AppTec360 Enterprise Mobile Manager & مدير تطبيقات ContentBox

دليل الإدارة | الإصدار 5.0 (202110)

جدول المحتويات

- جهاز إيقاف التشغيل
- إعادة تشغيل الجهاز
- الإنذار ووضع الفقدان | تعطيل وضع الفقدان | تعطيل وضع الفقدان
- حذف الجهاز
- جهاز المسح
- المسح المؤسسي | إزالة MDM
- إرسال رسالة
- برنامج TeamViewer للتحكم عن بُعد
- إرسال طلب التسجيل

أندرويد

- تحرير الجهاز
- مسح رمز المرور
- قفل الجهاز
- حذف الجهاز
- جهاز المسح
- إزالة MDM
- إرسال رسالة
- التحويل إلى وضع COPE
- إرسال طلب التسجيل
- ترحيل الجهاز القديم

النوافذ

- تحرير الجهاز
- حذف الجهاز
- المسح المؤسسي | إزالة MDM
- برنامج TeamViewer للتحكم عن بُعد
- إرسال طلب التسجيل

إدارة المحتوى

- ملفات المجموعة
- مستكشف الملفات
- مسار التدقيق
- القمامة
- التخزين الخارجي

سجل التدقيق

تهيئة نظام التشغيل iOS

- الرسالة (على مستوى الجهاز فقط)
- تهيئة الأمان
  - رمز المرور
  - التشفير
  - مضاد الفيروسات
- نهاية العمر الافتراضي (على مستوى الجهاز فقط)
- المسح (على مستوى الجهاز فقط)
- إعدادات التقييد
  - القيود
  - مالك جهاز AE

حاوية BYOD

- أندرويد إنتربرايز
  - أندرويد إنتربرايز
  - Gmail Exchange
  - تطبيقات نظام AE
  - رمز مرور الحاوية
- Samsung KNOX
  - التفعيل
  - رمز مرور نوكس
  - نوكس سيكيوريتي
  - نوكس للصرافة
  - بريد نوكس الإلكتروني
  - تطبيقات نوكس

إدارة الاتصال

- الواي فاي
- نوع الأمان
  - WEP
  - WPA/WPA2
  - 802.1x EAP 802.1x
- VPN
- القيود
- شبكة APN
- بلوتوث

إدارة PIM

- المبادلات

- البريد الإلكتروني
- AE Gmail Exchange

إدارة التطبيقات

- مدير تطبيقات المؤسسات
  - التطبيقات المثبتة (على مستوى الجهاز فقط)
  - تطبيقات النظام (على مستوى الجهاز فقط)
  - التطبيقات الإلزامية
  - تطبيقات نظام AE
- القيود والإعدادات
  - القائمة السوداء والبيضاء
  - قيود تطبيق النظام
    - تطبيقات سامسونج
    - تطبيقات هواوي
  - إعدادات إدارة التطبيق
- متجر تطبيقات المؤسسات
  - بلاي ستور
  - داخل الشركة
- متجر Play Play للمؤسسات
- وضع الكشك والتشغيل
  - وضع الكشك
  - مُشغِّل تطبيقات AppTec360
  - إعدادات AppTec360

جهاز التحكم عن بُعد

- سبلاش توب
- برنامج Teamviewer

إدارة المحتوى

- صندوق المحتوى
- متصفح آمن

التكوين ويندوز 10 كمبيوتر شخصي

جنرال لواء

- نظرة عامة على ملف تعريف المجموعة (على مستوى المجموعة فقط)
- نظرة عامة على الجهاز (على مستوى الجهاز فقط)
- الإعدادات
- مراجعة التكوين (على مستوى الجهاز فقط)

- المزامنة النشطة للتبادل
- البريد الإلكتروني
- إدارة التطبيقات
- مدير تطبيقات المؤسسات
  - التطبيقات المثبتة
  - التطبيقات الإلزامية
  - قيود تطبيق النظام
  - القائمة السوداء والبيضاء

تهيئة نظام التشغيل MacOS

جنرال لواء

- نظرة عامة على ملف تعريف المجموعة (على مستوى المجموعة فقط)
- نظرة عامة على الجهاز (على مستوى الجهاز فقط)
- مراجعة التكوين (على مستوى الجهاز فقط)
- سجل الجهاز (على مستوى الجهاز فقط)
  - سجل الأوامر
  - حالات الأوامر المحتملة

إدارة الأصول (على مستوى الجهاز فقط)

- معلومات الجهاز
- الواي فاي
- خلوي
- بلوتوث

إدارة التحديث (على مستوى الجهاز فقط)

- معلومات التحديث

إدارة الأمن

- مكافحة السرقة
  - المسح والقفل
- تهيئة الأمان
  - رمز المرور
  - الشهادة
- إعدادات التقييد
  - وظائف الجهاز
  - آي كلاود
  - إدارة وسائل الإعلام

إدارة الاتصال

لمحة عامة

مقدمة إلى AppTec360

يوفر حل إدارة الأجهزة المحمولة للمؤسسات من AppTec خيار إدارة وتهيئة جميع الأجهزة المحمولة من خلال وحدة التحكم في الإدارة البديهية. في هذا السيناريو، يمكن تشغيل خادم EMM إما في محيطك الخاص أو يمكنك استخدام حلنا القائم على السحابة.

