إدارة التطبيقات

في هذا القسم، يمكنك تعيين سياسات تتعلق بتوفر التطبيقات وتثبيتها وتحديثاتها وإدارة الأذونات.

> تُنشأ حسابات Managed Google Play تلقائيًا عند تجهيز الأجهزة.

1. وضع Play Store

يتحكم هذا الوضع في التطبيقات المتاحة للمستخدم في Play Store وفي السلوك على الجهاز عند إزالة التطبيقات من السياسة.

القائمة البيضاء (الافتراضي): لا تتوفر إلا التطبيقات الموجودة في السياسة، وأي تطبيق غير موجود فيها ستتم إزالته تلقائيًا من الجهاز. لن يعرض Play Store إلا التطبيقات المتاحة.

القائمة السوداء: تتوفر جميع التطبيقات، وأي تطبيق لا يجب أن يكون على الجهاز ينبغي وضع علامة **محظور** عليه صراحةً في سياسة التطبيقات. سيعرض Play Store جميع التطبيقات باستثناء المحظورة.

2. سياسة التطبيقات غير الموثوقة

السياسة الخاصة بالتطبيقات غير الموثوقة (التطبيقات من مصادر غير معروفة) التي تُفرض على الجهاز. يتحكم هذا الخيار في إعداد نظام Android الذي يحدد ما إذا كان المستخدم يستطيع تثبيت تطبيقات من خارج Play Store (التثبيت الجانبي).

عدم السماح (الافتراضي): عدم السماح بتثبيت تطبيقات غير موثوقة على الجهاز بأكمله.

الملف الشخصي فقط: بالنسبة للأجهزة التي تحتوي على ملفات تعريف عمل، اسمح بتثبيت التطبيقات غير الموثوقة في الملف الشخصي للجهاز فقط.

السماح: السماح بتثبيت تطبيقات غير موثوقة على الجهاز بأكمله.

3. Google Play Protect

ام إذا كان التحقق من التطبيقات عبر Google Play Protect مفروضًا.

مفروض (الافتراضي): يفعّل التحقق من التطبيقات قسرًا.

اختيار المستخدم: يسمح للمستخدم باختيار ما إذا كان سيفعّل التحقق من التطبيقات.

4. سياسة الأذونات الافتراضية

السياسة الخاصة بمنح طلبات أذونات وقت التشغيل للتطبيقات.

المطالبة (الافتراضي): مطالبة المستخدم بمنح إذن.

المنح: منح إذن تلقائيًا.

الرفض: رفض إذن تلقائيًا.

5. وظائف التطبيقات

يتحكم في ما إذا كان يُسمح للتطبيقات على الأجهزة المدُارة بالكامل أو في ملفات تعريف العمل بكشف وظائف التطبيقات. يتطلب Android 16 أو أحدث.

مسموح (الافتراضي): يمكن للتطبيقات على الأجهزة المدُارة بالكامل أو في ملفات تعريف العمل كشف وظائف التطبيقات.

غير مسموح: لا يمكن للتطبيقات على الأجهزة المدُارة بالكامل أو في ملفات تعريف العمل كشف وظائف التطبيقات.

6. تثبيت التطبيقات معطّل

ما إذا كان تثبيت المستخدم للتطبيقات معطّلًا.

7. إلغاء تثبيت التطبيقات معطّل

ما إذا كان إلغاء المستخدم لتثبيت التطبيقات معطّلًا.

8. سياسات الأذونات

منح أو رفض صريح للأذونات أو المجموعات لجميع التطبيقات. تتجاوز هذه القيم إعداد **سياسة الأذونات الافتراضية**.

استخدم **إضافة سياسة أذونات** لإنشاء إدخالات، وأزلها باستخدام إجراء الحذف.

يتضمن كل إدخال:

> **إذن/مجموعة Android**: إذن أو مجموعة Android (مطلوب)، مثل **android.permission.READ_CALENDAR** أو **android.permission_group.CALENDAR**.
>
> **السياسة**: منح / رفض / مطالبة (تستخدم خيارات السياسة نفسها كـ**سياسة الأذونات الافتراضية**).

9. التطبيقات

قائمة التطبيقات التي يجب تضمينها في السياسة. يعتمد سلوك محتوى القائمة على القيمة المحددة في **وضع Play Store**.

