الشبكات (Networking)

في هذا القسم، يمكنك تكوين السياسات المتعلقة بالشبكات.

> يمكن توفير وإدارة تكوينات Wi-Fi بواسطة النظام عبر **تكوينات WiFi**. وبناءً على القيمة المحددة في **تكوين Wi-Fi**، قد يكون للمستخدمين تحكم محدود أو لا يوجد تحكم على الإطلاق في إضافة/تعديل الشبكات.

حالة راديو الجهاز (Device radio state)

١. حالة Wi-Fi

يتحكم في الحالة الحالية لـ Wi-Fi وما إذا كان بإمكان المستخدم تغيير حالتها.

خيار المستخدم (الافتراضي): يُسمح للمستخدم بتفعيل أو تعطيل Wi-Fi.

مُفعّل: يكون Wi-Fi مفعلاً ولا يُسمح للمستخدم بإيقاف تشغيله (في إصدار Android 13 فما فوق).

معطل: يكون Wi-Fi معطلاً ولا يُسمح للمستخدم بتشغيله (في إصدار Android 13 فما فوق).

٢. الحد الأدنى لمستوى أمان Wi-Fi

الحد الأدنى لمستوى أمان شبكات Wi-Fi التي يمكن للجهاز الاتصال بها. مدعوم في إصدار Android 13 وما فوق، للأجهزة المدارة بالكامل وملفات العمل على الأجهزة المملوكة للشركة.

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

شبكة شخصية: يمنع شبكات Wi-Fi المفتوحة؛ ويتطلب أمانًا شخصيًا على الأقل (مثل WPA2-PSK).

شبكة المؤسسة: يتطلب شبكات EAP الخاصة بالمؤسسة؛ ويمنع شبكات Wi-Fi التي تقل عن هذا المستوى من الأمان.

شبكة مؤسسة 192 بت: يتطلب شبكات مؤسسة 192 بت؛ وهو الخيار الأكثر صرامة.

٣. حالة النطاق فائق العرض (UWB)

يتحكم في حالة إعداد النطاق فائق العرض (UWB) وما إذا كان بإمكان المستخدم تفعيلها أو إيقاف تشغيلها.

خيار المستخدم (الافتراضي): يُسمح للمستخدم بتفعيل أو إيقاف تشغيل UWB.

معطل: يتم تعطيل UWB ولا يُسمح للمستخدم بتفعيلها عبر الإعدادات (في إصدار Android 14 فما فوق).

إدارة اتصال الجهاز

٤. مشاركة البلوتوث (Bluetooth)

يتحكم في ما إذا كان يُسمح بمشاركة البلوتوث.

مسموح: يُسمح بمشاركة البلوتوث (الوضع الافتراضي في الأجهزة المدارة بالكامل، إصدار Android 8 فما فوق).

غير مسموح: يُمنع مشاركة البلوتوث (الوضع الافتراضي في ملفات العمل، إصدار Android 8 فما فوق).

٥. تكوين Wi-Fi

يتحكم في صلاحيات تكوين Wi-Fi. وبناءً على الخيار المحدد، سيكون للمستخدم تحكم كامل أو محدود أو لا يوجد تحكم في تكوين شبكات Wi-Fi.

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

منع إضافة تكوين Wi-Fi: يُمنع إضافة تكوينات Wi-Fi جديدة. يمكن للمستخدم التبديل بين الشبكات المكوّنة مسبقاً (في إصدار Android 13 فما فوق؛ وفي الأجهزة المدارة بالكامل وملفات العمل المملوكة للشركة).

منع تكوين Wi-Fi: يمنع تكوين شبكات Wi-Fi. بالنسبة للأجهزة المدارة بالكامل، يؤدي هذا إلى إزالة الشبكات التي قام المستخدم بتكوينها والاحتفاظ فقط بالشبكات المكوّنة عبر **تكوينات WiFi**. أما بالنسبة لملفات العمل المملوكة للشركة، فلن تتأثر الشبكات الموجودة ولكن لن يتمكن المستخدمون من إضافة/إزالة/تعديل شبكات Wi-Fi.

