iPhone in Enterprise

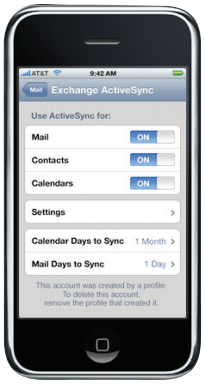
Deployment Scenarios and Device Configuration Overview

June 2008

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

- iPhone and Microsoft Exchange Server
- iPhone and Virtual Private Networks (VPNs)
- iPhone and WPA2 Enterprise/802.1x
- iPhone and IMAP
- iPhone Device Configuration Overview

iPhone and Microsoft Exchange Server



Exchange ActiveSync support

- Microsoft Exchange Server 2003 Service Pack 2
- Microsoft Exchange Server 2007 Service Pack 1

Exchange ActiveSync security policies

- Remote wipe
- Enforce password on device
- Minimum password length
- Require alphanumeric password
- Require complex password
- Inactivity time in minutes

iPhone 2.0 software can now communicate directly with your Microsoft Exchange Server via Microsoft Exchange ActiveSync, giving users push email, contacts, and calendar. Exchange ActiveSync maintains a connection between Exchange Server and iPhone so when a new email message or meeting invitation arrives, iPhone is instantly updated. If your company currently supports Exchange ActiveSync on Exchange Server 2003 or 2007, you already have the necessary services in place to support iPhone 2.0 software—no additional configuration is required. If you have Exchange Server but your company is new to Exchange ActiveSync, you or your IT team should review the following steps to enable Exchange ActiveSync.

Exchange ActiveSync Setup

Network configuration

- Check to ensure port 443 is open on the firewall. (Note: If your company allows Outlook Web Access, port 443 is most likely already open on your firewall.)
- On the Front-End Server, verify that a server certificate is installed and enable SSL for the Exchange ActiveSync virtual directory (require basic SSL authentication).
- On the Microsoft Internet Security and Acceleration (ISA) Server, verify that a server certificate is installed and update the public DNS to properly resolve incoming connections.
- On the ISA Server, create a Web listener as well as an Exchange Web client access publishing rule according to Microsoft documentation. This is a necessary step in enabling Exchange ActiveSync.
- For all firewalls and network appliances, set the Idle Session Timeout to 30 minutes (check your Microsoft Exchange documentation for alternative heartbeat and timeout intervals).