إذا كان **وضع Play Store** مضبوطاً على **القائمة البيضاء**، فلا تتوفر إلا التطبيقات الموجودة في السياسة، وأي تطبيق غير موجود فيها ستتم إزالته تلقائياً من الجهاز.

إذا كان **وضع Play Store** مضبوطاً على **القائمة السوداء**، تتوفر جميع التطبيقات، وأي تطبيق لا يجب أن يكون على الجهاز ينبغي وضع علامة **محظور** عليه صراحةً في سياسة التطبيقات.

لإضافة تطبيق جديد، انقر على زر **إضافة تطبيقات** (أو أيقونة **إضافة تطبيقات**)، واختر **من Managed Google Play**، ثم اختر التطبيق من Play Store وانقر على زر **تحديد** في بطاقة التطبيق.

لإضافة تطبيق غير منشور على Google Play لكنه موجود بالفعل على الجهاز (مثل تطبيق نظام أو تطبيق من الشركة المصنعة)، انقر على **إضافة تطبيقات**، واختر **حسب اسم الحزمة (التطبيقات المثبتة مسبقاً)**، واكتب اسم حزمة التطبيق (مثل **com.example.app**) ثم انقر على **إضافة**.يُضاف التطبيق بنوع التثبيت **مثبّت قسراً**. لإظهار التطبيق في مشغّل Kiosk المخصص، يجب أن يكون **نوع التثبيت** الخاص به **مثبّتاً مسبقاً** أو **مثبّتاً قسراً**: مع **متاح** لا يظهر التطبيق.

> تُوسم التطبيقات غير المتاحة على Managed Google Play بأيقونة Android في قائمة التطبيقات. لا يمكن تثبيتها من Google Play، لذا يجب أن تكون موجودة بالفعل على الجهاز: الأجهزة التي لا تحتوي على التطبيق لا تستطيع تثبيته.

> جميع التطبيقات المنشورة على Play Store في بلدك متاحة للاختيار افتراضياً. لتحديد تطبيقاتك الخاصة أو تطبيقات الويب، يجب رفعها إلى النظام أولاً. لمزيد من المعلومات، اقرأ صفحة

> **التطبيقات الخاصة**.

يمكن تهيئة كل تطبيق بإعداداته الخاصة، التي تظهر داخل بطاقة:

9.1. نوع التثبيت

نوع التثبيت الذي سيُجرى للتطبيق.

متاح: التطبيق متاح للتثبيت.

مثبّت مسبقاً: يُثبّت التطبيق تلقائياً ويمكن للمستخدم إزالته.

مثبّت قسراً: يُثبّت التطبيق تلقائياً ولا يمكن للمستخدم إزالته.

محظور: التطبيق محظور ولا يمكن تثبيته. إذا كان التطبيق مثبّتاً بموجب سياسة سابقة، فستتم إزالته.

مطلوب للإعداد: يُثبّت التطبيق تلقائياً ولا يمكن للمستخدم إزالته، وسيمنع اكتمال الإعداد حتى يكتمل التثبيت.

Kiosk: يُثبّت التطبيق تلقائياً في وضع Kiosk: يُضبط كنية الشاشة الرئيسية المفضلة ويُدرج في القائمة البيضاء وضع مهمة القفل. لن يكتمل إعداد الجهاز حتى يُثبّت التطبيق. بعد التثبيت، لن يتمكن المستخدمون من إزالة التطبيق. يمكنك ضبط **نوع التثبيت** هذا لتطبيق واحد فقط لكل سياسة. عند وجوده في السياسة، سيُعطّل شريط الحالة تلقائياً. لمزيد من المعلومات، يرجى قراءة صفحة **وضع Kiosk** المخصصة.

9.2. قيود التثبيت

يحدد مجموعة من القيود لتثبيت التطبيق. عند تحديد عدة قيود، يجب استيفاؤها جميعاً ليُثبّت التطبيق.

> يظهر هذا الخيار فقط عندما يكون **نوع التثبيت مثبّتاً مسبقاً** أو **مثبّتاً قسراً**.

شبكة غير محدودة: ثبّت التطبيق فقط عندما يكون الجهاز متصلاً بشبكة غير محدودة (مثل Wi-Fi).

الشحن: ثبّت التطبيق فقط عندما يكون الجهاز قيد الشحن.

خامل: ثبّت التطبيق فقط عندما يكون الجهاز خاملاً.

9.3. وضع التحديث التلقائي

يتحكم في وضع التحديث التلقائي للتطبيق.