> عندما يكون تكوين Wi-Fi معطلاً، لا يستطيع الجهاز الاتصال عند وقت بدء التشغيل، يمكن للنظام إظهار **مخرج الهروب من الشبكة** للسماح للمستخدم بالاتصال مؤقتاً وتحديث السياسة.

٦. إعدادات Wi-Fi Direct

يتحكم في تكوين واستخدام إعدادات Wi-Fi Direct. مدعوم على الأجهزة المملوكة للشركة التي تعمل بإصدار Android 13 وما فوق.

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

غير مسموح: لا يُسمح للمستخدم باستخدام Wi-Fi Direct.

٧. إعدادات ربط نقطة الاتصال (Tethering)

يتحكم في إعدادات ربط نقطة الاتصال (Tethering). وبناءً على القيمة المحددة، يتم منع المستخدم جزئياً أو كلياً من استخدام أشكال مختلفة من ربط نقطة الاتصال.

السماح بجميع أنواع ربط نقطة الاتصال (الافتراضي): يسمح بتكوين واستخدام جميع أشكال ربط نقطة الاتصال.

منع ربط نقطة الاتصال عبر Wi-Fi: يمنع المستخدم من استخدام ربط نقطة الاتصال عبر Wi-Fi (في الأجهزة المملوكة للشركة بنظام Android 13 فما فوق).

منع جميع أنواع ربط نقطة الاتصال: يمنع جميع أشكال ربط نقطة الاتصال (في الأجهزة المدارة بالكامل وملفات العمل المملوكة للشركة).

٨. سياسة معرف مجموعة الخدمات (SSID) لـ Wi-Fi

القيود المفروضة على معرفات SSID لشبكات Wi-Fi التي يمكن للجهاز الاتصال بها (لا يؤثر هذا على الشبكات التي يمكن تكوينها على الجهاز). مدعوم في الأجهزة المملوكة للشركة التي تعمل بإصدار Android 13 وما فوق.

قائمة حظر SSID (الافتراضي): لا يمكن للجهاز الاتصال بأي شبكة Wi-Fi مدرجة في القائمة، ولكن يمكنه الاتصال بالشبكات الأخرى.

قائمة السماح بـ SSID: يمكن للجهاز الاتصال فقط بمعرفات SSID المدرجة. يجب أن تكون قائمة SSID فارغة.

استخدم **إضافة SSID** لإضافة إدخالات. وبناءً على نوع السياسة المحددة، يتم تفسير القائمة كمعرفات SSID مسموح بها أو محظورة.

في واجهة مستخدم محرر السياسات، يتم تسمية قائمة SSID بـ **معرفات SSID المسموح بها لـ Wi-Fi** في قوائم السماح، وبـ **معرفات SSID المحظورة لـ Wi-Fi** في قوائم الحظر.

٩. إعدادات تجوال Wi-Fi

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

يتضمن كل إدخال ما يلي:

SSID: معرف مجموعة الخدمة (SSID) الذي ينطبق عليه إعداد التجوال (مطلوب).

وضع تجوال Wi-Fi: الافتراضي / معطل / عدواني. يتطلب الوضعان "معطل" و"عدواني" إصدار Android 15 أو أحدث، وهما مدعومان فقط في الأجهزة ذات الإدارة الكاملة وملفات تعريف العمل على الأجهزة المملوكة للشركة.

قيود الشبكة

10. تعطيل البلوتوث

ما إذا كان قد تم تعطيل البلوتوث. يُفضل استخدام هذا الإعداد بدلاً من "تعطيل تكوين البلوتوث" لأن المستخدم يمكنه تجاوز "تعطيل تكوين البلوتوث".

11. تعطيل مشاركة جهات الاتصال عبر البلوتوث

ما إذا كان قد تم تعطيل مشاركة جهات الاتصال عبر البلوتوث.