حتى فيما يتعلق بموضوع التثبيت المركزي لتطبيقات الشركة على الهواتف الذكية، فقد وصلت إلى المكان الصحيح. فباستخدام برنامج Enterprise Mobile Manager، يمكنك توزيع تطبيقات الشركة ومستنداتها على الأجهزة في غضون ثوانٍ أو حظر التطبيقات غير المرغوب فيها باستخدام القائمة البيضاء/قائمة الحظر.

يشكل استخدام الأجهزة الخاصة في الشركات تحدياً جديداً لتأمين الهواتف الذكية والأجهزة اللوحية. ونظراً لرغبة الموظفين في استخدام هواتفهم الذكية أكثر فأكثر، يجب على مسؤولي تكنولوجيا المعلومات حماية عدد كبير من أنواع الأجهزة المختلفة. سنساعدك في تأمين جميع الأجهزة والبيانات الحساسة المخزنة عليها وإدارتها من خلال وحدة تحكم سهلة الاستخدام.

أنظمة تشغيل الأجهزة المدعومة

يقدم AppTec360 الدعم لأجهزة iOS و Android و Windows. يرجى ملاحظة أن قدرة وظائف المنصات المذكورة يمكن أن تختلف من نظام تشغيل إلى آخر.

- Apple iOS 11.0 أو أعلى*
- Apple macOS 10.11 أو أعلى
- جوجل أندرويد 4.4 أو أعلى** على الإصدار السحابي من جوجل أندرويد 4.4 أو أعلى
- جوجل أندرويد 4.1 أو أعلى** على الإصدار OnPrem
- نظام التشغيل MS Windows 10 أو أعلى*** (كمبيوتر مكتبي-حاسوب مكتبي وكمبيوتر محمول وكمبيوتر لوحي)

يرجى ملاحظة أنه لا يمكن تسجيل الأجهزة التي تعمل بنظام iOS 10 أو أقدم من ذلك بسبب التغييرات الجذرية التي أجرتها Apple في عملية التسجيل.

**يمكن توصيل الأجهزة وتهيئتها حتى لو كانت تستخدم إصدارًا لم يعد مدعومًا من قبل الشركة المصنعة. يُرجى ملاحظة أنه قد تكون هناك ميزات تتطلب إصدار Android معين. في حالات الدعم، نتبع الدعم الرسمي من الشركة المصنعة. في حالة وجود مشاكل أو أخطاء ناجمة عن إصدار قديم لم يعد مدعومًا من قبل الشركة المصنّعة، نحتفظ بالحق في تقديم دعم محدود فقط.*

***الإصدار المنزلي من Windows غير مدعوم بسبب قيود نظام التشغيل. نوصي بشدة باستخدام إصدار نظام التشغيل الذي لا يزال مدعومًا من قبل الشركة المصنعة. ليس فقط من أجل التوافق ولكن أيضًا لأسباب أمنية. لذلك نوصي باستخدام نظام التشغيل iOS 12 أو أعلى وAndroid 9 أو أعلى.*

دلائل LDAP المدعومة

- دليل مايكروسوفت النشط
- فتح LDAP

يمكن العثور على معلومات محدّثة حول "أنظمة تشغيل الأجهزة المدعومة" و"دلائل LDAP المدعومة" هنا:

https://www.apptec360.com/products/systemrequirements/

شرح "الوضع الخاضع للإشراف" على أجهزة Apple

يمثل الوضع الخاضع للإشراف واجهة موسعة لأجهزة iOS.

على الجهاز الذي تم تكوينه على التوالي، يمكن تطبيق قيود إضافية، حيث إنها تتعلق بوظائف جهاز المستخدم النهائي. يتم تضمينها أيضًا في كتيب الإدارة ويتم تمييزها بشعار.