الافتراضي: يُحدّث التطبيق تلقائيًا بأولوية منخفضة لتقليل التأثير على المستخدم. يُحدّث التطبيق عند استيفاء جميع القيود التالية: (1) الجهاز غير مستخدم بشكل نشط، (2) الجهاز متصل بشبكة غير محدودة، (3) الجهاز قيد الشحن. يُبلَّغ الجهاز عن تحديث جديد خلال 24 ساعة بعد نشره من المطوّر، ثم يُحدّث التطبيق في المرة التالية التي تُستوفى فيها القيود أعلاه.

مؤجّل: لا يُحدّث التطبيق تلقائيًا لمدة أقصاها 90 يومًا بعد أن يصبح قديمًا. بعد 90 يومًا من أن يصبح التطبيق قديمًا، يُثبّت أحدث إصدار متاح تلقائيًا بأولوية منخفضة (انظر **الافتراضي** وضع التحديث التلقائي). بعد تحديث التطبيق، لا يُحدّث تلقائيًا مرة أخرى حتى 90 يومًا بعد أن يصبح قديمًا مجددًا. ولا يزال بإمكان المستخدم تحديث التطبيق يدويًا من Play Store في أي وقت.

أولوية عالية: يُحدّث التطبيق في أقرب وقت ممكن. لا تُطبّق أي قيود. يُبلَّغ الجهاز فورًا عن تحديث جديد بعد أن يصبح متاحًا.

9.4. الحد الأدنى لرمز الإصدار

الحد الأدنى لإصدار التطبيق الذي يعمل على الجهاز. إذا تم تعيينه، يحاول الجهاز تحديث التطبيق إلى رمز الإصدار هذا على الأقل. إذا لم يكن التطبيق محدّثًا، سيحتوي الجهاز على **تفصيل عدم الامتثال** مع **سبب عدم الامتثال** مضبوطًا على **APP_NOT_UPDATED**. يجب أن يكون التطبيق منشورًا بالفعل على Google Play برمز إصدار أكبر من أو يساوي هذه القيمة. يمكن لـ20 تطبيقًا كحد أقصى تحديد رمز إصدار أدنى لكل سياسة.

9.5. النطاقات المفوّضة

النطاقات المفوّضة إلى التطبيق من Android Device Policy. يمكنك منح تطبيقات أخرى مجموعة مختارة من أذونات Android الخاصة:

تثبيت الشهادات: يمنح الوصول إلى تثبيت الشهادات وإدارتها.

التكوينات المُدارة: يمنح الوصول إلى إدارة التكوينات المُدارة.

حظر إلغاء التثبيت: يمنح الوصول إلى حظر إلغاء التثبيت.

الأذونات: يمنح الوصول إلى سياسة الأذونات وحالة منح الأذونات.

الوصول إلى الحزم: يمنح الوصول إلى حالة الوصول إلى الحزم.

تطبيق النظام: يمنح الوصول لتفعيل تطبيقات النظام.

9.6. الشبكة التفضيلية

خدمة الشبكة التفضيلية التي ستُستخدم لهذا التطبيق. إذا تم ضبطها، سيستخدم التطبيق شريحة الشبكة المؤسسية المحددة لاتصالاته عند توفرها. يجب أن تتطابق هذه مع شريحة شبكة مهيأة في قسم **تكوين تقطيع شبكة 5G** في لوحة **الشبكة الخلوية**.

9.7. سياسة الأذونات الافتراضية

السياسة الافتراضية لجميع الأذونات التي يطلبها التطبيق. إذا تم تحديدها، فإنها تتجاوز **سياسة الأذونات الافتراضية** على مستوى السياسة التي تنطبق على جميع التطبيقات. وهي ال تتجاوز **سياسات الأذونات** التي تنطبق على جميع التطبيقات.

المطالبة (الافتراضي): مطالبة المستخدم بمنح إذن.

المنح: منح إذن تلقائياً.

الرفض: رفض إذن تلقائياً.

9.8. تطبيق العمل والشخصي المتصل

يتحكم في ما إذا كان التطبيق يستطيع التواصل مع نفسه عبر ملفي تعريف العمل والشخصي على الجهاز، وفقاً لموافقة المستخدم (Android 11+).

غير مسموح (الافتراضي): يمنع التطبيق من التواصل عبر ملفات التعريف.

