Réseautage

Dans cette section, vous pouvez configurer les politiques relatives au réseautage.

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

État de la radio de l'appareil

1. État du Wi-Fi

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

Le niveau de sécurité minimal requis des réseaux Wi-Fi auxquels l'appareil peut se connecter. Pris en charge sur Android 13 et versions ultérieures, pour les appareils en gestion complète 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 ; nécessite au moins une sécurité de type personnel (par exemple WPA2-PSK).

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

Réseau d'entreprise 192 bits : Nécessite des réseaux d'entreprise 192 bits ; l'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 en gestion complète, 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 config. Wi-Fi : L'ajout de nouvelles configurations Wi-Fi est interdit. L'utilisateur peut basculer entre les réseaux déjà configurés (Android 13+ ; appareils en

gestion complète et profils professionnels sur appareils appartenant à l'entreprise).

Interdire la configuration du Wi-Fi : Interdit la configuration des réseaux Wi-Fi. Pour les appareils en gestion complète, cela supprime les réseaux configurés par l'utilisateur et ne conserve que les réseaux configurés via les **configurations Wi-Fi**. Pour les profils professionnels sur appareils appartenant à l'entreprise, les réseaux existants ne sont pas affectés, mais les utilisateurs ne peuvent ni ajouter, ni supprimer, ni 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 la **soupape de sécurité réseau** pour permettre à l'utilisateur de se connecter temporairement et d'actualiser la politique.

6. Paramètres 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 de différentes formes de partage de connexion.

Autoriser tout le 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+ appartenant à l'entreprise).

Interdire tout le partage de connexion : empêche toutes les formes de partage de connexion (gestion complète + profils de travail appartenant à l'entreprise).

8. Politique de SSID Wi-Fi

Restrictions sur les SSID Wi-Fi auxquels l'appareil peut se connecter (cela n'affecte pas les réseaux pouvant être configurés sur l'appareil). Pris en charge sur les appareils appartenant à l'entreprise

fonctionnant sous Android 13 et versions ultérieures.

Liste d'exclusion de SSID (par défaut) : l'appareil ne peut se connecter à aucun réseau Wi-Fi dont le SSID est répertorié, mais peut se connecter aux autres réseaux.

Liste d'autorisation de 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 politique sélectionné, la liste est interprétée comme des SSID autorisés ou refusés.

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

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 s'applique le paramètre d'itinérance (requis).

Mode d'itinérance Wi-Fi : Par défaut / Désactivé / Agressif. Les modes Désactivé et Agressif nécessitent Android 15+ et sont pris en charge uniquement sur les appareils en gestion complète ainsi que sur les profils de travail des appareils appartenant à l'entreprise.

Restrictions réseau

10. Désactivation du Bluetooth

Indique si le Bluetooth est désactivé. Privilégiez ce paramètre par rapport à la désactivation de la configuration Bluetooth, car cette dernière peut être contournée par l'utilisateur.

11. Désactivation du partage de contacts via Bluetooth

Indique si le partage de contacts via Bluetooth est désactivé.

12. Désactivation de la configuration Bluetooth

Indique si la configuration du Bluetooth est désactivée.

13. Désactivation de la réinitialisation du réseau

Indique si la réinitialisation des paramètres réseau est désactivée.

14. Désactivation du partage par Android Beam (sortant)

Indique si l'utilisation du NFC pour le partage de données via Beam est désactivée.

VPN

15. Application VPN toujours activé (Always On)

Spécifiez le nom du package de l'application VPN toujours activé (Always On) pour garantir que les données des applications gérées spécifiées passeront toujours par un VPN configuré.

> Remarque : Cette fonctionnalité nécessite le déploiement d'un client VPN prenant en charge à la fois les fonctions « Always On » (toujours activé) et le VPN par application.

16. Verrouillage VPN (VPN lockdown)

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

17. Désactivation de la configuration VPN

Indique si la configuration du VPN est désactivée.

Proxy et services réseau

18. Service de réseau préférentiel

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

Désactivé : le service de réseau préférentiel est désactivé sur le profil de travail.

Activé : le service de réseau préférentiel est activé sur le profil de travail.

> Si vous utilisez le découpage de réseau (network slicing) d'entreprise, configurez également la **Configuration du découpage de réseau 5G** dans le panneau de politique **Réseau cellulaire** et assignez les applications à une tranche en utilisant leur paramètre **Réseau préférentiel**.

19. Proxy global recommandé

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

Désactivé

Proxy direct

Proxy auto-config (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'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 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 : Requis.

SSID : Requis.

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

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

SSID caché : indique si le SSID sera diffusé.

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

20.1. Sécurité

Options de sécurité Wi-Fi :

WEP-PSK : WEP (clé pré-partagée).

WPA-PSK : WPA/WPA2/WPA3-Personnel (clé pré-partagée).

WPA-EAP : WPA/WPA2/WPA3-Entreprise (Extensible Authentication Protocol).

Mode WPA3 192 bits : réseau WPA-EAP n'autorisant que le mode WPA3 192 bits.

20.2. Mot de passe (clé pré-partagée)

Affiché lorsque la sécurité est **WEP-PSK** ou **WPA-PSK**. Le mot de passe est requis.

20.3. Méthode EAP (Entreprise)

Affiché lorsque la sécurité est **WPA-EAP** ou **Mode WPA3 192 bits**. 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 à tunnel (**EAP-TTLS** et **PEAP**).

MSCHAPv2

PAP

20.5. Identifiants EAP des utilisateurs

Lorsqu'elle 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 assigner un certificat client utilisé pour l'authentification Wi-Fi. Pour plus d'informations, consultez la page **Gestion des certificats**.

Si un certificat est déjà assigné, 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 tous deux configurés, l'alias de la paire de clés est ignoré.

20.7. Identité

Identité de l'utilisateur. Pour les protocoles externes à tunnel (PEAP, EAP-TTLS), celle-ci est utilisée 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 sans tunnel, elle est utilisée pour l'identité EAP.

20.8. Identité anonyme

Pour les protocoles à tunnel uniquement, cela 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 d'autorité de certification (CA) du serveur

Liste des certificats d'autorité de certification (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 d'autorité de certification (CA) du serveur** pour ajouter des entrées et supprimez-les avec l'action de suppression.

20.11. Correspondances de suffixes de domaine

Une liste de contraintes pour le nom de domaine du serveur. Les 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 #6
Created 2026-06-24 08:07:56 UTC by Admin
Updated 2026-06-24 09:42:23 UTC by Admin