



# 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.

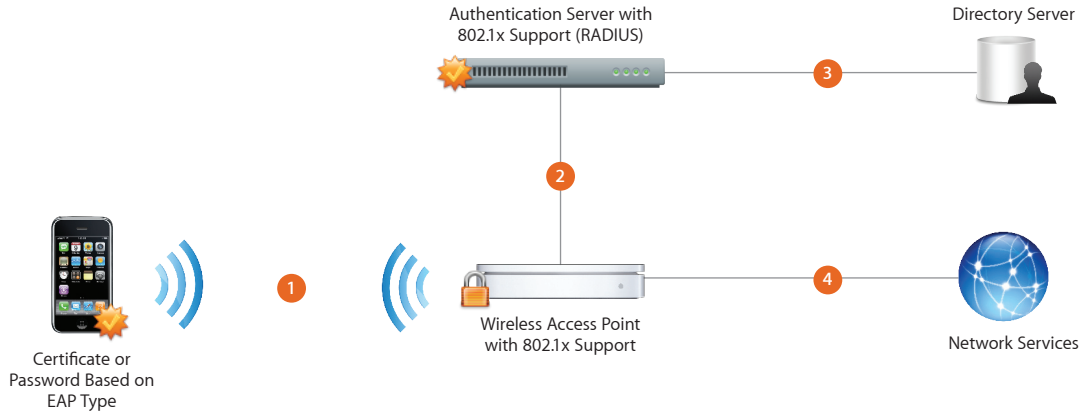
## WPA2 Enterprise Setup

### 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](http://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.