الشبكات

في هذا القسم، يمكنك تكوين السياسات المتعلقة بالشبكات.

> يمكن توفير تكوينات Wi-Fi وإدارتها بواسطة النظام عبر **تكوينات WiFi**. وفقًا للقيمة المعيّنة في **تكوين Wi-Fi**، قد يمتلك المستخدمون تحكمًا محدودًا أو لا تحكم في إضافة الشبكات/تعديلها.

حالة راديو الجهاز

1. حالة Wi-Fi

يتحكم في الحالة الحالية لـ Wi-Fi وما إذا كان يمكن للمستخدم تغيير حالتها.

اختيار المستخدم (الافتراضي): يُسمح للمستخدم بتمكين/تعطيل Wi-Fi.

مفعّل: Wi-Fi قيد التشغيل ولا يُسمح للمستخدم بإيقافها (Android 13+).

معطّل: Wi-Fi متوقفة ولا يُسمح للمستخدم بتشغيلها (Android 13+).

2. الحد الأدنى لمستوى أمان Wi-Fi

الحد الأدنى المطلوب لمستوى أمان شبكات Wi-Fi التي يمكن للجهاز الاتصال بها. مدعوم على Android 13 فما فوق، للأجهزة المُدارة بالكامل وملفات تعريف العمل على الأجهزة المملوكة للشركة.

شبكة مفتوحة (الافتراضي): يمكن للجهاز الاتصال بجميع أنواع شبكات Wi-Fi.

شبكة شخصية: تمنع شبكات Wi-Fi المفتوحة؛ تتطلب أمانًا شخصيًا على الأقل (على سبيل المثال WPA2-PSK).

شبكة مؤسسة: تتطلب شبكات EAP للمؤسسات؛ تمنع شبكات Wi-Fi الأقل من مستوى الأمان هذا.

شبكة مؤسسة 192-بت: تتطلب شبكات مؤسسة 192-بت؛ الخيار الأكثر صرامة.

3. حالة النطاق العريض الفائق (UWB)

يتحكم في حالة إعداد النطاق العريض الفائق وما إذا كان يمكن للمستخدم تبديله تشغيلاً وإيقافاً.

اختيار المستخدم (الافتراضي): يُسمح للمستخدم بتبديل UWB تشغيلاً وإيقافاً.

معطّل: UWB معطّل ولا يُسمح للمستخدم بتبديله عبر الإعدادات (Android 14+).

إدارة اتصال الجهاز

4. مشاركة Bluetooth

يتحكم في ما إذا كانت مشاركة Bluetooth مسموحة.

مسموح: مشاركة Bluetooth مسموحة (الافتراضي على الأجهزة المُدارة بالكامل، Android 8+).

غير مسموح: مشاركة Bluetooth غير مسموحة (الافتراضي على ملفات تعريف العمل، Android 8+).

5. تكوين Wi-Fi

يتحكم في صلاحيات تكوين Wi-Fi. وفقاً للخيار المحدد، يمتلك المستخدم تحكماً كاملاً أو محدوداً أو لا تحكم في تكوين شبكات Wi-Fi.

السماح بتكوين Wi-Fi (الافتراضي): يُسمح للمستخدم بتكوين Wi-Fi.

عدم السماح بإضافة تكوين Wi-Fi: إضافة تكوينات Wi-Fi جديدة غير مسموحة. يمكن للمستخدم التبديل بين الشبكات المكوّنة بالفعل (Android 13+؛ الأجهزة المُدارة بالكامل وملفات تعريف العمل المملوكة للشركة).

عدم السماح بتكوين Wi-Fi: يمنع تكوين شبكات Wi-Fi. بالنسبة للأجهزة المُدارة بالكامل، يزيل هذا الشبكات التي كوّنها المستخدم ويحتفظ فقط بالشبكات المكوّنة عبر **تكوينات WiFi**. بالنسبة لملفات تعريف العمل المملوكة للشركة، لا تتأثر الشبكات الحالية لكن لا يمكن للمستخدمين إضافة شبكات Wi-Fi أو إزالتها أو تعديلها.

