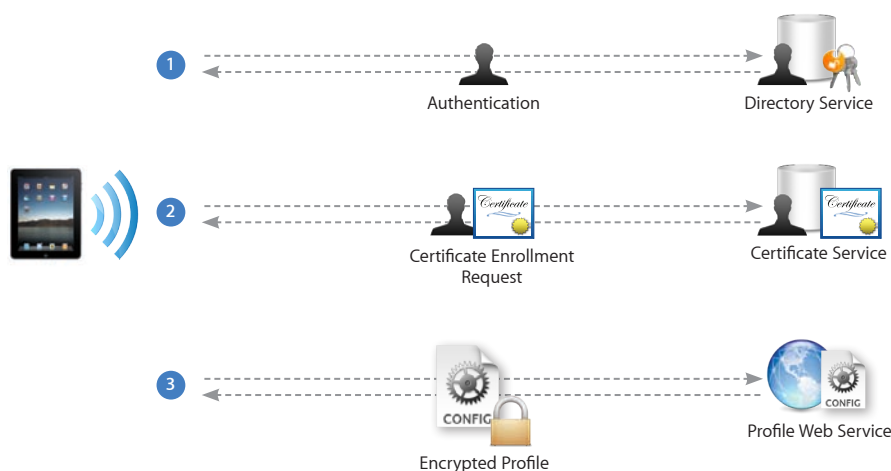
Device configuration

Once an identity certificate is installed, iPad is able to receive an encrypted configuration profile over the air. This encrypted configuration profile can only be installed only on the device it was intended for and can contain settings for iPad to connect to corporate services (Exchange, VPN, Wi-Fi, and so on.)



User Scenario

The following example shows how iPad connects to a typical over-the-air enrollment and configuration deployment.



- 1 The user enters the URL of the profile service in Safari on iPad and is presented a login web page. The user enters a user name and password and is authenticated via basic HTTP authentication or via existing directory services.
- 2 Once the user is authenticated, an enrollment profile is sent to the user. The user is prompted to install the profile. Once the initial enrollment profile is installed, iPad responds back to the certificate authority with information necessary to deliver an identity certificate to the device.
- 3 That identity certificate enables the device to receive device settings via an encrypted configuration profile. This exchange is automated. No additional interaction from the user is required.

Infrastructure Setup

To implement this process you'll need to create an infrastructure that can support the authentication, enrollment, and profile delivery process. The deployment and integration of three primary enterprise services is involved.

Directory services

User authentication can be as simple as basic HTTP authentication, or you can integrate with your existing directory services. Regardless of the services used, you'll need to provide a web-based authentication method for your users to request enrollment.

Certificate services

The process of enrollment requires deployment of standard x.509 identity certificates to iPad users. You'll need a certificate authority to issue the device credentials using SCEP. Cisco IOS and Microsoft Server 2003, with the add-on for certificate services, both support SCEP. A number of hosted PKI services also support SCEP, such as VeriSign, Entrust, and RSA.

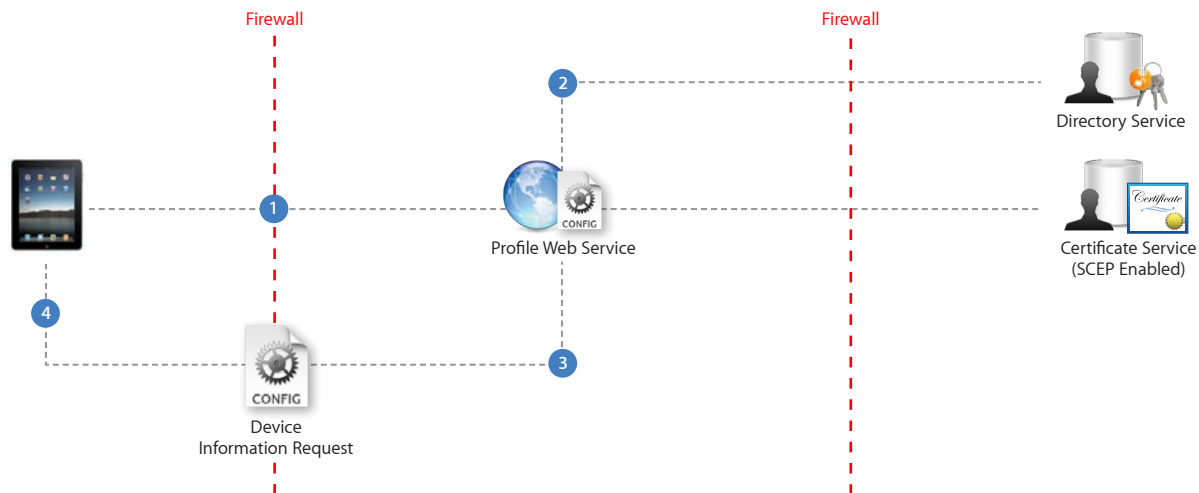
Profile services

To implement this process, you will need to develop a profile service—an HTTP-based service that manages iPad connections throughout the process, generates configuration profiles for the user, and verifies user credentials along the way. The profile service should provide a few key functions:

- Host a user-accessible website to support the HTTPS session
- Authenticate incoming user requests using a web-based authentication method (basic, or integrated with directory services)
- Generate the necessary configuration profiles (XML format) depending on the phase of the process
- Sign and encrypt configuration profiles using public key cryptography
- Track the user through the steps in the process (via timestamp and logging methods)
- Manage connections to the certificate authority or directory services

