تزويد الأجهزة - Android

- الأجهزة المدعومة
- رموز التسجيل
- الأجهزة المملوكة شخصيًا
- الأجهزة المملوكة للشركة للاستخدام المهني والشخصي
- الأجهزة المملوكة للشركة للاستخدام المهني فقط
- Zero-touch
- المصادقة باستخدام تسجيل Google

الأجهزة المدعومة

عموماً، أي جهاز يعمل بنظام Android 6 أو أحدث مع خدمات Google Play متوافق مع Cerberus Enterprise.

لتحسين تجربة المستخدم، نوصي باستخدام أجهزة تستوفي متطلبات Android Enterprise Recommended.

> تقتصر بعض الميزات على إصدارات Android معينة، أو قد تتصرف بشكل مختلف عبر إصدارات نظام التشغيل. لمزيد من المعلومات حول ميزة معينة، راجع قسم السياسات في الوثائق.

يدعم Cerberus Enterprise الأجهزة المملوكة للشركة والأجهزة المملوكة شخصياً، ووضعي إدارة: مالك الجهاز ومالك ملف التعريف.

الأجهزة المملوكة شخصياً يمكن إدارتها عبر **ملف تعريف العمل**. يتيح ذلك حل BYOD من خلال إبقاء بيانات العمل وتطبيقاته منفصلة عن البيانات والتطبيقات الشخصية، ما يحسّن الأمان والخصوصية معاً. يناسب هذا الخيار الأجهزة المملوكة بالفعل للموظفين والتي ترید تسجيلها في مؤسستك للاستخدام المهني.

الأجهزة المملوكة للشركة يمكن إدارتها أيضاً عبر ملف تعريف عمل، لكن يمكنك كذلك اختيار خيار **الإدارة الكاملة**، الذي يتيح تحكماً أكثر صرامة في الجهاز. تناسب الأجهزة المملوكة للشركة التي تحتوي على ملف تعريف عمل عندما توفر أجهزة مؤسسية للموظفين للعمل مع السماح بالاستخدام الشخصي. أما الأجهزة المُدارة بالكامل فتناسب بشكل أفضل الأجهزة التي يجب استخدامها للعمل فقط، وأ **الأجهزة المخصصة** (COSU، أجهزة مؤسسية للاستخدام الواحد)، مثل أجهزة الكشك.

لمزيد من المعلومات حول تجهيز الأجهزة، راجع صفحة نظرة عامة على تجهيز الأجهزة.

رموز التسجيل

يستخدم Cerberus Enterprise رموز التسجيل لبدء عملية تسجيل أجهزة Android (التجهيز). يحدد الرمز الذي تختاره السياسة الأولية المطبقة على الأجهزة المسجّلة ويؤثر في أوضاع التجهيز المسموح بها.

> لا تتوفر علامة التبويب الخاصة برموز تسجيل Android إلا بعد إكمال **إعداد Android Management**.

أين تجد رموز التسجيل

في لوحة التحكم، افتح **رموز التسجيل**. وفقاً لتكوين حسابك، قد تعرض الصفحة علامات تبويب متعددة (رموز Android، وتسجيل الدخول عبر Google، والتسجيل اليدوي لأجهزة Apple، والتسجيل التلقائي للأجهزة من Apple).

> إذا كان نشاط Android المؤسسي لديك مدعوماً بنطاق Google مُدار (Google Workspace)، فقد تعرض لوحة التحكم أيضاً علامة تبويب **المصادقة باستخدام تسجيل Google**.
>
> للحصول على تفاصيل حول تمكينها واستخدامها، راجع **المصادقة باستخدام تسجيل Google**.

قائمة رموز التسجيل (Android)

تعرض علامة تبويب رموز Android جدولاً بجميع الرموز. يؤدي النقر على صف إلى فتح صفحة تفاصيل الرمز.