عند تعطيل تكوين Wi-Fi والسماح للجهاز بالاتصال وقت بدء التشغيل، يمكن للنظام عرض **مخرج الشبكة البديل** لتمكين المستخدم من الاتصال مؤقتاً وتحديث السياسة.

6. إعدادات Wi-Fi Direct

يتحكم في تكوين إعدادات Wi-Fi Direct واستخدامها. مدعوم على الأجهزة المملوكة للشركة التي تعمل بنظام Android 13 فما فوق.

السماح (الافتراضي): يُسمح للمستخدم باستخدام Wi-Fi Direct.

عدم السماح: لا يُسمح للمستخدم باستخدام Wi-Fi Direct.

7. إعدادات المشاركة عبر نقطة الاتصال

يتحكم في إعدادات المشاركة عبر نقطة الاتصال. بناءً على القيمة المعيّنة، يُمنع المستخدم جزئياً أو كلياً من استخدام أشكال مختلفة من المشاركة عبر نقطة الاتصال.

السماح بجميع أشكال المشاركة عبر نقطة الاتصال (الافتراضي): يسمح بتكوين واستخدام جميع أشكال المشاركة عبر نقطة الاتصال.

عدم السماح بالمشاركة عبر نقطة اتصال Wi-Fi: يمنع المستخدم من استخدام المشاركة عبر نقطة اتصال Wi-Fi (الأجهزة المملوكة للشركة على Android 13+).

عدم السماح بجميع أشكال المشاركة عبر نقطة الاتصال: يمنع جميع أشكال المشاركة عبر نقطة الاتصال (الأجهزة المُدارة بالكامل + ملفات تعريف العمل المملوكة للشركة).

8. سياسة SSID لـ Wi-Fi

قيود على معرّفات SSID لـ Wi-Fi التي يمكن للجهاز الاتصال بها (لا يؤثر هذا في الشبكات التي يمكن تكوينها على الجهاز). مدعوم على الأجهزة المملوكة للشركة التي تعمل بنظام Android 13 فما فوق.

قائمة حظر SSID (الافتراضي): لا يمكن للجهاز الاتصال بأي شبكة Wi-Fi مدرج معرّف SSID الخاص بها، لكن يمكنه الاتصال بشبكات أخرى.

قائمة سماح SSID: يمكن للجهاز الاتصال بمعرّفات SSID المدرجة فقط. يجب ألا تكون قائمة SSID فارغة.

استخدم **إضافة SSID** لإضافة إدخالات. وفقًا لنوع السياسة المحدد، تُفسّر القائمة على أنها معرّفات SSID مسموحة أو محظورة.

في واجهة محرر السياسات، تُسمّى قائمة SSID **معرّفات SSID المسموحة لـ Wi-Fi** لقوائم السماح و**معرّفات SSID المحظورة لـ Wi-Fi** لقوائم الحظر.

9. إعدادات تجوال Wi-Fi

كوّن وضع تجوال Wi-Fi لكل SSID. استخدم **إضافة إعداد تجوال Wi-Fi** لإنشاء إدخالات.

يتضمن كل إدخال:

> **SSID**: معرّف SSID الذي ينطبق عليه إعداد التجوال (مطلوب).
>
> **وضع تجوال Wi-Fi**: الافتراضي / معطّل / عدواني. يتطلب المعطّل والعدواني Android 15+ وهما مدعومان فقط على الأجهزة المُدارة بالكامل وملفات تعريف العمل على الأجهزة المملوكة للشركة.

قيود الشبكة

10. Bluetooth معطّل

ما إذا كان Bluetooth معطّلًا. فضّل هذا الإعداد على خيار تكوين Bluetooth معطّل لأن المستخدم يمكنه تجاوز خيار تكوين Bluetooth معطّل.