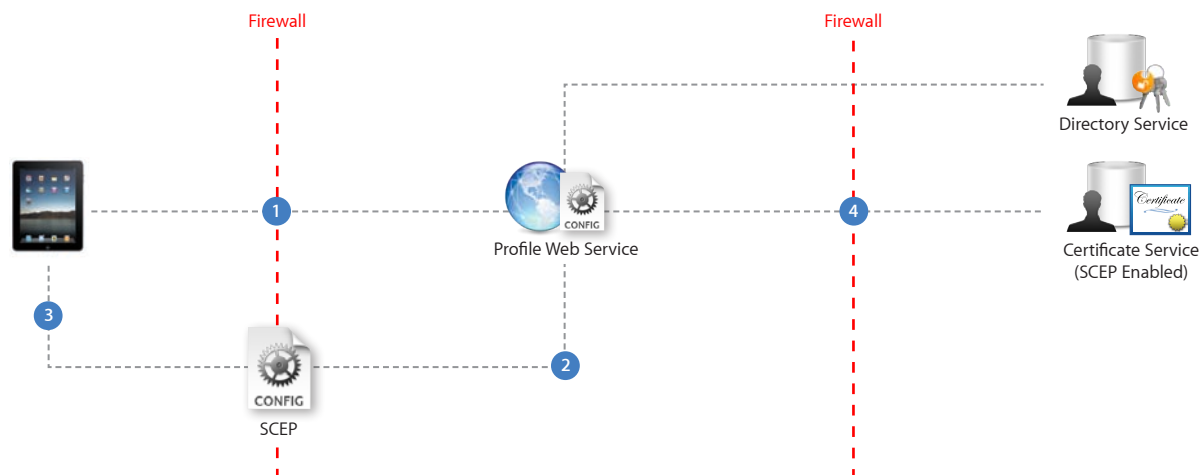
The following three diagrams describe the individual steps in each phase that need to be in place for a typical over-the-air enrollment and configuration implementation.

Phase 1: User authentication



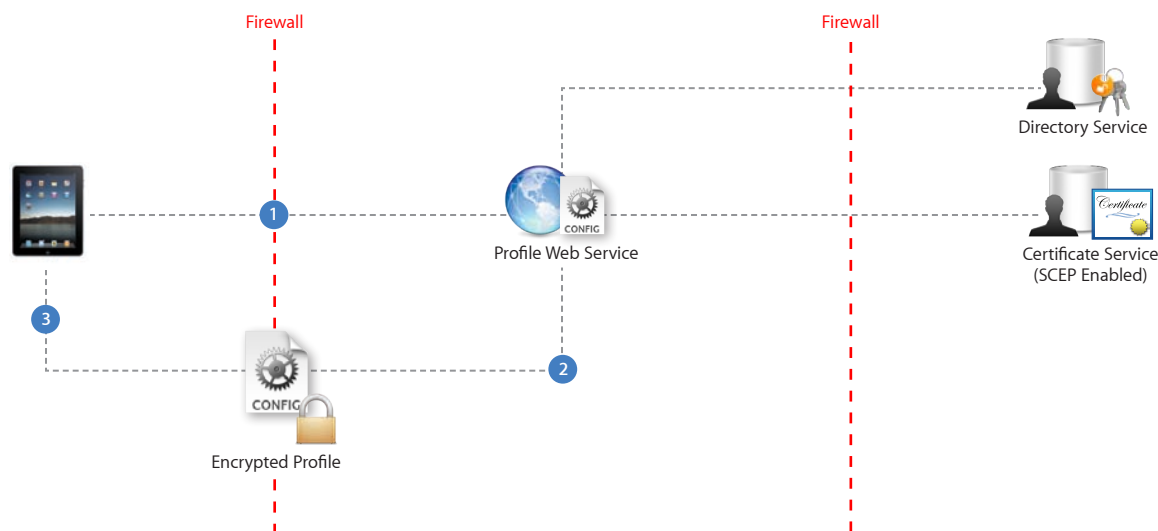
- 1 The user enters the URL of the profile service in Safari on iPad and is presented a login web page. The user enters a user name and password.
- 2 The user is authenticated via basic HTTP authentication or existing directory services.
- 3 Once the user is authenticated, a configuration profile is sent to the user. This profile includes a request for device attributes including the device identifier, OS version, device ID, IMEI, and ICCID. For a sample configuration profile for this phase, see “Server Response” on page 81 of the “Enterprise Deployment Guide.”
- 4 The user is prompted to install the profile.

Phase 2: Certificate enrollment



- 1 Once the configuration profile from phase 1 is installed, the device automatically responds to the server. The response from the device includes device attributes and a preshared key (challenge). The challenge can be used to verify the identity of the user through the next phase of the process. The response is signed using the device's built-in identity (Apple-issued certificate) and sent to the server using HTTP POST.
- 2 Once the profile service receives the device response, a second configuration profile with the SCEP payload is delivered to the device. For a sample configuration profile for this phase, see “Server Response with SCEP Specifications” on page 82 of the “Enterprise Deployment Guide.”
- 3 The profile is installed automatically, no user intervention is required. The SCEP payload contains instructions for the device to generate a certificate signing request and get a certificate using SCEP.
- 4 Once the request is verified, the certificate authority issues the certificate for the device.

Phase 3: Device configuration



- 1 Once the device certificate is received, the device generates a response back to the profile service that's signed with the new certificate (again, via HTTP POST). The response includes device attributes (product identifier, OS version, device ID, IMEI, and ICCID). At the time of request, this information provides a confirmation to the server and can be used to ensure that devices are up to date with the latest OS before delivering a configuration profile.
- 2 The profile service then responds with an encrypted .mobileconfig file. This configuration profile can contain policies, settings, credentials, or additional SCEP requests.
- 3 The profile is received by the device and installed automatically (no user intervention is required).