الأعمدة

- **الحالة**: **نشط** (يمكن للأجهزة التسجيل بالرمز)، **منتهي الصلاحية** (لقد مرّ تاريخ الانتهاء) أو **مستنفد** (رمز لمرة واحدة استُخدم بالفعل).
- **السياسة**: السياسة المعيّنة للرمز (يعرض التلميح معرّف السياسة). تعني **سياسة محذوفة** أن السياسة حُذفت بعد إنشاء الرمز.
- **المستخدم**: مستخدم اختياري يُعيّن مسبقاً للأجهزة المسجّلة بالرمز. تعني **مستخدم محذوف** أن المستخدم حُذف بعد إنشاء الرمز.

- **عمليات التسجيل**: عدد الأجهزة التي سجّلت بالرمز، ويظهر على هيئة **n / 1** بالنسبة لرمز لمرة واحدة.
- **الاستخدام الشخصي**: مسموح / غير مسموح / جهاز مخصص.
- **تاريخ الإنشاء**: وقت إنشاء الرمز. يعرض الجدول أحدث الرموز أولاً.
- **تاريخ الانتهاء**: تاريخ/وقت الانتهاء، أو **أبدًا**.
- **رمز التسجيل**: قيمة الرمز المميز، أي الرمز الذي تكتبه على الجهاز عند تسجيله دون رمز QR.

الإجراءات

- يحتوي كل صف على إجراء حذف (**حذف رمز التسجيل**). يكون الحذف معطّلاً عندما يكون الترخيص منتهي الصلاحية.
- يدعم الجدول تحديد صفوف متعددة: يمكنك تمكين وضع التحديد، وتحديد عدة رموز، وحذفها باستخدام **حذف الرموز المحددة**.
- استخدم إجراء التحديث لإعادة تحميل القائمة. الجدول مقسّم إلى صفحات (10/25/50 عنصرًا في الصفحة).

إنشاء رمز تسجيل جديد

في علامة تبويب رموز Android، انقر على **رمز تسجيل جديد** لفتح صفحة إنشاء الرمز. إذا كان ترخيصك منتهي الصلاحية، يكون زر الإنشاء معطّلاً.

خيارات الرمز

1. السياسة

مطلوب. السياسة المطبقة تلقائيًا على جميع الأجهزة المسجّلة باستخدام هذا الرمز. اختر إحدى **سياسات Android** لديك. إذا لم يكن لديك أي سياسة بعد، فأنشئ واحدة أولاً.

2. المستخدم

اختياري. إذا تم تعيينه، ترتبط الأجهزة المسجّلة حديثًا تلقائيًا بهذا المستخدم.

3. الاستخدام الشخصي

يتحكم في ما إذا كان الاستخدام الشخصي مسموحًا على جهاز تم تجهيزه بهذا الرمز:

- **مسموح**: مناسب للأجهزة المملوكة شخصيًا (ملف تعريف العمل) والأجهزة المملوكة للشركة للاستخدام المهني والشخصي.

- **غير مسموح**: مناسب للأجهزة المملوكة للشركة للاستخدام المهني فقط (مُدار بالكامل).
- **جهاز مخصص**: مناسب لأجهزة الكشك/الأجهزة المخصصة (الجهاز غير مرتبط بمستخدم واحد).

4. الاستخدامات المسموح بها

حدد ما إذا كان يمكن استخدام الرمز عدة مرات (**متعدد**) أو مرة واحدة فقط (**لمرة واحدة فقط**).

5. تاريخ الانتهاء

حدد وحدة الانتهاء (**دقائق**، أو **ساعات**، أو **أيام**، أو **أبدًا**). عند عدم الضبط على أبدًا، أدخل قيمة الانتهاء. يعتمد النطاق المسموح به على الوحدة المحددة ويمكن أن يصل إلى 10,000 يوم.