مسموح: يسمح للتطبيق بالتواصل عبر ملفات التعريف بعد تلقي موافقة المستخدم.

9.9. إعفاء من قفل Always On VPN

يحدد ما إذا كان يُسمح للتطبيق بالشبكات عندما ال يكون VPN متصلاً ويكون **تفعيل القفل** نشطاً. مدعوم فقط على الأجهزة التي تعمل بنظام Android 10 أو أحدث.

مفروض (الافتراضي): يحترم التطبيق إعداد قفل Always On VPN.

معفى: التطبيق معفى من إعداد قفل Always On VPN.

9.10. أدوات ملف تعريف العمل

يحدد ما إذا كان يُسمح للتطبيق المثبّت في ملف تعريف العمل بإضافة أدوات إلى الشاشة الرئيسية.

مسموح: يمكن للتطبيق إضافة أدوات إلى الشاشة الرئيسية.

غير مسموح: ال يمكن للتطبيق إضافة أدوات إلى الشاشة الرئيسية.

9.11. إعدادات تحكم المستخدم

يحدد ما إذا كان تحكم المستخدم مسموحاً لتطبيق معين. يشمل تحكم المستخدم إجراءات مثل إيقاف التطبيق قسراً ومسح بيانات التطبيق (Android 11+). إذا كانت **extensionConfig** مفعّلة لتطبيق، فإن تحكم المستخدم غير مسموح بغض النظر عن هذا الإعداد. لتطبيقات Kiosk، يمكن استخدام **مسموح** للسماح بتحكم المستخدم.

غير محدد: يستخدم السلوك الافتراضي للتطبيق لتحديد ما إذا كان تحكم المستخدم مسموحاً أو غير مسموح.

مسموح: تحكم المستخدم مسموح للتطبيق.

غير مسموح: تحكم المستخدم غير مسموح للتطبيق.

9.12. معطّل

ما إذا كان التطبيق معطّلاً. عند التعطيل، تظل بيانات التطبيق محفوظة.

9.13. السماح بمزوّد بيانات الاعتماد

ما إذا كان يُسمح للتطبيق بالعمل كمزوّد بيانات اعتماد على Android 14 أو أحدث.

9.14. التكوين المُدار

لتهيئة الإعدادات المُدارة للتطبيق، انقر على زر **تفعيل التكوين المُدار**. إذا كان قد تم ضبط تكوين مُدار للتطبيق بالفعل، يمكنك تعديل التكوين بزر **التكوين المُدار**، أو حذفه بزر **إزالة التكوين**.

> **التكوين المُدار** متاح فقط للتطبيقات التي تدعم هذه الوظيفة.

9.15. سياسات الأذونات

منح أو رفض صريح للأذونات للتطبيق. تتجاوز هذه القيم **سياسة الأذونات الافتراضية** و **سياسات الأذونات** التي تنطبق على جميع التطبيقات.

استخدم **إضافة سياسة أذونات** لإضافة قاعدة أذونات واحدة أو أكثر لبطاقة التطبيق، وأزلها باستخدام إجراء الحذف.

9.16. معرّفات المسارات

قائمة معرّفات مسارات الاختبار المغلق للتطبيق التي يمكن للجهاز الوصول إليها. إذا تم تحديد عدة معرّفات مسارات، تتلقى الأجهزة أحدث إصدار من بين جميع المسارات المتاحة. إذا لم يتم تحديد أي معرّف مسار، فلا يمكن للأجهزة الوصول إلا إلى مسار الإنتاج للتطبيق.

> خيار **معرّفات المسارات** متاح فقط للتطبيقات التي لديها معرّف مسار واحد على الأقل متاح لمؤسستك. لمزيد من التفاصيل حول كيفية إضافة مؤسستك إلى مسار اختبار مغلق لتطبيق معين، يرجى القراءة هنا.

10. إعدادات التطبيقات الافتراضية

عيّن تطبيقات افتراضية للأنواع المدعومة. عند تعيين تطبيق افتراضي لنوع واحد على الأقل، يُمنع المستخدمون من تغيير التطبيقات الافتراضية في ملف التعريف ذلك.

>

يُسمح بإعداد تطبيق افتراضي واحد فقط لكل**نوع تطبيق افتراضي**. يجب ألا تحتوي قائمة التطبيقات الافتراضية على تكرارات.

