Réseau

Dans cette section, vous pouvez configurer les stratégies liées au réseau.

> Les configurations Wi-Fi peuvent être provisionnées et gérées par le système via **Configurations Wi-Fi**. Selon la valeur définie pour **Configurer le Wi-Fi**, les utilisateurs peuvent avoir un contrôle limité ou nul sur l'ajout et la modification des réseaux.

État des radios de l'appareil

1. État du Wi-Fi

Contrôle l'état actuel du Wi-Fi et si l'utilisateur peut modifier cet état.

> **Choix de l'utilisateur (par défaut)** : l'utilisateur est autorisé à activer ou désactiver le Wi-Fi.
>
> **Activé** : le Wi-Fi est activé et l'utilisateur n'est pas autorisé à le désactiver (Android 13+).
>
> **Désactivé** : le Wi-Fi est désactivé et l'utilisateur n'est pas autorisé à l'activer (Android 13+).

2. Niveau de sécurité Wi-Fi minimal

Niveau de sécurité minimal requis des réseaux Wi-Fi auxquels l'appareil peut se connecter. Pris en charge sous Android 13 et versions ultérieures, pour les appareils entièrement gérés et les profils professionnels sur les appareils appartenant à l'entreprise.

> **Réseau ouvert (par défaut)** : l'appareil peut se connecter à tous les types de réseaux Wi-Fi.
>
> **Réseau personnel** : interdit les réseaux Wi-Fi ouverts ; exige au moins une sécurité personnelle (par exemple WPA2-PSK).
>
> **Réseau d'entreprise** : exige des réseaux EAP d'entreprise ; interdit les réseaux Wi-Fi inférieurs à ce niveau de sécurité.

Réseau d'entreprise 192 bits : exige des réseaux d'entreprise 192 bits ; option la plus stricte.

3. État de l'ultra large bande (UWB)

Contrôle l'état du paramètre ultra large bande et si l'utilisateur peut l'activer ou le désactiver.

Choix de l'utilisateur (par défaut) : l'utilisateur est autorisé à activer ou désactiver l'UWB.

Désactivé : l'UWB est désactivé et l'utilisateur n'est pas autorisé à l'activer via les paramètres (Android 14+).

Gestion de la connectivité de l'appareil

4. Partage Bluetooth

Contrôle si le partage Bluetooth est autorisé.

Autorisé : le partage Bluetooth est autorisé (par défaut sur les appareils entièrement gérés, Android 8+).

Interdit : le partage Bluetooth est interdit (par défaut sur les profils professionnels, Android 8+).

5. Configurer le Wi-Fi

Contrôle les privilèges de configuration du Wi-Fi. Selon l'option sélectionnée, l'utilisateur dispose d'un contrôle total, limité ou nul sur la configuration des réseaux Wi-Fi.

Autoriser la configuration du Wi-Fi (par défaut) : l'utilisateur est autorisé à configurer le Wi-Fi.

Interdire l'ajout de configurations Wi-Fi : l'ajout de nouvelles configurations Wi-Fi est interdit. L'utilisateur peut basculer entre les réseaux déjà configurés (Android 13+ ; appareils entièrement gérés et profils professionnels sur appareils d'entreprise).

Interdire la configuration du Wi-Fi : interdit la configuration des réseaux Wi-Fi. Pour les appareils entièrement gérés, cela supprime les réseaux configurés par l'utilisateur et conserve uniquement les réseaux configurés via **Configurations Wi-Fi**. Pour les profils professionnels sur appareils d'entreprise, les réseaux existants ne sont pas affectés, mais les utilisateurs ne peuvent pas ajouter, supprimer ou modifier de réseaux Wi-Fi.

> Lorsque la configuration du Wi-Fi est désactivée et que l'appareil ne peut pas se connecter au démarrage, le système peut afficher le **moyen de secours réseau** pour permettre à l'utilisateur de se connecter temporairement et d'actualiser la stratégie.

6. Paramètres du Wi-Fi Direct

Contrôle la configuration et l'utilisation des paramètres Wi-Fi Direct. Pris en charge sur les appareils appartenant à l'entreprise sous Android 13 et versions ultérieures.

Autoriser (par défaut) : l'utilisateur est autorisé à utiliser le Wi-Fi Direct.

Interdire : l'utilisateur n'est pas autorisé à utiliser le Wi-Fi Direct.

7. Paramètres de partage de connexion

Contrôle les paramètres de partage de connexion. Selon la valeur définie, l'utilisateur se voit partiellement ou totalement interdire l'utilisation des différentes formes de partage de connexion.