6. مصادقة Google

يتحكم في ما إذا كان يجب على المستخدم المصادقة بحساب Google أثناء تسجيل الجهاز:

- **غير محدد**: يُستخدم إعداد مصادقة Google على مستوى المؤسسة لتحديد ما إذا كان المستخدم بحاجة إلى المصادقة باستخدام Google أثناء التسجيل.
- **اختياري**: يمكن للمستخدم اختيار تخطي مصادقة Google أثناء التسجيل.
- **مطلوب**: يجب على المستخدم المصادقة بحساب Google للمتابعة في التسجيل.

عند تحديد **مطلوب**، يظهر حقل اختياري **البريد الإلكتروني للحساب المطلوب**. إذا تم تعيينه، يجب على المستخدم المصادقة بذلك الحساب المحدد على Google أثناء التسجيل.

خيارات التجهيز (رمز QR فقط)

تُضمّن هذه الخيارات الإضافية في رمز QR وتُطبّق أثناء تجهيز الأجهزة المُدارة بالكامل المسجّلة عبر مسح رمز QR. والتي تنطبق على ملفات تعريف العمل أو الأجهزة المسجّلة باستخدام عنوان URL للتسجيل أو الرمز.

تكوين Wi-Fi

استخدم هذا للسماح للجهاز بالاتصال تلقائيًا بـ Wi-Fi أثناء التجهيز، حتى يتمكن من تنزيل تطبيق الإدارة وتهيئته. تتضمن الحقول المتاحة **SSID**، و**SSID المخفي**، و**الأمان**، و(عند الحاجة) **عبارة المرور**.

يمكنك أيضًا تكوين وكيل HTTP (**الوكيل**)، ووقفًا للوضع، تعيين **المضيف/المنفذ**، و**PAC URI**، و**مضيف تجاوز الوكيل**.

خيارات أخرى

تشمل الخيارات الإضافية **اللغة المحلية**، و**المنطقة الزمنية**، و**تخطي التشفير**.

تفاصيل رمز التسجيل

عند فتح رمز، تعرض صفحة التفاصيل تكوين الرمز ومعلومات الاستخدام:

- **الحالة**، و**تاريخ الانتهاء**، و**الاستخدام**، و**الاستخدام الشخصي**، و**الاستخدامات المسموح بها**، و(عند التعيين) **مصادقة Google** مع **البريد الإلكتروني للحساب المطلوب** الاختياري.
- **الرمز**: قيمة رمز التسجيل الأولية (قابلة للنسخ).
- **عنوان URL للتسجيل**: عنوان URL لتسجيل Google Android Enterprise (قابل للنسخ والإرسال بالبريد الإلكتروني).
- **رمز QR**: يظهر على الجانب الأيمن من الصفحة، ويُستخدم لتسجيل الأجهزة المُدارة بالكامل.

> للحصول على إجراءات التجهيز خطوة بخطوة، اتبع أدلة تسجيل Android: **الأجهزة المملوكة شخصيًا**، و**الأجهزة المملوكة للشركة للاستخدام المهني والشخصي**، و**الأجهزة المملوكة للشركة للاستخدام المهني فقط**، و**Zero-touch**.

الأجهزة المملوكة شخصيًا

يمكن إعداد الأجهزة المملوكة للموظفين باستخدام **ملف تعريف العمل**. يوفر ملف تعريف العمل مساحة مستقلة لتطبيقات العمل وبياناته، منفصلة عن التطبيقات والبيانات الشخصية. تُطبّق معظم سياسات التطبيقات والبيانات والإدارة الأخرى على ملف تعريف العمل فقط، بينما تبقى تطبيقات الموظفين وبياناتهم الشخصية خاصة.
لإعداد ملف تعريف عمل على جهاز مملوك شخصيًا، استخدم إحدى طرق التجهيز التالية (تأكد من ضبط رمز التسجيل على □□□□□□□□ □□□□□ = **مسموح**):

رابط رمز التسجيل

إصدار Android
6.0+

يمكنك تقديم عنوان URL للتسجيل إلى المستخدمين النهائيين. عندما يفتح المستخدم النهائي الرابط من جهازه، سيُرشد خلال إعداد ملف تعريف العمل.