11. مشاركة جهات الاتصال عبر Bluetooth معطّلة

ما إذا كانت مشاركة جهات الاتصال عبر Bluetooth معطّلة.

12. تكوين Bluetooth معطّل

ما إذا كان تكوين Bluetooth معطّلًا.

13. إعادة تعيين الشبكة معطّلة

ما إذا كانت إعادة تعيين إعدادات الشبكة معطّلة.

14. البث الصادر معطّل

ما إذا كان استخدام NFC لبث البيانات من التطبيقات معطّلاً.

VPN

15. تطبيق Always On VPN

حدد اسم حزمة Always On VPN لضمان أن بيانات التطبيقات المُدارة المحددة ستمر دائماً عبر VPN مكوّن.

> ملاحظة: تتطلب هذه الميزة نشر عميل VPN يدعم ميزتي Always On وVPN لكل تطبيق.

16. قفل VPN

يمنع الشبكات عندما لا يكون VPN متصلاً.

17. تكوين VPN معطّل

ما إذا كان تكوين VPN معطّلاً.

الوكيل وخدمات الشبكة

18. خدمة الشبكة التفضيلية

يتحكم في ما إذا كانت خدمة الشبكة التفضيلية ممكّنة على ملف تعريف العمل. على سبيل المثال، قد تكون لدى المؤسسة اتفاقية مع مشغّل شبكة تُرسَل بموجبها بيانات العمل عبر خدمة شبكة مخصّصة لاستخدام المؤسسات (على سبيل المثال، شريحة مؤسسة على شبكات

5G). ليس لهذا أي تأثير على الأجهزة المُدارة بالكامل.

معطّل: خدمة الشبكة التفضيلية معطّلة على ملف تعريف العمل.

مفعّل: خدمة الشبكة التفضيلية ممكّنة على ملف تعريف العمل.

> إذا كنت تستخدم تقسيم شبكة المؤسسات، فكوّن أيضاً **تكوين تقسيم شبكة 5G** ضمن لوحة سياسة **الشبكة الخلوية** وعيّن التطبيقات إلى شريحة باستخدام إعداد **الشبكة التفضيلية** الخاص بها.

19. الوكيل العام الموصى به

وكيل HTTP العام المستقل عن الشبكة. عادةً، ينبغي تكوين الوكلاء لكل شبكة في تكوينات WiFi. قد يكون الوكيل العام مفيداً للتكوينات غير المعتادة مثل التصفية الداخلية العامة. الوكيل العام مجرد توصية وقد تتجاهله بعض التطبيقات.

معطّل

الوكيل المباشر

التهيئة التلقائية للوكيل (PAC)

19.1. المضيف

مضيف الوكيل المباشر.

19.2. المنفذ

منفذ الوكيل المباشر.

19.3. عنوان URI لـ PAC

عنوان URI لنص PAC المستخدم لتهيئة الوكيل.

19.4. المضيفون المستثنون

في الوكيل المباشر، المضيفون الذين يتم تجاوز الوكيل لهم. قد تحتوي أسماء المضيفين على أحرف بدل مثل ***.example.com**.

استخدم **إضافة مضيف مستثنى** لإضافة إدخالات (متاح للوكيل المباشر فقط).

تهيئات Wi-Fi

حدّد تهيئات شبكات Wi-Fi التي سيطبّقها النظام على الأجهزة. استخدم **إضافة تهيئة Wi-Fi** لإنشاء إدخال، وأزله باستخدام إجراء الحذف.

20. حقول تهيئة Wi-Fi

تتضمن كل تهيئة:

اسم التهيئة: مطلوب.

SSID: مطلوب.

الاتصال التلقائي: ما إذا كان يجب الاتصال بالشبكة تلقائيًا عند توفرها.

الانتقال السريع: ما إذا كان يجب على العميل محاولة استخدام الانتقال السريع (IEEE 802.11r-2008) مع الشبكة.

SSID مخفي: ما إذا كان سيتم بث SSID.

