Réseau

La section **Réseau** de l'éditeur de stratégie Apple configure les réseaux Wi-Fi et les VPN sur les appareils, installe des certificats et restreint les fonctions de connectivité comme AirDrop et Bluetooth. Chaque réseau Wi-Fi, VPN et certificat est installé sous forme de profil de configuration distinct, que vous pouvez voir sur l'appareil dans **Réglages > Général > VPN et gestion de l'appareil** (Mac : **Réglages Système > Général > Gestion de l'appareil**, ou **Confidentialité et sécurité > Profils** sur macOS 13 et 14) et dans le panneau **Profils, certificats et sécurité** de la page de l'appareil.

> Les certificats proviennent de la page **Certificats** : importez-les d'abord à cet endroit. La stratégie ne fait que les référencer, ainsi un certificat n'est jamais copié dans la stratégie.

Restrictions

- **Autoriser AirDrop**
- **Autoriser les demandes AirPlay entrantes**
- **Autoriser la modification de Bluetooth**
- **Autoriser la modification du partage Bluetooth**
- **Autoriser l'accès aux lecteurs réseau dans Fichiers**
- **Autoriser la modification du partage Internet**
- **Autoriser la mise en cache du contenu**
- **Autoriser le partage de fichiers iTunes**

Réseaux Wi-Fi

Cliquez sur **Ajouter un réseau Wi-Fi** et renseignez :

- **Nom du réseau (SSID)** : le nom du réseau, jusqu'à 32 caractères.
- **Sécurité** : aucune (réseau ouvert), WEP, WPA ou WPA2, WPA2 ou WPA3, WPA3 uniquement, ou indifférent.
- **Mot de passe** : le mot de passe d'un réseau personnel.
- **Rejoindre automatiquement** et **Réseau masqué** (pour les réseaux qui ne diffusent pas leur nom).
- **Proxy** : aucun, manuel (serveur et port) ou automatique (une URL de fichier PAC, ou vide pour trouver les réglages sur le réseau avec WPAD).

- **Nom du profil** (facultatif) et **S'applique à**, pour limiter le réseau à certains types d'appareils.

Réseaux d'entreprise (802.1X)

Activez **Entreprise (802.1X)** lorsque les utilisateurs s'authentifient avec leurs propres identifiants ou un certificat au lieu d'un mot de passe partagé.

- **Authentification** : PEAP, TTLS (avec son authentification interne, par exemple MSCHAPv2) ou TLS (certificat uniquement).
- **Identifiants de l'utilisateur de l'appareil** : chaque appareil utilise l'identité EAP, l'identité anonyme et le mot de passe de son utilisateur, définis dans la page Utilisateurs. Les appareils sans utilisateur ne reçoivent pas le réseau.
- **Identité**, **Identité anonyme** et **Mot de passe** : les mêmes pour chaque appareil. L'identité peut contenir les variables $EMAIL$, $USERNAME$, $FULLNAME$, $SERIAL$ et $UDID$. Laissez le mot de passe vide pour que l'utilisateur le saisisse sur l'appareil.
- **Certificat d'identité** : le certificat client que l'appareil présente (obligatoire pour TLS). Voir les options de certificat ci-dessous.
- **Certificats de confiance** : les certificats CA qui ont émis le certificat de votre serveur RADIUS. Ils sont installés avec le réseau.
- **Noms de serveur de confiance** : les noms des certificats du serveur RADIUS que les appareils acceptent, par exemple radius.example.com ou *.example.com.

VPN

Cliquez sur **Ajouter un VPN** pour configurer un VPN IKEv2 ou Cisco IPSec, intégré à iOS, iPadOS et macOS (aucune app VPN nécessaire).

- **Type** et **Serveur**. Pour IKEv2 également l'**Identifiant distant** (l'identité du serveur, vide signifie l'adresse du serveur) et l'**Identifiant local**, qui peut contenir les variables $EMAIL$, $USERNAME$, $FULLNAME$, $SERIAL$ et $UDID$.
- **Authentification** de l'appareil : un certificat (depuis la page Certificats, le certificat de l'utilisateur de l'appareil, ou demandé à un serveur SCEP), un secret partagé (avec le nom de groupe facultatif pour IPSec), ou aucune pour les serveurs IKEv2 qui vérifient uniquement le nom d'utilisateur et le mot de passe.
- **Certificats de confiance** : les certificats CA de votre serveur VPN, installés avec le VPN. Pour IKEv2, vous pouvez aussi définir l'émetteur et le nom attendus du certificat du serveur.
- **Nom d'utilisateur et mot de passe** : l'utilisateur s'authentifie aussi avec un nom d'utilisateur (variables autorisées) et un mot de passe (EAP pour IKEv2, XAuth pour IPSec). Laissez le mot de passe vide pour que l'utilisateur le saisisse sur l'appareil.
- **Nom du VPN** (affiché dans Réglages) et **S'applique à**.

