

# CLIENT VPN iOS

Le client VPN de confiance pour vos connexions depuis un iPhone ou iPad

Facile à installer et à utiliser dans une infrastructure existante, le Client VPN iOS est adapté aux échanges de données sécurisées sur iPhone et iPad. Il répond aux exigences de sécurisation des communications pour le nomadisme digital et le télétravail.



## Haut niveau de sécurité

Le Client VPN iOS a été développé en suivant les recommandations du NIST et de l'ANSSI. L'ensemble des protocoles et algorithmes mis en oeuvre dans le logiciel en font un client universel pour se connecter à toutes les passerelles VPN IPsec et OpenVPN du marché, qu'elles soient logicielles ou matérielles.



## Facilité d'installation

L'installation sur n'importe quel iPhone ou iPad avec iOS 13.0 ou supérieur s'effectue de façon guidée en quelques clics de souris.

Le logiciel offre une variété de protocoles, de paramètres et d'options permettant une interopérabilité avec votre passerelle / pare-feu et votre PKI.



## Simplicité d'utilisation

Le Client VPN iOS simplifie l'usage du VPN en proposant une interface utilisateur ergonomique pour établir des connexions sécurisées vers votre système d'information.

Les utilisateurs ont une vision directe de l'état des connexions VPN pour vérifier que leurs communications sont bien protégées. Une interface d'administration complète donne accès à l'ensemble des paramètres pour définir les règles de sécurité à appliquer sur le poste, ou à déployer sur d'autres postes.

## CARACTÉRISTIQUES TECHNIQUES

Protocoles	<ul style="list-style-type: none"> <li>● IPsec IKEv2</li> <li>● OpenVPN</li> <li>● Réseau : IPv4, IPv6, NAT-Traversal, fragmentation IKE</li> </ul>
Authentification	<ul style="list-style-type: none"> <li>● Authentification : EAP, PSK, certificats</li> <li>● Gestion des certificats X.509 : DER/PEM ; PFX/P12</li> </ul>
Cryptographie	<ul style="list-style-type: none"> <li>● DH 14-21, AES-CBC, AES-GCM, AES-CTR (128/196/256), SHA-2 (256/384/512)</li> <li>● Méthodes d'authentification des certificats : Méthode 1 : RSA Digital Signature</li> </ul>
Configuration requise	<ul style="list-style-type: none"> <li>● iOS 13 ou supérieur</li> <li>● 10 Mo d'espace disponible pour l'application</li> </ul>

### Principales fonctionnalités

- Panneau de configuration
- Gestion des tunnels : full tunneling, split tunneling
- Continuité de service : DPD (Dead Peer Detection), passerelle redondante
- Gestion du mode CP (IKEv2)
- Configuration et établissement de connexion SSL (OpenVPN)