إضافة ملف تعريف عمل من "□□□□□□□□ "

إصدار Android
6.0+

لإعداد ملف تعريف عمل على جهازه، يمكن للمستخدم فتح تطبيق □□□□□□□□ على الجهاز، ثم استخدام شريط البحث للعثور على خيار □□□□ □□ □□□□ □□□□ والنقر عليه.

إذا لم ينجح البحث، فقد يختلف موضع هذا الخيار. إليك بعض الاحتمالات:

- □□□□□□□□ -> □□□□ *Google* □□□□□□□□ -> □□□ □□□□□□ -> □□□□ □□ □□□□ □□□□ .
- □□□□□□□□ -> *Google* -> □□□□□□ □□□□□□□□ -> □□□□ □□ □□□□ □□□□ .

تبدأ هذه الخطوات معالج إعداد يُنزّل *Android Device Policy* على الجهاز. بعد ذلك، يُطلب من المستخدم مسح رمز QR أو إدخال رمز تسجيل يدويًا لإكمال إعداد ملف تعريف العمل.

تنزيل Android Device Policy

إصدار Android
6.0+

لإعداد ملف تعريف عمل على جهازه، يمكن للمستخدم تنزيل Android Device Policy من Google Play Store. بعد تثبيت التطبيق، يُطلب من المستخدم مسح رمز QR أو إدخال رمز تسجيل يدوياً لإكمال إعداد ملف تعريف العمل.

أجهزة iPhone وiPad الشخصية

تُسجّل أجهزة iPhone وiPad الشخصية (وأجهزة Mac) باستخدام **User Enrollment** من Apple: يسجّل المستخدم الدخول بحساب Managed Apple Account الخاص به في إعدادات الجهاز، وتُدار تطبيقات العمل والحسابات والبيانات فقط. على أجهزة iPhone وiPad تُثبّت تطبيقات App Store التابعة للسياسة وتطبيق **Cerberus Enterprise** بترخيص مستخدم لذلك الحساب. لا يُجمع موقع الأجهزة الشخصية إلا إذا فعّلت سياستها **الموقع والنطاقات الجغرافية على الأجهزة الشخصية** وسمح المستخدم بذلك. اقرأ **تسجيل Apple المُوجّه بالحساب**.

الأجهزة المملوكة للشركة للاستخدام المهني والشخصي

يؤدي إعداد جهاز مملوك للشركة باستخدام **ملف تعريف العمل** إلى تمكين الجهاز للاستخدام المهني والشخصي معًا. على الأجهزة المملوكة للشركة التي تحتوي على ملفات تعريف عمل:

- تُطبّق معظم سياسات التطبيقات والبيانات والإدارة الأخرى على ملف تعريف العمل فقط.
- تبقى ملفات التعريف الشخصية للموظفين خاصة. ومع ذلك، يمكن للمؤسسات فرض سياسات معينة على مستوى الجهاز وسياسات استخدام شخصي.
- يمكن للمؤسسات استخدام □□□□ □□□□□ لفرض إجراءات الامتثال على الجهاز بأكمله أو على ملف تعريف العمل فقط.
- تُطبّق أوامر إلغاء تسجيل الجهاز وأوامر الجهاز على الجهاز بأكمله.

لإعداد جهاز مملوك للشركة باستخدام ملف تعريف عمل، استخدم إحدى طرق التجهيز التالية (تأكد من ضبط رمز التسجيل على **الاستخدام الشخصي** = **مسموح**):

طريقة رمز QR

إصدار Android
8.0+

على جهاز جديد أو بعد إعادة ضبط المصنع، يضغط المستخدم (عادةً مسؤول تقنية معلومات) على الشاشة ست مرات في الموضع نفسه. يؤدي ذلك إلى مطالبة الجهاز للمستخدم بمسح رمز QR.