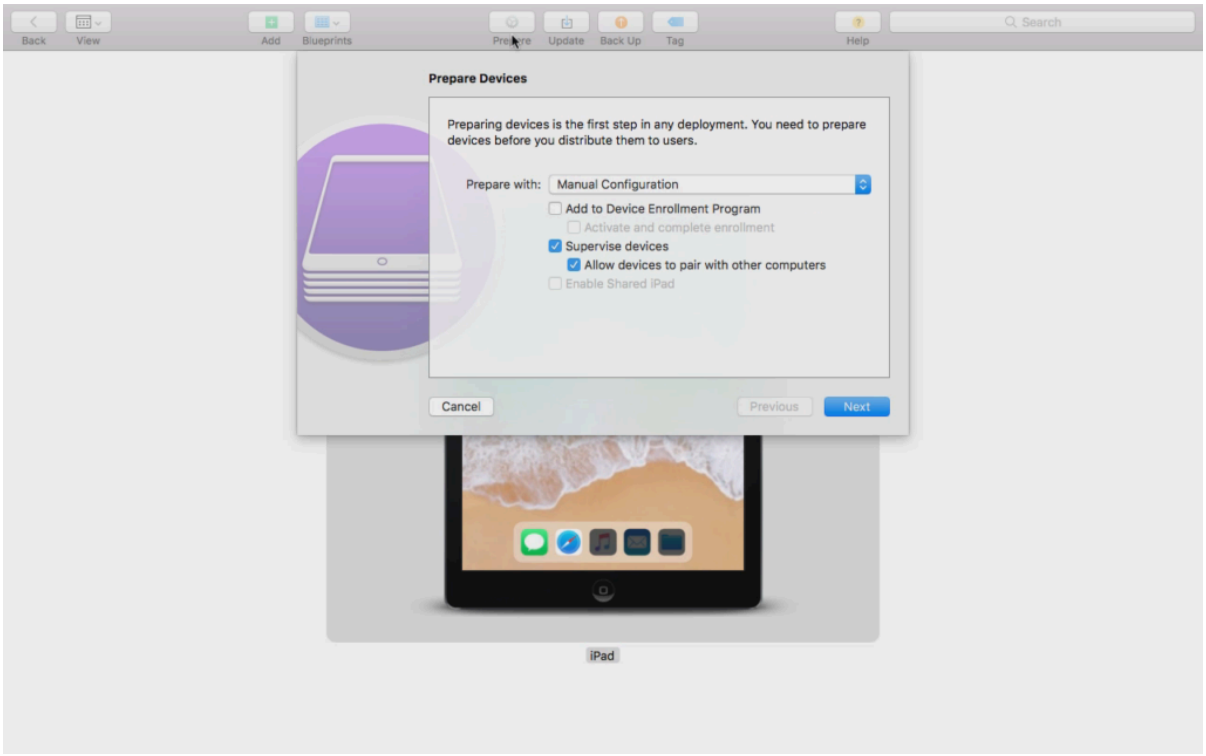
متوفر في الوضع الخاضع للإشراف

يمكن تفعيل "الوضع الخاضع للإشراف" باستخدام برنامج "Apple Configurator". يمكن لبرنامج "Apple Configurator" ضبط الإعدادات الافتراضية على أجهزة iOS الجديدة كأداة تهيئة (عبر واجهة USB).

لا يمكن للأداة تثبيت ملفات تعريف التكوين فحسب، بل يمكن للأداة تثبيت التطبيقات أيضًا. وهي مجانية، ولكنها تتطلب حاسوب ماك.

تنشيط الوضع الخاضع للإشراف

1. افتح أداة تهيئة Apple



2. انقر على الجهاز واختر "إعداد"
3. اختر "التكوين اليدوي" و "الإشراف على الأجهزة"
4. انقر على "التالي"
5. (اختياري) يمكنك الآن إضافة خادم MDM حيث سيتم تسجيل الجهاز. يمكن العثور على الرابط الخاص بذلك في "الإعدادات العامة - تهيئة نظام iOS - المهيئ وعنوان URL" اختر مؤسستك أو أنشئ واحدة جديدة
6. اختر مؤسستك أو أنشئ مؤسسة جديدة
7. اختر الخطوات التي يجب تخطيها في الإعداد الأولي وانقر على "التالي" (تنبيه: سيؤدي المتابعة إلى حذف جهازك!)

الآن سيتم وضع جهازك في الوضع الخاضع للإشراف. قد يستغرق ذلك بضع دقائق. بعد الانتهاء من ذلك، سيتم إعادة تشغيل الجهاز.

الآن جهازك تحت الإشراف!

إضافة جهاز إلى DEP

يمكنك أيضًا إضافة الأجهزة إلى برنامج تسجيل الأجهزة (DEP) باستخدام أداة Apple Configurator، إذا كانت أجهزتك تعمل بنظام iOS 11 أو أعلى.

مزيد من المعلومات حول DEP: https://www.apple.com/business/dep/

اتبع نفس الخطوات التي تتبعها في الإشراف على جهاز، بالإضافة إلى تحديد "إضافة إلى برنامج تسجيل الجهاز". سيُطلب منك بيانات تسجيل الدخول إلى DEP إذا لم تقم بتسجيل الدخول إلى DEP من قبل باستخدام أداة Apple Configurator.

بعد اكتمال العملية، يمكن العثور على الجهاز في خادم DEP Server "الأجهزة المضافة بواسطة Apple Configurator 2". يمكنك الآن استخدام هذا الخادم وتوصيله بوحدة تحكم الإدارة أو نقل الجهاز إلى خادم موجود بالفعل.

لقد نجحت الآن في إضافة جهاز إلى DEP!

شرح نظام أندرويد إنتربرايز

ما هي شركة أندرويد إنتربرايز؟

يوفر نظام Android Enterprise تحكماً أفضل في أجهزة العمل التي تتم إدارتها باستخدام نظام إدارة الأجهزة المتنقلة (MDM). يتيح ذلك للمسؤولين إما التحكم الكامل في أجهزة Android الخاصة بهم أو فصل بيانات الشركة عن البيانات الخاصة على أجهزة الحاوية. بالإضافة إلى ذلك، يسمح Android Enterprise بتسجيل أسهل للأجهزة وتوزيع التطبيقات بسهولة.