10.1. نوع التطبيق الافتراضي

اختر فئة التطبيق لتهيئتها (مثل المتصفح أو تطبيق الاتصال أو الرسائل النصية أو المحفظة أو المساعد). يعتمد التوفر على إصدار Android ووضع الإدارة.

10.2. نطاقات التطبيق الافتراضي

حدّد المكان الذي ينطبق فيه التطبيق الافتراضي (مُدار بالكامل، ملف تعريف العمل، أو الملف الشخصي). لا يمكن اختيار إلا النطاقات المدعومة من النوع المحدد.

إذا لم يكن أي من النطاقات المحددة قابلاً للتطبيق على وضع إدارة الجهاز، فسيُبلغ الجهاز بتفصيل عدم امتثال.

10.3. التطبيقات الافتراضية

قائمة التطبيقات التي يمكن تعيينها كافتراضية للنوع المحدد. يُعيّن أول تطبيق مثبّت ومؤهل كتطبيق افتراضي.

إذا كانت النطاقات تشمل **مُدار بالكامل** أو **ملف تعريف العمل**، فيجب أن يكون كل تطبيق موجوداً أيضاً في قائمة **التطبيقات** مع **نوع تثبيت** غير مضبوط على **محظور**.

11. اختيار المفاتيح الخاص

يسمح بعرض واجهة على الجهاز ليختار المستخدم اسماً مستعاراً لمفاتيح خاص إذا لم تكن هناك قواعد مطابقة في **اختيار قواعد المفاتيح الخاصة**.

بالنسبة للأجهزة الأقدم من Android P، قد يؤدي ضبط هذا إلى ترك مفاتيح المؤسسة عرضة للخطر.

12. اختيار قواعد المفاتيح الخاصة

يتحكم في وصول التطبيقات إلى المفاتيح الخاصة. تحدد القاعدة المفتاح الخاص، إن وُجد، الذي يمنحه Android Device Policy للتطبيق المحدد. يُمنح الوصول إما عندما يستدعي التطبيق KeyChain.choosePrivateKeyAlias (أو أي نسخ محمّلة) لطلب اسم مستعار لمفتاح خاص لعنوان URL معين، أو للقواعد غير الخاصة بعنوان URL (أي إذا لم يتم ضبط urlPattern، أو تم ضبطه على سلسلة فارغة أو .*) على Android 11 وأحدث، مباشرةً بحيث يمكن للتطبيق استدعاء

KeyChain.getPrivateKey دون الحاجة أولاً إلى استدعاء KeyChain.choosePrivateKeyAlias. عندما يستدعي تطبيق KeyChain.choosePrivateKeyAlias وكانت أكثر من قاعدة choosePrivateKeyRules متطابقة، تحدد آخر قاعدة متطابقة اسم المفتاح المستعار الذي يُعاد.

استخدم **إضافة قاعدة مفتاح خاص** لإنشاء إدخالات، وأزلها باستخدام إجراء الحذف.

12.1. اسم المفتاح الخاص المستعار

الاسم المستعار للمفتاح الخاص المراد استخدامه.

12.2. نمط URL

نمط URL المطلوب مطابقته مع عنوان URL للطلب. إذا لم يتم ضبطه أو كان فارغاً، فإنه يطابق جميع عناوين URL. يستخدم هذا صيغة التعبيرات النمطية الخاصة بـ java.util.regex.Pattern.

12.3. أسماء الحزم

أسماء الحزم التي تنطبق عليها هذه القاعدة. يتم التحقق من تجزئة شهادة توقيع كل تطبيق مقابل التجزئة المقدمة من Play. إذا لم تُحدد أسماء حزم، فيُقدّم الاسم المستعار لجميع التطبيقات التي تستدعي KeyChain.choosePrivateKeyAlias أو أي نسخ محمّلة (ولكن ليس دون استدعاء KeyChain.choosePrivateKeyAlias، حتى على Android 11 وأحدث). أي تطبيق يحمل معرّف Android UID نفسه لحزمة محددة هنا سيكون لديه وصول عند استدعاء KeyChain.choosePrivateKeyAlias.

استخدم **إضافة اسم حزمة** لإضافة إدخالات، وأزلها باستخدام إجراء الحذف.

> لحذف تطبيق، انقر على أيقونة **سلة المهملات** في أسفل بطاقة التطبيق.

Revision #59
Created 2025-12-17 09:32:37 UTC by Admin
Updated 2026-11-12 09:53:19 UTC by Admin