12. تعطيل تكوين البلوتوث

ام إذا كان قد تم تعطيل تكوين البلوتوث.

13. تعطيل إعادة ضبط الشبكة

ام إذا كان قد تم تعطيل إعادة ضبط إعدادات الشبكة.

14. تعطيل الإرسال عبر Android Beam

ام إذا كان قد تم تعطيل استخدام تقنية NFC لإرسال البيانات من التطبيقات.

VPN

15. تطبيق VPN المتصل دائماً

حدد اسم حزمة تطبيق VPN المتصل دائماً لضمان مرور البيانات من التطبيقات المدارة المحددة عبر شبكة VPN مهيأة دائماً.

> ملاحظة: تتطلب هذه الميزة نشر عميل VPN يدعم ميزتي "الاتصال الدائم" (Always On) و"VPN لكل تطبيق" (per-app VPN).

16. إغلاق الشبكة عند انقطاع الـ VPN

يمنع استخدام الشبكة عندما لا يكون الـ VPN متصلاً.

17. تعطيل تكوين الـ VPN

ام إذا كان قد تم تعطيل تكوين الـ VPN.

الوكيل وخدمات الشبكة

18. خدمة الشبكة المفضلة

يتحكم في ما إذا كانت خدمة الشبكة المفضلة مفعلة على ملف تعريف العمل. على سبيل المثال، قد يكون لدى المؤسسة اتفاقية مع شركة اتصالات تقضي بإرسال بيانات العمل عبر خدمة شبكة مخصصة لاستخدام الشركات (مثل شريحة المؤسسة على شبكات 5G). ليس لهذا الإعداد أي تأثير على الأجهزة ذات الإدارة الكاملة.

معطل: يتم تعطيل خدمة الشبكة المفضلة على ملف تعريف العمل.

مُفعّل: يتم تفعيل خدمة الشبكة المفضلة على ملف تعريف العمل.

> إذا كنت تستخدم تقنية تقسيم الشبكة للمؤسسات (network slicing)، فقم أيضاً بتهيئة **تكوين تقسيم شبكة 5G** ضمن لوحة سياسة **الشبكة الخلوية**، وقم بتعيين التطبيقات لشريحة معينة باستخدام إعداد **الشبكة المفضلة**.

19. الوكيل العالمي الموصى به

الوكيل العالمي لبروتوكول HTTP المستقل عن الشبكة. عادةً ما ينبغي تهيئة الوكلاء لكل شبكة على حدة في إعدادات Wi-Fi. قد يكون الوكيل العالمي مفيداً في حالات التهيئة غير المعتادة مثل التصفية الداخلية العامة. يُعد الوكيل العالمي مجرد توصية فقط، وقد تتجاهله بعض التطبيقات.

معطل

وكيل مباشر

التكوين التلقائي للوكيل (PAC)

19.1. المضيف

مضيف الوكيل المباشر.

19.2. المنفذ

منفذ الوكيل المباشر.

19.3. معرف PAC URI

معرف (URI) الخاص بنص PAC البرمجي المستخدم لتهيئة الوكيل.

19.4. المضيفون المستبعدون

بالنسبة للوكيل المباشر، هي المضيفات التي يتم تجاوز الوكيل من خلالها. قد تحتوي أسماء المضيفات على رموز بديلة مثل ***.example.com**.

استخدم **إضافة مضيف مستبعد** لإضافة المدخلات (متاح للوكيل المباشر فقط).

تكوينات Wi-Fi

حدد تكوينات شبكة Wi-Fi التي سيطبقها النظام على الأجهزة. استخدم **إضافة تكوين Wi-Fi** لإنشاء مدخل، وقم بإزالته باستخدام إجراء الحذف.

20. حقول تكوين Wi-Fi

يتضمن كل تكوين ما يلي:

اسم التكوين: مطلوب.

SSID: مطلوب.