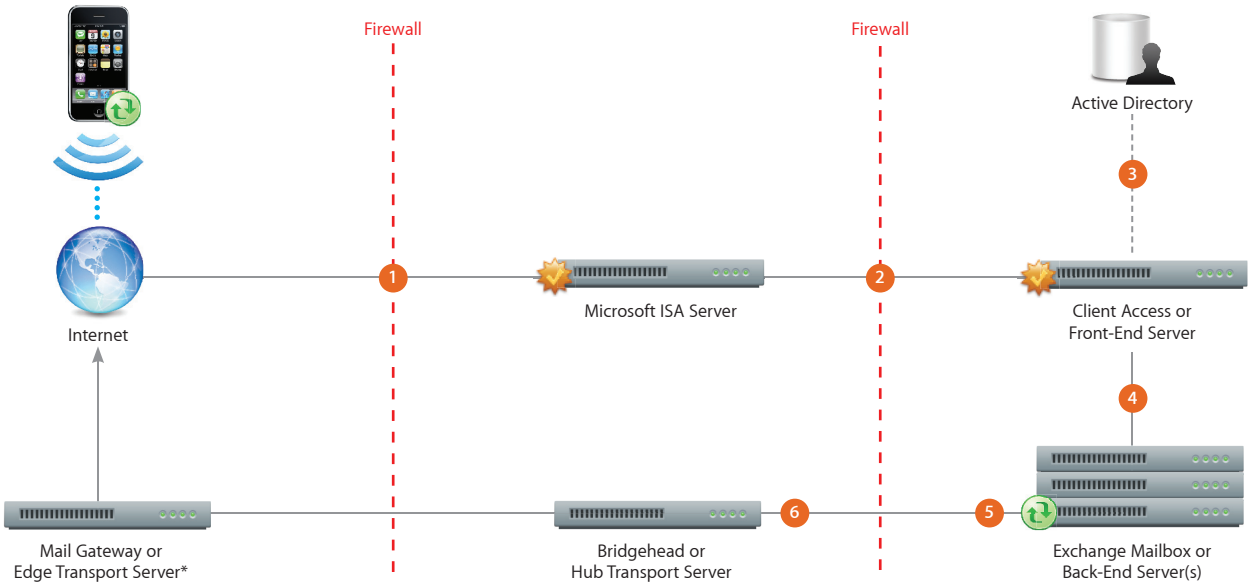
Exchange account setup

Exchange Activesync features are enabled by default for all mobile devices at the organizational level on Exchange Server 2003 and Exchange Server 2007. You can use Active Directory to enable or disable specific users or groups.

- Enable Exchange ActiveSync for specific users/groups using the Active Directory service. (For Exchange Server 2007, this is done in the Exchange Management Console under Recipient Configuration.)
- Configure mobile features, policies, and device security settings using the Exchange System Manager. (For Exchange Server 2007, these features and settings are configured in the Exchange Management Console.)
- Download and install the Microsoft Exchange ActiveSync Mobile Administration Web Tool, which is necessary for remote wipe. (For Exchange Server 2007, remote wipe can be initiated from Outlook Web Access or the Exchange Management Console.)

Exchange ActiveSync Deployment Scenario

This example shows how iPhone 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. 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.
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 are routed to external recipients 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.

iPhone and Virtual Private Networks (VPNs)

VPN protocols

- Cisco IPSec
- L2TP/IPSec
- PPTP

Authentication methods

- Password (MS-CHAPv2)
- RSA SecureID
- CRYPTOCard
- Certificates (PKCS1, PKCS12)
- Shared secret

Secure Access to private corporate networks is available on iPhone using the most popular industry-standard VPN protocols. iPhone 2.0 software 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.

Cisco IPSec deployments can take advantage of certificate-based authentication via industry-standard x.509 digital certificates (PKCS1, PKCS12). For two-factor token-based authentication, iPhone supports RSA SecureID as well as CRYPTOCard. Users enter their PIN and token-generated, one-time password directly on their iPhone when establishing a VPN connection.

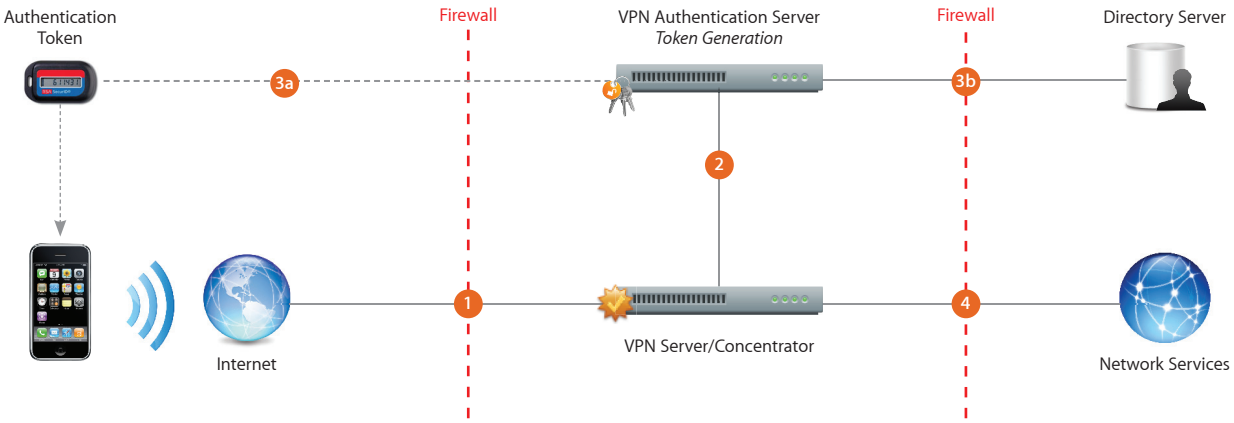
iPhone supports shared secret authentication for Cisco IPSec and L2TP/IPSec deployments. And for basic username and password authentication, iPhone supports MS-CHAPv2. Regardless of the authentication method, preconfigured VPN settings can be distributed to users via a Configuration Profile or entered directly on iPhone.