ما هي متطلبات استخدام Android Enterprise؟

يمكن للجميع استخدام Android Enterprise مجانًا. ما عليك سوى توصيل حساب google بحساب google بـ MDM لتمكين جميع ميزات Android Enterprise. يمكن الاطلاع على المزيد حول هذا الأمر في قسم Android Enterprise.

يمكن استخدام Android Enterprise على الأجهزة التي تعمل بنظام Android 5.1 أو أعلى، باستثناء ملف تعريف العمل المحسّن (انظر أدناه). نوصي باستخدام نظام أندرويد 7 أو أعلى على الأقل لتسهيل التسجيل أو أندرويد 11 للاستفادة من جميع الميزات المتاحة.

ما هي الأوضاع المتاحة مع Android Enterprise؟

هناك 3 أوضاع مختلفة لاستخدامها عند استخدام Android Enterprise.

جهاز مُدار بالكامل (مُدار للعمل فقط): جهاز مُدار بالكامل يُستخدم للعمل فقط. يسمح ذلك للمسؤول بالتحكم الكامل في الجهاز. هذا لا يسمح بالاستخدام الخاص للجهاز. لتسجيل الأجهزة في هذا الوضع، يجب إعادة تعيين الأجهزة وتسجيلها باستخدام رمز الاستجابة السريعة (انظر تسجيل AE) أو تسجيلها عبر تسجيل Knox Enrollment أو Zero Touch.

حاوية"أحضر جهازك الخاص": تسمح حاوية BYOD (أحضر جهازك الخاص) للمستخدمين بالوصول إلى بيانات الشركة على هواتفهم الخاصة في حاوية منفصلة. في هذا الوضع، لا تستطيع التطبيقات الخاصة رؤية بيانات وتطبيقات الشركة والعكس صحيح. لتسجيل الأجهزة في هذا الوضع، يجب تنزيل تطبيق AppTec ومسح رمز الاستجابة السريعة ضوئيًا. أنشئ جهازًا في وحدة التحكم وحدد "حاوية AE (BYOD وملف تعريف العمل المدمج)" كنوع الجهاز. انقر على رمز الاستجابة السريعة على الجهاز الذي تم إنشاؤه حديثاً للحصول على رمز الاستجابة السريعة وقم بتعيين المفتاح الأول إلى "Legacy & BYOD".

ملف تعريف العمل المحسّن AE: (يتطلب أندرويد 11 أو أعلى) في حين أن حاوية BYOD المذكورة أعلاه تجلب بيانات الشركة على جهاز خاص، فإن ملف تعريف العمل المحسّن يقوم بنفس الشيء ولكن لجهاز مملوك للشركة. فهو ينشئ نفس الحاوية، ولكنه يمنح المسؤول مزيدًا من التحكم في الجهاز، بحيث لا يمكن للمستخدم ببساطة إزالة MDM من الجهاز. أنشئ جهازًا في وحدة التحكم وحدد "حاوية AE (BYOD وملف تعريف العمل المملوك للشركة)" كنوع الجهاز. انقر على رمز الاستجابة السريعة على الجهاز الذي تم إنشاؤه حديثًا للحصول على رمز الاستجابة السريعة وقم بتعيين المفتاح الأول إلى "ملف تعريف العمل المحسّن". يمكن مسح رمز الاستجابة السريعة هذا بعد إعادة ضبط الجهاز والنقر 6 مرات على الشاشة كما هو موضح في الطريقة 1 في تسجيل AE.

