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.

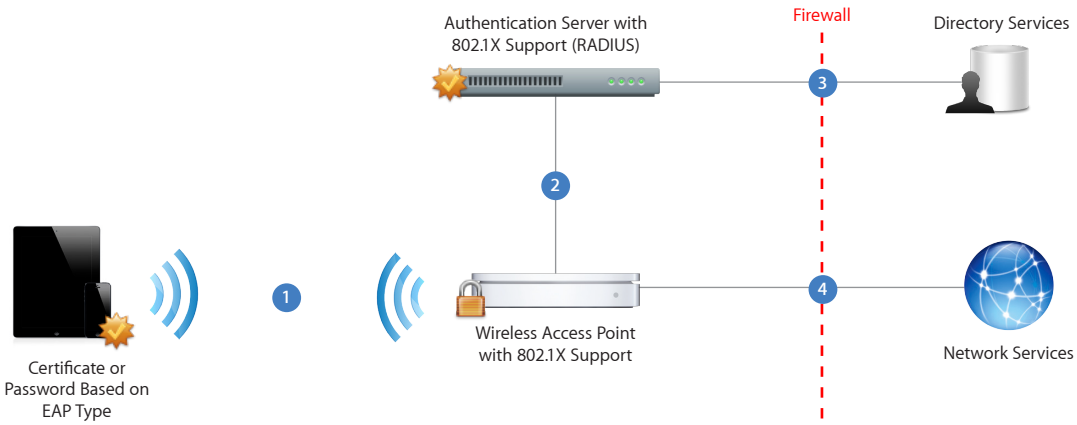
For quick setup and deployment, wireless network, security, proxy, and authentication settings can be configured using Configuration Profiles.

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.