VPN Setup

- Because iPhone integrates with most existing VPN networks, minimal configuration should be necessary to enable iPhone access to your network. The best way to prepare for deployment is to ensure iPhone is compatible with your company's existing VPN protocols and authentication methods.
- Ensure compatibility of existing standards with your VPN concentrators. It's also a good idea to review the authentication path to your RADIUS or authentication server to ensure standards supported on iPhone are enabled within your existing implementation.
- Check with your solutions providers to confirm that your software and equipment are up to date with the latest security patches and firmware.
- For additional documentation regarding the Cisco IPSec protocol and specifications, visit www.cisco.com.

VPN Deployment Scenario

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



1. iPhone requests access to network services (typically over a PPP connection).
2. The VPN server/concentrator receives the request, then passes the request 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 or 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 network access policies.
4. After user and group policies are validated, the VPN server provides tunneled and encrypted access to network services (typically via IPSec).

iPhone and 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
- PEAPv0 (EAP-MSCHAPv2)
- PEAPv1 (EAP-GTC)
- LEAP

iPhone 2.0 software delivers WPA2 Enterprise, ensuring corporate wireless networks are securely accessed on iPhone. WPA2 Enterprise uses 128-bit 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 authentication, iPhone can be integrated into a broad range of RADIUS server environments. 802.1x wireless authentication methods supported on iPhone include EAP-TLS, EAP-TTLS, EAP-FAST, PEAPv0, PEAPv1 and LEAP.

For quick setup and deployment, WPA2 Enterprise network, security, and authentication settings can be configured using Configuration Profiles. For more information, see the iPhone Device Configuration Overview.

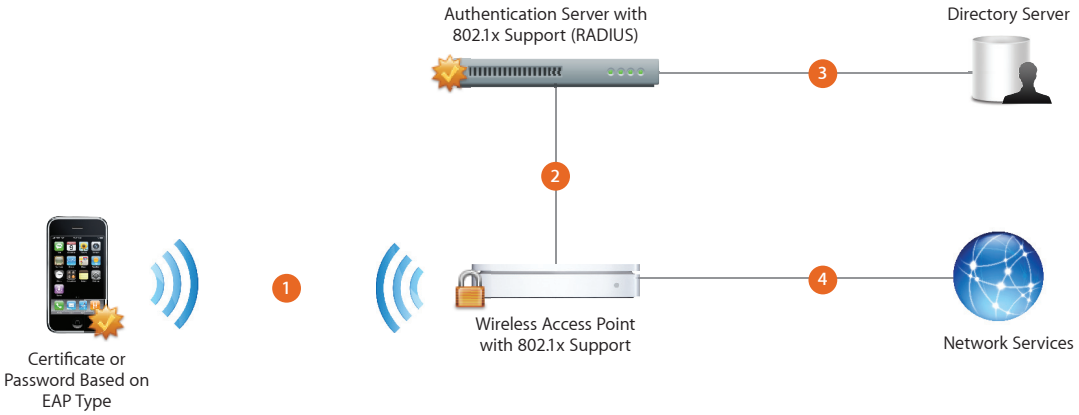
WPA2 Enterprise Setup

Network configuration

- Verify network appliances for compatibility and select an authentication type (EAP type) supported by iPhone.
- 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 you have your public key infrastructure configured to support device and user-based certificates with the corresponding key distribution process.
- Verify certificate format and authentication server compatibility. iPhone supports PKCS1 (.cer, .crt, .der) and PKCS12 (.p12, .pfx).
- For additional documentation regarding wireless networking standards and Wi-Fi Protected Access (WPA), visit www.wi-fi.org.

WPA2 Enterprise Deployment Scenario

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



1. iPhone requests access to network services. By selecting a wireless network, or configuring access to a specific SSID, iPhone 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.

iPhone and IMAP

IMAP or POP-enabled mail solutions
iPhone supports industry-standard IMAP4- and POP3-enabled mail solutions 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.