Autoriser tous les partages de connexion (par défaut) : autorise la configuration et l'utilisation de toutes les formes de partage de connexion.

Interdire le partage de connexion Wi-Fi : interdit à l'utilisateur d'utiliser le partage de connexion Wi-Fi (appareils d'entreprise Android 13+).

Interdire tous les partages de connexion : interdit toutes les formes de partage de connexion (appareils entièrement gérés + profils professionnels sur appareils d'entreprise).

8. Stratégie de SSID Wi-Fi

Restrictions sur les SSID Wi-Fi auxquels l'appareil peut se connecter (cela n'affecte pas les réseaux qui peuvent être configurés sur l'appareil). Pris en charge sur les appareils appartenant à l'entreprise sous Android 13 et versions ultérieures.

Liste de refus des SSID (par défaut) : l'appareil ne peut se connecter à aucun réseau Wi-Fi dont le SSID figure dans la liste, mais peut se connecter à d'autres réseaux.

Liste d'autorisation des SSID : l'appareil peut se connecter uniquement aux SSID répertoriés. La liste des SSID ne doit pas être vide.

Utilisez **Ajouter un SSID** pour ajouter des entrées. Selon le type de stratégie sélectionné, la liste est interprétée comme des SSID autorisés ou refusés.

Dans l'interface de l'éditeur de stratégie, la liste des SSID est intitulée **SSID Wi-Fi autorisés** pour les listes d'autorisation et **SSID Wi-Fi refusés** pour les listes de refus.

9. Paramètres d'itinérance Wi-Fi

Configurez le mode d'itinérance Wi-Fi par SSID. Utilisez **Ajouter un paramètre d'itinérance Wi-Fi** pour créer des entrées.

Chaque entrée comprend :

SSID : le SSID auquel le paramètre d'itinérance s'applique (obligatoire).

Mode d'itinérance Wi-Fi : Par défaut / Désactivé / Agressif. Les modes Désactivé et Agressif nécessitent Android 15+ et ne sont pris en charge que sur les appareils entièrement gérés et les profils professionnels sur les appareils appartenant à l'entreprise.

Restrictions réseau

10. Bluetooth désactivé

Indique si le Bluetooth est désactivé. Préférez ce paramètre à Configuration Bluetooth désactivée, car celle-ci peut être contournée par l'utilisateur.

11. Partage de contacts Bluetooth désactivé

Indique si le partage de contacts Bluetooth est désactivé.

12. Configuration Bluetooth désactivée

Indique si la configuration du Bluetooth est désactivée.

13. Réinitialisation réseau désactivée

Indique si la réinitialisation des paramètres réseau est désactivée.

14. Émission sortante via Beam désactivée

Indique si l'utilisation du NFC pour envoyer des données depuis des applications est désactivée.

VPN

15. Application VPN Always On

Spécifiez un nom de package VPN Always On pour garantir que les données des applications gérées spécifiées passent toujours par un VPN configuré.

> Remarque : cette fonctionnalité nécessite le déploiement d'un client VPN compatible avec les fonctions Always On et VPN par application.

16. Verrouillage VPN

Interdit la mise en réseau lorsque le VPN n'est pas connecté.

17. Configuration VPN désactivée

Indique si la configuration du VPN est désactivée.

Proxy et services réseau

18. Service réseau préférentiel

Contrôle si le service réseau préférentiel est activé sur le profil professionnel. Par exemple, une organisation peut avoir un accord avec un opérateur pour que les données professionnelles soient envoyées via un service réseau de l'opérateur dédié à l'usage professionnel (par exemple, une tranche d'entreprise sur les réseaux 5G). Cela n'a aucun effet sur les appareils entièrement gérés.

Désactivé : le service réseau préférentiel est désactivé sur le profil professionnel.

Activé : le service réseau préférentiel est activé sur le profil professionnel.

> Si vous utilisez le découpage réseau d'entreprise, configurez également **Configuration du découpage réseau 5G** dans le panneau de stratégie **Cellulaire** et affectez les applications à une tranche via leur paramètre **Réseau préférentiel**.

19. Proxy global recommandé

Proxy HTTP global indépendant du réseau. En général, les proxys doivent être configurés par réseau dans les configurations Wi-Fi. Un proxy global peut être utile pour des configurations particulières, comme un filtrage interne général. Le proxy global n'est qu'une recommandation et certaines applications peuvent l'ignorer.

Désactivé

Proxy direct

Configuration automatique du proxy (PAC)

19.1. Hôte

L'hôte du proxy direct.

19.2. Port

Le port du proxy direct.