الاتصال التلقائي: ما إذا كان ينبغي الاتصال بالشبكة تلقائياً عند توفرها في النطاق.

الانتقال السريع (Fast Transition): ما إذا كان ينبغي للعميل محاولة استخدام الانتقال السريع (IEEE 802.11r-2008) مع الشبكة.

SSID مخفي: ما إذا كان سيتم بث الـ SSID.

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

20.1. الأمان

خيارات أمان Wi-Fi:

WEP-PSK: WEP (مفتاح مشترك مسبقاً).

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

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

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

20.2. كلمة المرور (المفتاح المشترك مسبقاً)

تظهر عندما يكون الأمان مضبوطاً على **WEP-PSK** أو **WPA-PSK**. كلمة المرور مطلوبة.

20.3. طريقة EAP (للمؤسسات)

تظهر عندما يكون الأمان مضبوطاً على **WPA-EAP** أو **وضع WPA3 192-bit**. اختر طريقة EAP خارجية واحدة:

EAP-TLS

EAP-TTLS

PEAP

EAP-SIM

EAP-AKA

20.4. مصادقة المرحلة الثانية (Phase 2)

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

MSCHAPv2

PAP

20.5. بيانات اعتماد EAP من المستخدمين

عند تفعيل هذا الخيار، يقوم النظام تلقائياً بتطبيق بيانات اعتماد EAP على الأجهزة لكل مستخدم على حدة. يمكنك تهيئة بيانات اعتماد المستخدمين في قسم **المستخدمين**.

20.6. شهادة العميل

بالنسبة لـ **EAP-TLS**، يمكنك تعيين شهادة عميل تُستخدم للمصادقة عبر Wi-Fi. لمزيد من المعلومات، اقرأ صفحة **[إدارة الشهادات]**.

إذا تم تعيين شهادة بالفعل، يمكنك استخدام **فتح الشهادة** لعرضها أو **تغيير الشهادة** لاختيار شهادة أخرى.

بدلاً من ذلك، يمكنك تحديد **الاسم المستعار لزوج مفاتيح شهادة العميل**، والذي يشير إلى شهادة عميل مخزنة في سلسلة مفاتيح Android ومسموح بها للمصادقة عبر Wi-Fi.

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

20.7. الهوية

هوية المستخدم. بالنسبة لبروتوكولات النفق الخارجية (PEAP و EAP-TTLS)، تُستخدم هذه الهوية للمصادقة داخل النفق، بينما تُستخدم **الهوية المجهولة** لهوية EAP خارج النفق. أما بالنسبة للبروتوكولات الخارجية غير النفقية، فتُستخدم هذه الهوية لهوية EAP.

20.8. الهوية المجهولة

بالنسبة للبروتوكولات النفقية فقط، يشير هذا إلى هوية المستخدم المقدمة للبروتوكول الخارجي.

20.9. كلمة المرور

كلمة مرور المستخدم. إذا لم يتم تحديدها، فسيتم الاكتفاء بطلبها من المستخدم.

20.10. شهادات CA للخادم

قائمة بشهادات CA التي سيتم استخدامها للتحقق من سلسلة شهادات المضيف. يجب أن تطابق شهادة CA واحدة على الأقل. لمزيد من المعلومات، اقرأ صفحة **إدارة الشهادات**.

استخدم **إضافة شهادة CA للخادم** لإضافة المدخلات، وقم بإزالتها باستخدام إجراء الحذف.

20.11. تطابقات لاحقة النطاق (Domain suffix matches)

قائمة بالقيود الخاصة باسم نطاق الخادم. تُستخدم هذه المدخلات كمتطلبات لمطابقة اللاحقة مقابل اسم (أو أسماء) نظام أسماء النطاقات (DNS) للاسم البديل للموضوع في شهادة خادم المصادقة.

Revision #11
Created 2026-06-24 08:05:48 UTC by Admin
Updated 2026-07-07 10:52:57 UTC by Admin