With support for the IMAP mail protocol, iPhone can integrate with just about any mail server environment. If the server supports IMAP and is configured to require user authentication and SSL, iPhone provides a highly secure, standards-based approach to email deployment. In a typical deployment, iPhone establishes direct access to an IMAP-enabled server over port 993 and access to SMTP servers over port 587. These 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. iPhone also supports strong authentication methods, including industry-standard MD5 Challenge-Response and NTLMv2.

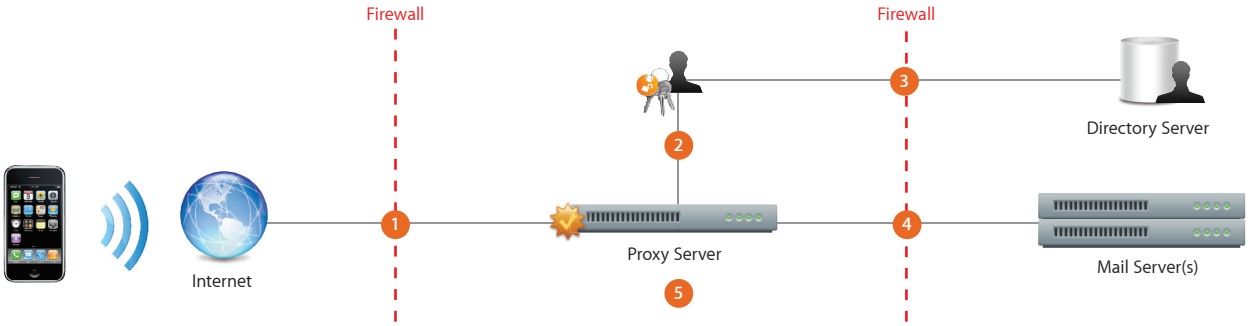
IMAP Network Setup

The IT or network administrator will need to complete these key steps to enable direct access from iPhone to an IMAP-enabled mail solution:

- Open port 993 to allow email to be received through the firewall. The proxy server must be set to IMAP over SSL. SSL ensures that mail is securely encrypted during wireless transmission.
- As a best practice and for additional security protection, install a digital certificate on the server from a trusted certificate authority (CA) such as VeriSign. Installing a certificate from a CA is an important step in ensuring that your proxy server is a trusted entity within your corporate infrastructure.
- 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 is considered the least secure because it's been around the longest and is subject to more attacks by hackers. It's also the port that some ISPs block by default to prevent spam.

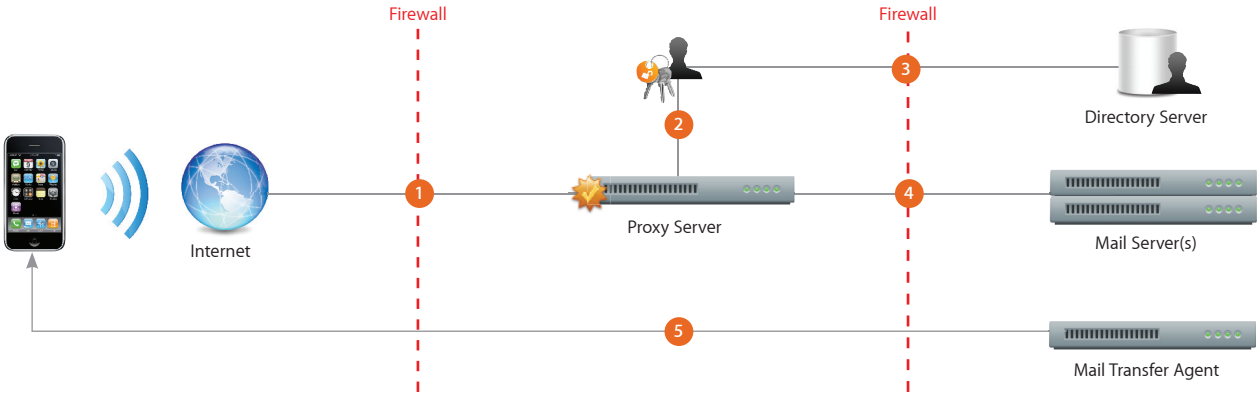
IMAP Deployment Scenario

Receiving email



1. iPhone requests access to email over port 993 (IMAP/SSL).
2. Next, the iPhone user must be authenticated by the corporate network. This is handled by the proxy server, which functions as a secure gateway.
3. The proxy server verifies account information using the directory service.
4. Once the user is authenticated, the proxy server routes the request to the mail server.
5. Messages and updates are retrieved and sent back through port 993. What the user sees are new messages and inbox updates on iPhone.