الأجهزة المملوكة للشركة للاستخدام المهني فقط

إدارة الجهاز الكاملة مناسبة للأجهزة المملوكة للشركة والمخصصة للعمل حصريًا. يمكن للمؤسسات إدارة جميع التطبيقات على الجهاز وفرض المجموعة الكاملة من سياسات وأوامر Android Management API.
من الممكن أيضًا تقييد الجهاز (عبر سياسة) بتطبيق واحد أو مجموعة صغيرة من التطبيقات لخدمة غرض مخصص أو حالة استخدام معينة. يُشار إلى هذه المجموعة الفرعية من الأجهزة المُدارة بالكامل باسم **الأجهزة المخصصة**.
لإعداد الإدارة الكاملة على جهاز مملوك للشركة، استخدم إحدى طرق التجهيز التالية (تأكد من ضبط رمز التسجيل على **الاستخدام الشخصي = غير مسموح**):

طريقة رمز QR

إصدار Android
7.0+

على جهاز جديد أو بعد إعادة ضبط المصنع، يضغط المستخدم (عادةً موظف تقنية معلومات) على الشاشة ست مرات في الموضع نفسه. يؤدي ذلك إلى مطالبة الجهاز للمستخدم بمسح رمز QR.

طريقة معرّف DPC

إصدار Android
5.1+

إذا تعذّرت إضافة Android Device Policy عبر رمز QR، يمكن للمستخدم أو موظف تقنية المعلومات اتباع هذه الخطوات لتجهيز جهاز مُدار بالكامل أو جهاز مخصص:

1. اتبع معالج الإعداد على جهاز جديد أو بعد إعادة ضبط المصنع.
2. أدخل بيانات تسجيل الدخول إلى Wi-Fi لتوصيل الجهاز بالإنترنت.
3. عند مطالبتك بتسجيل الدخول، أدخل **afw#setup**، ما يؤدي إلى تنزيل Android Device Policy.
4. امسح رمز QR أو أدخل رمز تسجيل يدويًا لتجهيز الجهاز.

Zero-touch

يمكن لمسؤولي تقنية المعلومات تجهيز الأجهزة المملوكة للشركة باستخدام طريقة التسجيل Zero-touch، الموضحة في تسجيل Zero-touch لمسؤولي تقنية المعلومات. عند تشغيل الجهاز لأول مرة، يُفرض عليه تلقائيًا تطبيق الإعدادات التي حددها مسؤول تقنية المعلومات.

يمكن لمسؤولي تقنية المعلومات تكوين الأجهزة المشتراة من الموزعين المعتمدين مسبقًا وإدارتها باستخدام لوحة تحكم Cerberus Enterprise. لربط حساب Zero-touch الخاص بك، انتقل إلى قسم **Zero-touch** في لوحة التحكم، ثم اتبع التعليمات.

إصدار Android	ملف تعريف العمل	جهاز مُدار بالكامل	جهاز مخصص
8.0+ (Pixel 7.1+)	✓	✓	✓

المصادقة باستخدام تسجيل Google

تتيح ميزة المصادقة باستخدام تسجيل Google (المعروفة أيضًا باسم **مصادقة Google للتسجيل**) للمستخدمين المصادقة بحساب Google Workspace الخاص بهم أثناء تسجيل أجهزة Android.

> تتوفر هذه الميزة فقط لنشاط Android المؤسسي المدعوم بنطاق Google مُدار (Google Workspace).

أين تجده

في لوحة التحكم، افتح **رموز التسجيل** وحدد علامة تبويب **المصادقة باستخدام تسجيل Google**. لا تظهر علامة التبويب إلا عند تكوين Android Management وتوفر كامل Google Workspace لمؤسستك.

تمكين (أو تعطيل) مصادقة Google

يتم تمكين مصادقة Google من **وحدة تحكم مسؤول Google**. بعد تغيير الإعداد، عُد إلى Cerberus Enterprise واستخدم **تحديث الحالة** لإعادة تحميل التكوين الحالي.