كيف يمكنني تعيين التطبيقات لأجهزة Android Enterprise؟

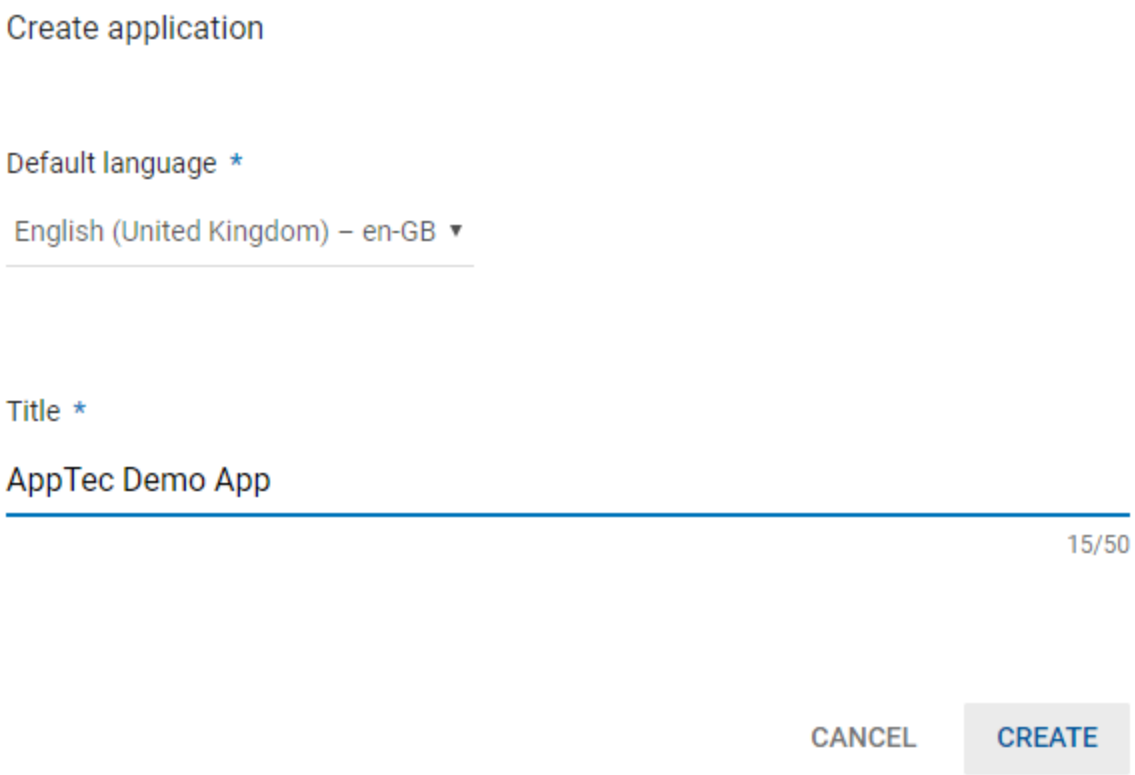
عليك أولاً الموافقة على التطبيقات التي تريد استخدامها في الإعدادات العامة ← إدارة التطبيقات ← إدارة التطبيقات ← متجر AE Play Store ← تطبيقات متجر Play. بعد الموافقة على أحد التطبيقات، يمكنك تعيينه إلى قائمة التطبيقات الإلزامية → في ملفك الشخصيّ من خلال النقر على "+" وتحديد التطبيق من علامة التبويب "متجر AE Play Store". سيؤدي ذلك إلى تنزيل التطبيق وتثبيته تلقائيًا. لا يلزم وجود حساب google على الجهاز ولا يتعين على المستخدم تأكيد ذلك أو السماح به.

تحميل تطبيقاتك الخاصة على متجر Google Play

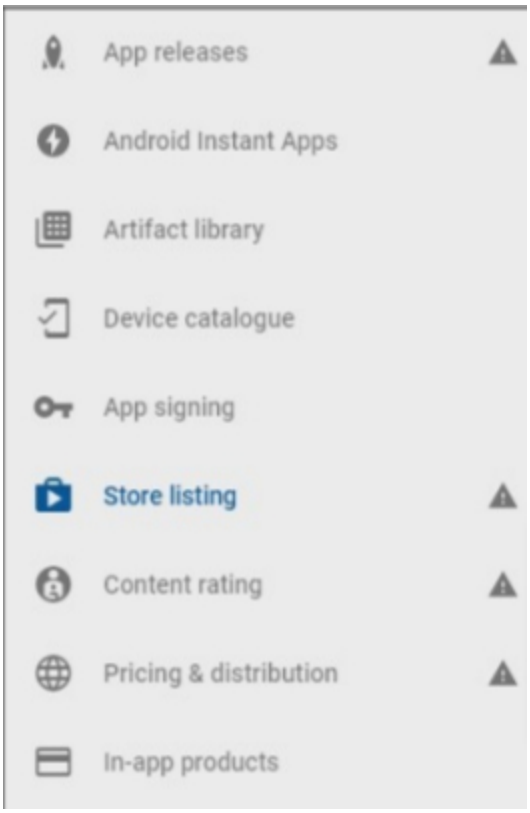
من الممكن تحميل تطبيقاتك الداخلية إلى متجر Google Play. وبهذه الطريقة يمكنك الاستفادة من مزايا مختلفة مثل آلية تحديث متجر Play.

للقيام بذلك، تحتاج إلى حساب مطوّر جوجل. قم بتسجيل الدخول باستخدام Google Play Console(https://play.google.com/apps/publish)

انقر على "إنشاء تطبيق". اختر لغتك الافتراضية وعنوان التطبيق.