وضع عشوائية MAC: الأجهزة أو تلقائي (Android 13+).

20.1. الأمان

خيارات أمان Wi-Fi:

WEP-PSK: WEP (مفتاح مشترك مسبقًا).

WPA-PSK: WPA/WPA2/WPA3-Personal (مفتاح مشترك مسبقًا).

WPA-EAP: WPA/WPA2/WPA3-Enterprise (بروتوكول المصادقة القابل للتوسيع).

وضع WPA3 192 بت: شبكة WPA-EAP تسمح بوضع WPA3 192 بت فقط.

20.2. عبارة المرور (المفتاح المشترك مسبقًا)

يظهر عندما يكون الأمان **WEP-PSK** أو **WPA-PSK**. عبارة المرور مطلوبة.

20.3. طريقة EAP (المؤسسة)

يظهر عندما يكون الأمان **WPA-EAP** أو **وضع WPA3 192 بت**. اختر طريقة EAP خارجية واحدة:

EAP-TLS

EAP-TTLS

PEAP

EAP-SIM

EAP-AKA

20.4. مصادقة المرحلة 2

يظهر لطرق النفق الخارجية (**EAP-TTLS** و**PEAP**).

MSCHAPv2

PAP

20.5. بيانات اعتماد EAP من المستخدمين

عند التمكين، يطبّق النظام بيانات اعتماد EAP على الأجهزة تلقائيًا لكل مستخدم. يمكنك تهيئة بيانات اعتماد المستخدمين في قسم **المستخدمون**.

20.6. شهادة العميل

بالنسبة إلى **EAP-TLS**، يمكنك تعيين شهادة عميل تُستخدم لمصادقة Wi-Fi. لمزيد من المعلومات، راجع صفحة **إدارة الشهادات**.

إذا كانت هناك شهادة معيّنة بالفعل، يمكنك استخدام **فتح الشهادة** لعرضها أو **تغيير الشهادة** لتحديد شهادة أخرى.

بدلًا من ذلك، يمكنك تحديد **الاسم المستعار لزوج مفاتيح شهادة العميل**، والذي يشير إلى شهادة عميل مخزّنة في سلسلة مفاتيح Android ومسموح بها لمصادقة Wi-Fi.

> إذا تم تعيين كل من **شهادة العميل** و**الاسم المستعار لزوج مفاتيح شهادة العميل**، يتم تجاهل الاسم المستعار لزوج المفاتيح.

20.7. الهوية

هوية المستخدم. بالنسبة إلى البروتوكولات الخارجية النفقية (PEAP، EAP-TTLS)، تُستخدم هذه للمصادقة داخل النفق، وتُستخدم **الهوية المجهولة** لهوية EAP خارج النفق. أما بالنسبة إلى البروتوكولات الخارجية غير النفقية، فتُستخدم هذه لهوية EAP.

20.8. الهوية المجهولة

للبروتوكولات النفقية فقط، يشير هذا إلى هوية المستخدم المعروضة على البروتوكول الخارجي.

20.9. كلمة المرور

كلمة مرور المستخدم. إذا لم تُحدّد، يكون الافتراضي هو مطالبة المستخدم.

20.10. شهادات CA للخادم

قائمة شهادات CA المستخدمة للتحقق من سلسلة شهادات المضيف. يجب أن تتطابق شهادة CA واحدة على الأقل. لمزيد من المعلومات، راجع صفحة **إدارة الشهادات**.

استخدم **إضافة شهادة CA للخادم** لإضافة إدخالات، وأزلها باستخدام إجراء الحذف.

20.11. مطابقات لاحقة النطاق

قائمة بقيود اسم نطاق الخادم. تُستخدم الإدخالات كمطالبات مطابقة اللاحقة مقابل اسم (أسماء) DNS للاسم الموضوعي البديل لشهادة خادم المصادقة.

Revision #7
Created 2026-11-10 15:13:40 UTC by Admin
Updated 2026-11-12 09:53:15 UTC by Admin