1. سجّل الدخول إلى **وحدة تحكم مسؤول Google** باستخدام حساب مسؤول.
2. افتح **الأجهزة**.
3. انتقل إلى **الأجهزة الجوّالة ونقاط النهاية** ← **الإعدادات** ← **عمليات التكامل مع الجهات الخارجية**.
4. ابحث عن **تكامل Android EMM** الخاص بـ Cerberus Enterprise وافتحه.
5. انقر على **إدارة موفري EMM**.
6. بدّل **المصادقة باستخدام Google** لتمكين أو تعطيل مصادقة Google للتسجيل.
7. انقر على **حفظ**.

8. عُد إلى لوحة تحكم Cerberus Enterprise وانقر على **تحديث الحالة** في علامة تبويب **المصادقة باستخدام تسجيل Google**.

رمز تسجيل مصادقة Google

عند تمكين مصادقة Google، تعرض لوحة التحكم رمز تسجيل مخصصاً يُستخدم لوضع التسجيل هذا. يمكن أن تعرض الصفحة **رمز QR**، وقيمة **رمز التسجيل**، و**عنوان URL للتسجيل** (قابل للنسخ والإرسال بالبريد الإلكتروني).

الخيارات الرئيسية

- **السماح بالاستخدام الشخصي**: يتحكم في ما إذا كان الرمز يمكنه تسجيل الأجهزة للاستخدام المهني والشخصي (سيناريوهات ملف تعريف العمل) أو للاستخدام المهني فقط (سيناريوهات مُدارة بالكامل / مخصصة).
- **السياسة الافتراضية الاحتياطية**: السياسة المطبقة عندما لا يكون للمستخدم المسجّل سياسة افتراضية محددة لمصادقة Google.

تفاعل السياسات

يتحكم إعداد السياسة **مصادقة إعداد حساب العمل** (workAccountSetupConfig.authenticationType) في كيفية مصادقة المستخدمين أثناء إعداد حساب العمل، لكن إعداد **المصادقة باستخدام Google** في وحدة تحكم مسؤول Google ونوع رمز التسجيل قد يظلان يفرضان المصادقة.

بالنسبة للأجهزة المسجّلة بالفعل، تُطبّق هذه السياسة فقط إذا كان الجهاز مُداراً بحساب Google Play مُدار (أي مسجّلاً دون **المصادقة باستخدام تسجيل Google**).

> قد تُعطّل بعض الإجراءات (على سبيل المثال تغيير خيارات الرمز) عندما يكون الترخيص منتهي الصلاحية.

تسجيل جهاز

أثناء التسجيل، يُطلب من المستخدم المصادقة بحساب Google Workspace الخاص به. بعد نجاح التسجيل، يرتبط الجهاز بالمستخدم الذي تمت مصادقته.

ملف تعريف العمل (الأجهزة المملوكة شخصياً)

- شارك **عنوان URL للتسجيل** مع المستخدم. عندما يفتح المستخدم على جهاز Android الخاص به، يُرشد خلال إعداد ملف تعريف العمل ومصادقة Google.
- بدلاً من ذلك، يمكن للمستخدم البدء من إعدادات Android واختيار مسار إعداد ملف تعريف العمل، ثم مسح رمز QR أو إدخال رمز التسجيل عند المطالبة.

الأجهزة المملوكة للشركة

- **طريقة رمز QR**: على جهاز جديد أو بعد إعادة ضبط المصنع، اضغط على الشاشة عدة مرات في الموضع نفسه حتى تظهر مطالبة رمز QR، ثم امسح رمز QR الظاهر في لوحة التحكم.
- **طريقة معرّف DPC** (عندما لا يتوفر مسح رمز QR): اتبع معالج الإعداد، واتصل بـ Wi-Fi، ثم عند مطالبتك بتسجيل الدخول أدخل **afw#setup** وتابع بمسح رمز QR أو إدخال رمز التسجيل. عند المطالبة، صادق باستخدام حساب Google Workspace.

لإجراءات تجهيز Android العامة (ملف تعريف العمل مقابل الإدارة الكاملة)، راجع صفحات تسجيل Android القياسية في هذا الدليل.