



# iPhone et WPA2 Enterprise/802.1x



## Protocoles de sécurité sans fil

- WEP
- WPA Personal
- WPA Enterprise
- WPA2 Personal
- WPA2 Enterprise

## Méthodes d'authentification 802.1x

- EAP-TLS
- EAP-TTLS
- EAP-FAST
- PEAPv0 (EAP-MS-CHAPv2)
- PEAPv1 (EAP-GTC)
- LEAP

La prise en charge par le logiciel iPhone 2.0 du protocole WPA2 Enterprise permet de s'assurer que l'on accède aux réseaux sans fil de manière sécurisée sur iPhone. WPA2 Enterprise utilise le cryptage AES à 128 bits, une méthode de cryptage par blocs qui a fait ses preuves et qui confère à la protection des données d'entreprise un haut degré d'assurance.

Avec la prise en charge de l'authentification 802.1x, iPhone peut s'intégrer dans une grande variété d'environnements de serveur RADIUS. Les méthodes d'authentification sans fil 802.1x, telles que EAP-TLS, EAP-TTLS, EAP-FAST, PEAPv0, PEAPv1 et LEAP, sont prises en charge.

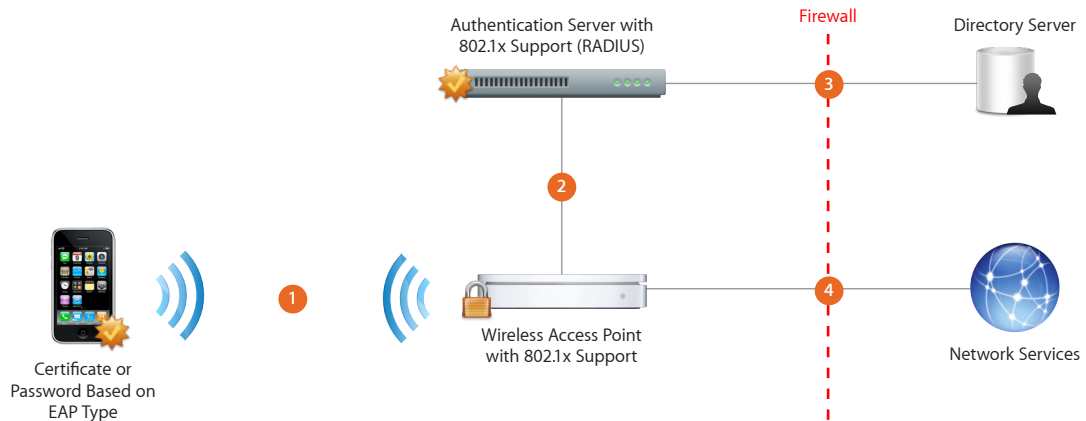
Pour faciliter la configuration et le déploiement, les paramètres de réseau, de sécurité et d'authentification WPA2 Enterprise peuvent être définis à l'aide de profils de configuration. Pour plus d'informations, consultez le document d'introduction à la configuration iPhone.

## Configuration du protocole WPA2 Enterprise

- Vérifiez que les équipements réseau sont compatibles et sélectionnez un type d'authentification (type EAP) pris en charge par iPhone.
- Assurez-vous que 802.1x est activé sur le serveur d'authentification et, si nécessaire, installez un certificat de serveur et assignez des permissions d'accès réseau aux utilisateurs et groupes.
- Configurez des points d'accès sans fil pour l'authentification 802.1x et saisissez les informations sur le serveur RADIUS correspondantes.
- Testez votre déploiement 802.1x avec un Mac ou un PC pour vous assurer que l'authentification RADIUS est configurée correctement.
- Si vous comptez utiliser l'authentification par certificats, assurez-vous que votre infrastructure à clé publique est configurée de manière à prendre en charge les certificats d'appareil et d'utilisateur avec le processus de distribution de clés correspondant.
- Vérifiez que le format des certificats est compatible avec le serveur d'authentification. iPhone prend en charge PKCS1 (.cer, .crt, .der) et PKCS12 (.p12, .pfx).
- Vérifiez auprès de votre fournisseur de solutions que les derniers correctifs de sécurité et programmes internes sont bien installés sur vos logiciels et votre équipement.
- Des informations complémentaires sur les protocoles réseau sans fil et sur le protocole Wi-Fi Protected Access (WPA) sont disponibles à l'adresse [www.wi-fi.org](http://www.wi-fi.org).

## Scénario de déploiement WPA2/802.1x Enterprise

Cet exemple présente un déploiement sans fil sécurisé standard tirant parti de l'authentification RADIUS.



- 1 iPhone demande l'accès aux services réseau. En sélectionnant un réseau sans fil ou en configurant l'accès à un SSID spécifique, iPhone lance la connexion.
- 2 Lorsque le point d'accès reçoit la requête, celle-ci est transmise au serveur RADIUS pour authentification.
- 3 Le serveur RADIUS identifie le compte utilisateur à l'aide du service d'annuaire.
- 4 Une fois l'utilisateur identifié, le point d'accès ouvre l'accès réseau en fonction des stratégies et des autorisations définies par le serveur RADIUS.