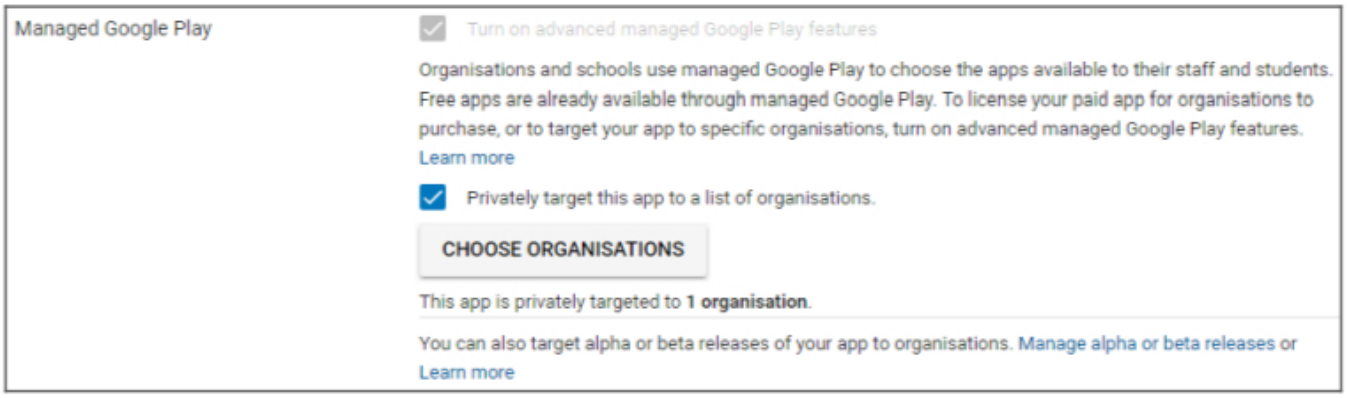
في الصفحة التالية سيُطلب منك إدخال تفاصيل مختلفة عن تطبيقك.



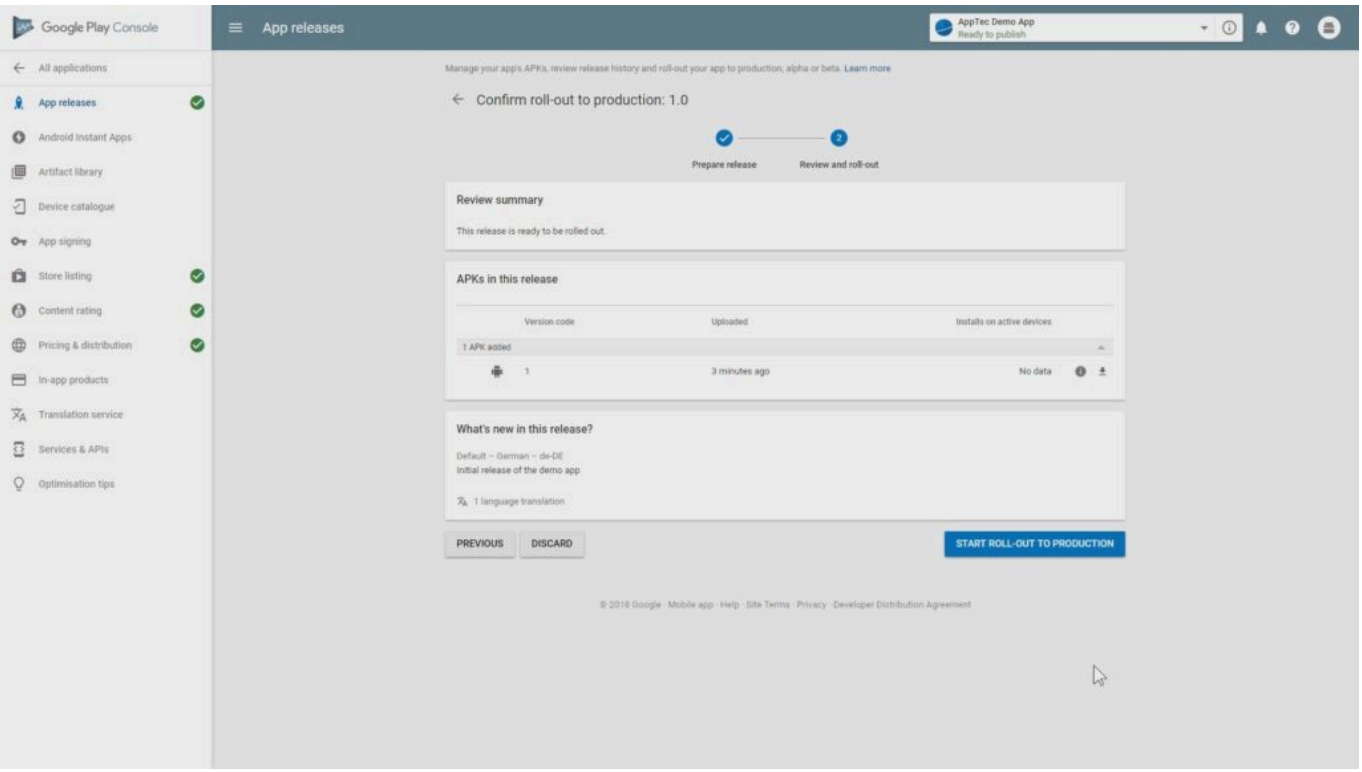
بعد إدخال جميع التفاصيل، سترى رموز تلميحات مختلفة على الجانب الأيسر.

مرر فوقها لترى الخطوات المتبقية واتبعها بأي ترتيب تريده.

ملاحظة: تأكد من تحديد خانتي الاختيار في "إدارة Google Play" ضمن "التسعير والتوزيع". وإلا سيكون التطبيق عامًا ويمكن للجميع الوصول إليه. تأكد أيضًا من اختيار المقاطعة للتوزيع.