Connexion

- **L'utilisateur se connecte dans Réglages** : le VPN est installé et l'utilisateur l'active lorsqu'il en a besoin.
- **À la demande** : l'appareil connecte automatiquement le VPN. Avec **sauf sur les Wi-Fi de confiance**, le VPN n'est pas utilisé sur les réseaux Wi-Fi que vous listez, par exemple le réseau du bureau.
- **Toujours actif** (IKEv2, iPhone et iPad supervisés uniquement) : tout le trafic passe par le VPN en cellulaire et en Wi-Fi et l'utilisateur ne peut pas le désactiver. Les autres appareils ne reçoivent pas ce VPN. Si le VPN utilise un nom d'utilisateur, le mot de passe doit être défini dans la stratégie.
- **VPN par app** : seules certaines apps utilisent le VPN. Choisissez le VPN pour chaque app dans la section **Gestion des apps** (champ **VPN** de l'app, non disponible sur Mac), et listez éventuellement les domaines Safari qui l'utilisent.

> Testez d'abord un VPN Toujours actif ou à la demande sur un appareil de test : si le serveur est inaccessible, l'appareil peut ne plus avoir de connexion.

Proxy global, DNS chiffré et filtre de contenu web

Ces paramètres s'appliquent à tout le trafic de l'appareil. Activez-les avec leur commutateur.

- **Proxy HTTP global** (iPhone et iPad supervisés, Mac) : tout le trafic HTTP passe par le proxy, sur chaque réseau. Définissez le serveur et le port (avec un nom d'utilisateur et un mot de passe facultatifs) ou une configuration automatique (URL de fichier PAC, ou vide pour la trouver sur le réseau). **Autoriser les pages de connexion Wi-Fi** permet à l'utilisateur de se connecter aux réseaux Wi-Fi publics sans le proxy.
- **DNS chiffré** : l'appareil résout les noms avec votre serveur DNS via DNS over HTTPS (URL du serveur) ou DNS over TLS (nom du serveur), éventuellement uniquement pour certains domaines. Sur les appareils supervisés, vous pouvez empêcher l'utilisateur de le désactiver.
- **Filtre de contenu web** (iPhone et iPad supervisés) : le filtre intégré à iOS limite les sites pour adultes, avec des listes de sites toujours autorisés ou toujours bloqués, ou autorise uniquement une liste de sites, affichés comme favoris dans Safari.

> Un proxy ou un serveur DNS incorrect peut laisser les appareils sans connexion : essayez d'abord les paramètres sur un appareil de test.

Certificats

Cliquez sur **Ajouter un certificat** pour installer un certificat seul : une autorité de certification à laquelle Safari et les apps doivent faire confiance, ou une identité utilisée par des apps. Les certificats d'un réseau Wi-Fi ou d'un VPN n'ont pas besoin d'être ajoutés ici.

Options de certificat

- **Un certificat de la page Certificats** : le même certificat sur chaque appareil. Cliquez sur **Choisir un certificat** pour le sélectionner.
- **Le certificat de l'utilisateur de l'appareil** : chaque appareil reçoit le certificat client lié à son utilisateur. Les appareils dont l'utilisateur n'a pas de certificat ne le reçoivent pas. Lorsque vous liez un autre certificat à l'utilisateur, les appareils sont mis à jour.
- **Demandé à un serveur SCEP** : chaque appareil demande son propre certificat à votre serveur SCEP (par exemple Microsoft NDES), de sorte que la clé privée ne quitte jamais l'appareil. Définissez l'URL du serveur, le défi si le serveur en exige un, le sujet (par exemple CN=$EMAIL$), les noms alternatifs, la taille de clé et l'usage de la clé.

> Les certificats client (.p12) protégés par l'ancien chiffrement RC2 ne peuvent pas être installés sur les appareils Apple. Exportez-les de nouveau avec le chiffrement 3DES ou AES avant de les importer.

Sécurité

Les profils qui contiennent des mots de passe ou des clés privées sont envoyés uniquement à l'appareil pour lequel ils ont été créés : l'appareil doit signer sa demande avec son certificat de gestion. Les mots de passe et les certificats ne sont pas écrits dans les journaux.

Revision #6
Created 2026-11-10 15:15:27 UTC by Admin
Updated 2026-11-12 09:55:16 UTC by Admin