Réseau

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

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

État de la radio de l'appareil

1. État du Wi-Fi

Contrôle de l'état actuel du Wi-Fi et de la possibilité pour l'utilisateur de le modifier.

Choix de l'utilisateur (par défaut): L'utilisateur peut activer ou désactiver le Wi-Fi.

Activé : Le Wi-Fi est activé et l'utilisateur n'est pas autorisé à le désactiver (Android 13 et versions ultérieures).

Désactivé : Le Wi-Fi est désactivé et l'utilisateur n'est pas autorisé à le réactiver (Android 13 et versions ultérieures).

2. Niveau de sécurité Wi-Fi minimum

Le niveau de sécurité Wi-Fi minimum requis pour les réseaux auxquels l'appareil peut se connecter. Supporté sur 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 publics ; requiert au moins une sécurité de niveau personnel (par exemple, WPA2-PSK).

Réseau d'entreprise : Nécessite des réseaux EAP d'entreprise ; interdit les réseaux Wi-Fi ayant un niveau de sécurité inférieur.

Réseau d'entreprise 192 bits : Nécessite des réseaux d'entreprise 192 bits ; option la plus sécurisée.

3. État de la technologie à très large bande (UWB)

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

Choix utilisateur (par défaut): L'utilisateur peut activer ou désactiver UWB.

Désactivé : UWB est désactivé et l'utilisateur ne peut pas le réactiver via les paramètres (Android 14 et versions ultérieures).

Gestion de la connectivité des appareils

4. Partage via Bluetooth

Activez ou désactivez le partage via Bluetooth.

Autorisé : Le partage via Bluetooth est autorisé (par défaut sur les appareils entièrement gérés, Android 8 et versions ultérieures).

Non autorisé : Le partage via Bluetooth est désactivé (par défaut pour les profils d'entreprise, Android 8 et versions ultérieures).

5. Configurez le Wi-Fi

Contrôle des privilèges de configuration Wi-Fi. Selon l'option sélectionnée, l'utilisateur dispose d'un contrôle total, limité ou inexistant 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 et versions ultérieures ; profils professionnels gérés et appartenant à l'entreprise).

Interdire la configuration du Wi-Fi : Empêche la configuration de réseaux Wi-Fi. Pour les appareils entièrement gérés, cela supprime les réseaux configurés par l'utilisateur et conserve uniquement les réseaux configurés via **les configurations Wi-Fi**. Pour les profils

professionnels d'entreprise, les réseaux existants ne sont pas affectés, mais les utilisateurs ne peuvent pas ajouter, supprimer ou modifier les réseaux Wi-Fi.

> Lorsque la configuration Wi-Fi est désactivée et que l'appareil ne peut pas se connecter au démarrage, le système peut afficher la **fonction de contournement réseau** pour permettre à l'utilisateur de se connecter temporairement et de rafraîchir la configuration.

6. Paramètres de la connexion Wi-Fi Direct

Paramètres de configuration et d'utilisation de la connexion Wi-Fi Direct. Supporté sur les appareils appartenant à l'entreprise et fonctionnant sous Android 13 et versions ultérieures.

Autoriser (par défaut) : L'utilisateur est autorisé à utiliser la connexion Wi-Fi Direct.

Interdire : L'utilisateur n'est pas autorisé à utiliser la connexion Wi-Fi Direct.

7. Paramètres du partage de connexion

Contrôle les paramètres du partage de connexion. En fonction de la valeur définie, l'utilisateur peut être partiellement ou totalement empêché d'utiliser différentes formes de partage de connexion.

Autoriser toutes les options de partage de connexion (par défaut) : Permet la configuration et l'utilisation de toutes les formes de partage de connexion.

Interdire le partage de connexion Wi-Fi : Empêche l'utilisateur d'utiliser le partage de connexion Wi-Fi (appareils Android 13 et versions ultérieures appartenant à l'entreprise).

Interdire tout le partage de connexion : Empêche toutes les formes de partage de connexion (appareils entièrement gérés et profils professionnels appartenant à l'entreprise).

8. Politique du 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). Disponible sur les appareils appartenant à l'entreprise et exécutant Android 13 et versions ultérieures.

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

Liste blanche des SSID : L'appareil ne peut se connecter qu'aux réseaux Wi-Fi dont le SSID figure dans cette liste. La liste des SSID ne doit pas être vide.

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

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 interdits** pour les listes de blocage.

9. Paramètres de compatibilité Wi?Fi

Configurez le mode de compatibilité Wi-Fi par SSID. Utilisez **Ajouter un paramètre de compatibilité Wi-Fi** pour créer des entrées.

Chaque entrée comprend :

> **SSID** : L'identifiant SSID auquel s'applique le paramètre de roaming (obligatoire).
>
> **Mode de roaming Wi-Fi** : Par défaut / Désactivé / Adaptatif. Les modes Désactivé et Adaptatif nécessitent Android 15 et ne sont pris en charge que sur les appareils entièrement gérés et les profils d'entreprise sur les appareils appartenant à l'entreprise.