19.3. URI PAC

L'URI du script PAC utilisé pour configurer le proxy.

19.4. Hôtes exclus

Pour un proxy direct, les hôtes pour lesquels le proxy est contourné. Les noms d'hôte peuvent contenir des caractères génériques tels que ***.example.com**.

Utilisez **Ajouter un hôte exclu** pour ajouter des entrées (disponible uniquement pour le proxy direct).

Configurations Wi-Fi

Définissez les configurations de réseau Wi-Fi que le système appliquera sur les appareils. Utilisez **Ajouter une configuration Wi-Fi** pour créer une entrée et supprimez-la avec l'action de suppression.

20. Champs de configuration Wi-Fi

Chaque configuration comprend :

Nom de la configuration : Obligatoire.

SSID : Obligatoire.

Connexion automatique : Indique si le réseau doit être connecté automatiquement lorsqu'il est à portée.

Transition rapide : Indique si le client doit tenter d'utiliser la transition rapide (IEEE 802.11r-2008) avec le réseau.

SSID masqué : Indique si le SSID sera diffusé.

Mode de randomisation MAC : Matériel ou Automatique (Android 13+).

20.1. Sécurité

Options de sécurité Wi-Fi :

WEP-PSK : WEP (clé prépartagée).

WPA-PSK : WPA/WPA2/WPA3-Personal (clé prépartagée).

WPA-EAP : WPA/WPA2/WPA3-Enterprise (protocole d'authentification extensible).

Mode 192 bits WPA3 : réseau WPA-EAP autorisant uniquement le mode 192 bits WPA3.

20.2. Phrase secrète (clé prépartagée)

Affiché lorsque la sécurité est **WEP-PSK** ou **WPA-PSK**. La phrase secrète est obligatoire.

20.3. Méthode EAP (Enterprise)

Affiché lorsque la sécurité est **WPA-EAP** ou **Mode 192 bits WPA3**. Sélectionnez une méthode EAP externe :

EAP-TLS

EAP-TTLS

PEAP

EAP-SIM

EAP-AKA

20.4. Authentification de phase 2

Affiché pour les méthodes externes utilisant un tunnel (**EAP-TTLS** et **PEAP**).

MSCHAPv2

PAP

20.5. Identifiants EAP fournis par les utilisateurs

Lorsque cette option est activée, le système applique automatiquement les identifiants EAP sur les appareils pour chaque utilisateur. Vous pouvez configurer les identifiants des utilisateurs dans la section **Utilisateurs**.

20.6. Certificat client

Pour **EAP-TLS**, vous pouvez attribuer un certificat client utilisé pour l'authentification Wi-Fi. Pour plus d'informations, consultez la page **Gestion des certificats**.

Si un certificat est déjà attribué, vous pouvez utiliser **Ouvrir le certificat** pour le consulter ou **Changer de certificat** pour en sélectionner un autre.

Vous pouvez également spécifier **Alias de paire de clés du certificat client**, qui référence un certificat client stocké dans le trousseau Android et autorisé pour l'authentification Wi-Fi.

> Si**Certificat client** et **Alias de paire de clés du certificat client** sont tous deux définis, l'alias de paire de clés est ignoré.

20.7. Identité

Identité de l'utilisateur. Pour les protocoles externes avec tunnel (PEAP, EAP-TTLS), elle est utilisée pour s'authentifier à l'intérieur du tunnel, et l'**Identité anonyme** est utilisée pour l'identité EAP à l'extérieur du tunnel. Pour les protocoles externes sans tunnel, elle est utilisée pour l'identité EAP.

20.8. Identité anonyme

Pour les protocoles avec tunnel uniquement, indique l'identité de l'utilisateur présentée au protocole externe.

20.9. Mot de passe

Mot de passe de l'utilisateur. S'il n'est pas spécifié, l'utilisateur sera invité à le saisir par défaut.

20.10. Certificats CA du serveur

Liste des certificats CA à utiliser pour vérifier la chaîne de certificats de l'hôte. Au moins un certificat CA doit correspondre. Pour plus d'informations, consultez la page **Gestion des certificats**.

Utilisez **Ajouter un certificat CA de serveur** pour ajouter des entrées et supprimez-les avec l'action de suppression.

20.11. Correspondances de suffixe de domaine

Liste de contraintes pour le nom de domaine du serveur. Les entrées sont utilisées comme exigences de correspondance de suffixe par rapport aux noms DNS du nom de sujet alternatif d'un certificat de serveur d'authentification.

Revision #6
Created 2026-11-10 15:15:34 UTC by Admin
Updated 2026-11-12 09:55:10 UTC by Admin