Sending email



1. Sent email is routed through port 587 (SSL/TLS).
2. Send mail requests are then routed through the proxy server.
3. The proxy server initiates the authentication process with the directory service.
4. Once the user is authenticated, the message is routed through the mail server and a copy is placed in the user's Sent folder.
5. The message then goes through the mail transfer agent and is sent through port 587 to the external recipient via SMTP (SSL/TLS).

iPhone Device Configuration

Deploying iPhone across your enterprise is easy with iPhone 2.0 software. iPhone devices can be configured via Configuration Profiles created and distributed by your IT department. Configuration Profiles are XML files that, when installed, provide information that iPhone can use to connect to and communicate with your enterprise systems.

Configuration Profile Components

Exchange settings
Include server, domain, and account information in a Configuration Profile so that your users simply provide a password to connect via Microsoft Exchange ActiveSync.

Wireless settings
Whether you are configuring iPhone to connect to a private network, or for RADIUS authentication to enterprise wireless access points, Configuration Profiles can be deployed to streamline corporate access point connections.

VPN settings
Configure VPN server settings, accounts, proxies, certificates, tokens, passwords, groups, and shared secrets for your corporate private networks.

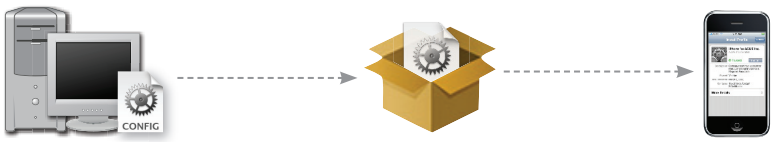
Email settings
Configure IMAP or POP mail settings, including incoming and outgoing mail servers.

Passcode policies
Protect your enterprise data by configuring and enforcing device passcode policies. Set the minimum number of characters, number of complex characters, passcode age, device lock interval, and maximum failed attempts.

Certificates
Ensure the identity of your users and control access to key enterprise services such as VPN and WPA2 Enterprise/802.1x networks on iPhone. Deploy certificates in raw formats PKCS1 (.cer, .crt, .der) and PKCS12 (.p12, .pfx).

Restrictions
Control the installation of third-party applications, Safari, YouTube, the iTunes Wi-Fi Music Store, and explicit content.

Signatures
Wrap your Configuration Profile with an identity so your users can be sure it's coming from a trusted source.



1 Create Configuration Profile (XML)

2 Distribute Profile via Email or Website

3 Install Profile on iPhone

1 Creating Profiles

iPhone Configuration Utility

A simple and intuitive application for IT administrators, the iPhone Configuration Utility gives you the ability to easily create Configuration Profiles. The iPhone Configuration Utility is available as a web application or as a native desktop application for Mac OS X.

2 Distributing Profiles

Secure website

- Export the profile from the iPhone Configuration Utility.
- Add the appropriate MIME type to your web server.
  application/x-apple-aspen-config mobileconfig
- Host Configuration Profile (uncompressed) in a secure site accessible to user(s).

Email attachment

- Export the profile from the iPhone Configuration Utility.
- Attach the Configuration Profile (uncompressed) to an email and send to user(s).

3 Installing Profiles

Installation on iPhone

- If the profile is web-hosted, navigate to the website using Safari on iPhone, and tap to install the Configuration Profile.
- Configuration Profiles that are sent as an email attachment can be installed by tapping the file directly from the message body in Mail on iPhone.
- Tap Install to accept the settings.
  During installation, users are asked to enter any necessary information (such as account passwords) to complete the device configuration.