Restrictions réseau

Bluetooth désactivé

Le Bluetooth est-il désactivé ? (Privilégiez ce paramètre plutôt que "Configuration Bluetooth désactivée", car cette dernière peut être contournée par l'utilisateur).

11. Le partage de contacts via Bluetooth est désactivé

Que le partage de contacts via Bluetooth est désactivé.

12. La configuration Bluetooth est désactivée

Que la configuration Bluetooth est désactivée.

13. Réinitialisation du réseau désactivée

Que la réinitialisation des paramètres réseau est désactivée.

14. Transmission en flux désactivée

L'utilisation de la technologie NFC pour transmettre des données depuis les applications est désactivée.

VPN

Application VPN toujours activée

Spécifiez un nom de package VPN permanent pour vous assurer que les données des applications gérées spécifiées transitent toujours par un VPN configuré.

> Note : Cette fonctionnalité nécessite le déploiement d'un client VPN prenant en charge à la fois les fonctionnalités VPN permanentes et VPN par application.

16. Blocage VPN

Empêche l'accès au réseau lorsque le VPN n'est pas connecté.

17. Configuration VPN désactivée

Que la configuration VPN soit désactivée.

Services proxy et réseau

18. Service réseau prioritaire

Activez ou désactivez le service réseau prioritaire sur le profil professionnel. Par exemple, une entreprise peut avoir un accord avec un opérateur qui prévoit que les données professionnelles sont envoyées via un service réseau dédié aux entreprises (par exemple, une tranche réservée aux entreprises sur les réseaux 5G). Cela n'a aucun effet sur les appareils entièrement gérés.

Désactivé : Le service réseau prioritaire est désactivé sur le profil professionnel.

Activé : Le service réseau prioritaire est activé sur le profil professionnel.

> Si vous utilisez le découpage de réseau entreprise, configurez également **Configuration du découpage réseau 5G** dans le panneau de la politique **Cellulaire** et attribuez des applications à un segment en utilisant leur paramètre **Réseau Prioritaire**.

19. Proxy global recommandé

Le proxy HTTP global indépendant du réseau. En général, les proxies doivent être configurés pour chaque réseau dans les paramètres WiFi. Un proxy global peut être utile pour des configurations inhabituelles, comme le 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, ce sont les hôtes pour lesquels le proxy est contourné. Les noms d'hôtes 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 réseau Wi-Fi que le système appliquera aux 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.

Nom du réseau : Obligatoire.

Connexion automatique : Indique si le réseau doit se connecter automatiquement lorsque vous êtes dans sa portée.

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

SSID masqué : Indique si le SSID doit être diffusé.

Mode de randomisation de l'adresse MAC : Matériel ou Automatique (Android 13 et versions ultérieures).

20.1. Sécurité

Options de sécurité Wi-Fi :

WEP-PSK : WEP (clé prépartagée).

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

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

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

20.2. Phrase de passe (clé pré-partagée)

Affiché lorsque la sécurité est **WEP-PSK** ou **WPA-PSK**. La phrase de passe est requise.

20.3. Méthode EAP (Entreprise)

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

EAP-TLS

EAP-TTLS

PEAP

EAP-SIM

EAP-AKA

20.4. Authentification, phase 2

Affiché pour le tunneling des méthodes externes (**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 aux appareils, par utilisateur. Vous pouvez configurer les identifiants utilisateur 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 **Modifier le certificat** pour en sélectionner un autre.

Alternativement, vous pouvez spécifier **l'alias de la paire de clés du certificat client**, qui fait référence à un certificat client stocké dans le trousseau Android et autorisé pour l'authentification Wi-Fi.

> Si le **certificat client** et l'alias de la paire de clés du **certificat client** sont spécifiés, l'alias de la paire de clés est ignoré.

20.7. Identité

Identité de l'utilisateur. Pour le tunneling des protocoles externes (PEAP, EAP-TTLS), ceci est utilisé pour l'authentification à l'intérieur du tunnel, et **l'identité anonyme** est utilisée pour l'identité EAP à l'extérieur du tunnel. Pour les protocoles externes non utilisant le tunneling, ceci est utilisé pour l'identité EAP.

20.8. Identité anonyme

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

20.9. Mot de passe

Mot de passe de l'utilisateur. Si non spécifié, le système invite l'utilisateur à le saisir.

20.10. Certificats CA du serveur

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

Utilisez **l'option Ajouter le certificat CA du serveur** pour ajouter des entrées et les supprimer à l'aide de l'action supprimer.

20.11. Le suffixe de domaine correspond

Une liste de contraintes pour le nom de domaine du serveur. Ces entrées sont utilisées comme exigences de correspondance de suffixe par rapport au(x) nom(s) DNS du nom de sujet alternatif d'un certificat de serveur d'authentification.

Revision #38
Created 2025-12-17 09:33:37 UTC by Admin
Updated 2026-06-23 17:14:41 UTC by Admin