Deploying iPhone and iPad
Virtual Private Networks

Secure access to private corporate networks is available on iPhone and iPad using established industry-standard virtual private network (VPN) protocols. Users can easily connect to enterprise systems via the built-in VPN client in iOS or through third-party applications from Juniper Networks, Cisco, SonicWALL, Check Point, Aruba Networks, and F5 Networks.

Out of the box, iOS 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 and iPad to your VPN.

Additionally, iOS supports SSL VPN, enabling access to Juniper Networks, Cisco, SonicWALL, Check Point, Aruba Networks, and F5 Networks SSL VPN servers. Users simply download a VPN client application developed by one of these companies from the App Store to get started. Like other VPN protocols supported in iOS, SSL VPN can be configured manually on the device or via Configuration Profile.

iOS supports industry-standard technologies such as IPv6, proxy servers, and split-tunneling, providing a rich VPN experience when connecting to corporate networks. And iOS 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, iOS 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, iOS supports VPN On Demand. VPN On Demand will establish a connection automatically when accessing predefined domains, providing a seamless VPN connectivity experience for 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

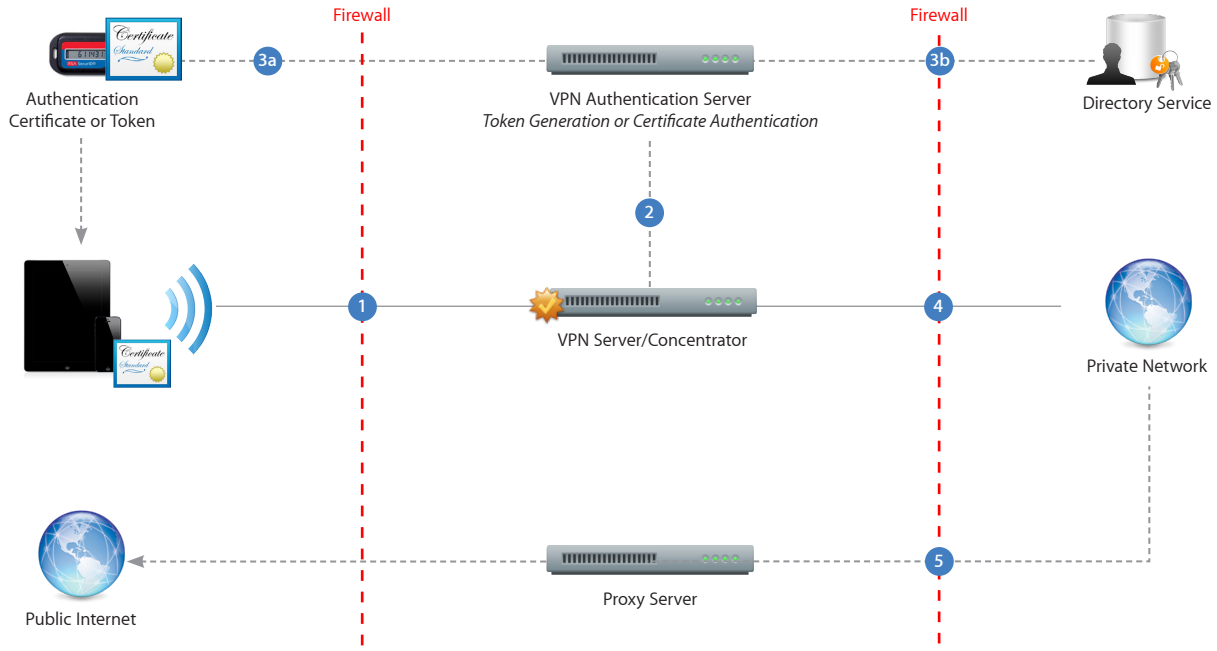
- iOS integrates with many existing VPN networks, with minimal configuration necessary. The best way to prepare for deployment is to check whether iOS supports your company's existing VPN protocols and authentication methods.
- It's recommended that you review the authentication path to your authentication server to make sure standards supported by iOS 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 and iPad 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 and iPad request 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 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.

   If a proxy server is in use, iPhone and iPad connect through the proxy server for access to information outside the firewall.

Deploying iPhone and iPad
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 and iPad 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.

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

Users can set iPhone and iPad 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 applications to use Wi-Fi networks to deliver push notifications.

For roaming on large enterprise Wi-Fi networks, iPhone and iPad support 802.11k and 802.11r.* 802.11k helps iPhone and iPad transition between base stations by utilizing the reports from the base station, while 802.11r streamlines 802.1X authentication as a device moves from one access point to another.

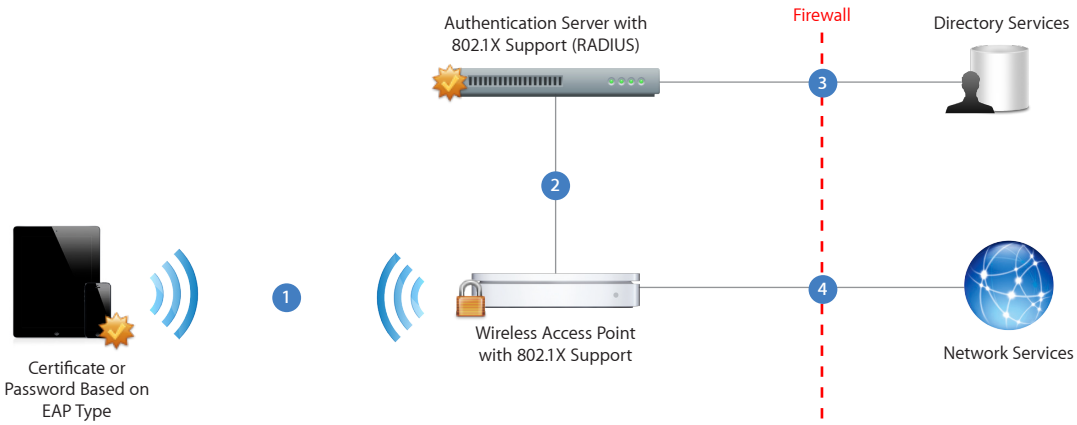
For quick setup and deployment, wireless network, security, proxy, and authentication settings can be configured using Configuration Profiles.

WPA2 Enterprise Setup

- Verify network appliances for compatibility and select an authentication type (EAP type) supported by iOS.
- 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. iOS 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 and iPad request access to the network. The connection is initiated in response to a user selecting an available wireless network, or is automatically initiated after a previously configured network is detected.
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 4S, iPhone 5, new iPad, and 5th-generation iPod touch support 802.11k and 802.11r.