بعد الانتهاء من كل خطوة، يمكنك الانتقال إلى "إصدارات التطبيق". انقر على "مراجعة" و "بدء الطرح للإنتاج" لوضع اللمسات الأخيرة على مسودتك ونشر التطبيق.



يستغرق الأمر بعض الوقت حتى يتوفر التطبيق في متجر Play. بعد انتهاء العملية، يمكنك البحث عن تطبيقك في متجر Play for Work والموافقة عليه. بعد ذلك يمكنك ببساطة تعيين التطبيق للأجهزة باستخدام وحدة تحكم EMM تماماً كما تفعل مع التطبيقات الأخرى.

المتطلبات والتركيب

المتطلبات

متطلبات النظام

يتوفر الجهاز الافتراضي بتنسيق المحاكاة الافتراضية المفتوحة (VMWare وVMWare وVirtualBox وCitrix Xen Server) وكملف مضغوط .vhdx (Hyper-V)*.

*ملاحظة: يجب إنشاء الجهاز بالجيل 1 عند استخدام Hyper-V.

يبلغ الحجم المستهدف للقرص الافتراضي 20 جيجابايت ويتطلب الجهاز 4 جيجابايت من ذاكرة الوصول العشوائي.

يستند الجهاز على نظام دبيان 9 64 بت

قم بترقية الآلة المستوردة إلى أحدث توافق (على سبيل المثال في VMWare) وتأكد من تعيين نوع نظام تشغيل الآلة بشكل صحيح في برنامج Hypervisor الخاص بك.

مفتاح الترخيص

لتفعيل الخادم وتثبيته بنجاح، ستحتاج إلى ملف ترخيص صالح. يمكنك الحصول على واحد من AppTec360 مباشرةً و/أو من بائع التجزئة الخاص بك.

عنوان IP-عنوان IP وحل DNS

يجب أن يكون جهاز AppTec360 قابلاً للوصول إليه من قبل الجهاز باستخدام اسم المضيف الذي تم إصدار الترخيص له.

لتسجيل أجهزة ويندوز 10، تحتاج أيضًا إلى إعداد نطاق فرعي إضافي على شكل "enterpriseenrollment." يشير إلى الجهاز.

شهادة SSL-شهادة SSL

نظرًا لأن جميع الاتصالات من وإلى الأجهزة يجب أن تكون مؤمنة باستخدام SSL، فأنت بحاجة إلى شهادة صالحة لاسم المضيف صادرة عن مرجع مصدق موثوق به من قبل الجهاز. يجب تحميل المفتاح الخاص للشهادة بدون حماية بكلمة مرور. في معظم الحالات، يلزم وجود شهادة وسيطة لـ CA لكي تتعرف الأجهزة على شهادة الخادم.

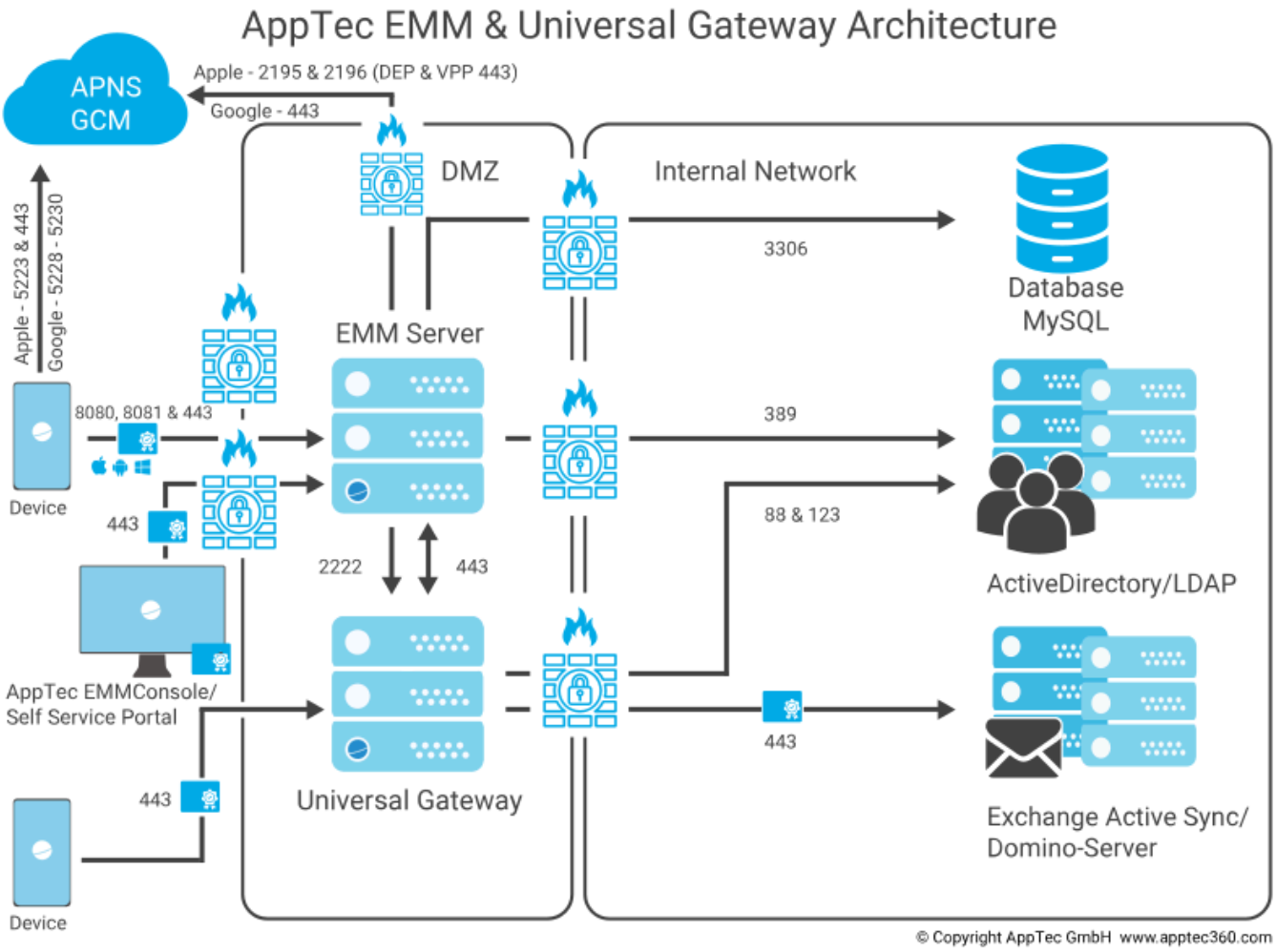
ستتطلب أجهزة Windows 10 شهادة محددة للنطاق الفرعي الخاص بمؤسستك.

بدءًا من الإصدار 202104 من الجهاز، يمكنك أيضًا استخدام شهادات Let's Encrypt، والتي يتم إنشاؤها تلقائيًا (كما هو موضح في الخطوة الثانية - شهادة SSL).

خادم SMTP

يلزم وجود خادم بريد إلكتروني و/أو ترحيل بريد إلكتروني للسماح ل AppTec360 EMM بإرسال رسائل البريد الإلكتروني (على سبيل المثال لتسجيل الجهاز والتحقق من صحة الحساب).

قواعد جدار الحماية



يوضح هذا الرسم البياني الاتصال المطلوب بناءً على الخدمات التي تريد استخدامها.

للحصول على وصف أكثر تفصيلاً انظر الجدول في الصفحة التالية.

أي (خارجي/أجهزة)	→	**تطبيق AppTec360 Appliance / emmconsole.com**
الموانئ	443	الإدارة، متجر تطبيقات المؤسسات واتصالات ويندوز فون
	8080	اتصالات أندرويد و iOS
	80	إعداد Let´s Encrypt لأول مرة. يستخدم 443 بعد ذلك.
أي (أجهزة)	→	**أي (خارجي)**
الموانئ	443 ,5223	خدمة Apple Push، يجب أن تكون قابلة للوصول إليها بدون وكيل، 443 كخدمة احتياطية، انظر https://support.apple.com/en-us/HT203609
	5228-5230	خدمة دفع أندرويد (FCM)، يجب أن تكون قابلة للوصول إليها بدون وكيل
جهاز AppTec360 AppTec360	→	**وحدة تحكم المجال**
الموانئ	389، LDAPS) (636	مزامنة المستخدم مع LDAP
جهاز AppTec360 AppTec360	→	**أي**
الميناء	443	تُستخدم لخدمة الدفع بنظام أندرويد (GCM) البحث في متجر التطبيقات / متجر Play
جهاز AppTec360 AppTec360	→	**emmconsole.com**
الموانئ	443	تحديثات جهاز AppTec360 AppTec360، إنشاء شهادة APNS
جهاز AppTec360 AppTec360	→	**شبكة Apple (17.0.0.0.0.0/8)**
الموانئ	2196 ,2195	خدمة Apple Push Push وخدمة التعليقات والملاحظات
	443	برنامج التنمية الاقتصادية وبرنامج الشراكة الطوعية

تحديثات الأمان

يجب تحديث نظام تشغيل دبيان بانتظام للحصول على أحدث الإصلاحات الأمنية. ولكن تأكد من عدم الترقية إلى إصدار رئيسي أحدث من دبيان يدوياً. عندما يكون AppTec360 EMM متوافقًا مع إصدار رئيسي أحدث، سنضيف طريقة للترقية في تحديث الجهاز.

كلمات المرور الافتراضية للجهاز الظاهري

مستخدم تسجيل الدخول (تم تعطيل تسجيل الدخول الجذر. استخدم "sudo" لمهام الإدارة)

آبتيك

كلمة مرور تسجيل الدخول

آبتيك

مستخدم جذر MySQL

الجذر

كلمة المرور الجذرية لـ MySQL

آبتيك

المستخدم الافتراضي لـ MySQL

آبتيك

كلمة مرور المستخدم الافتراضية لـ MySQL

آبتيك

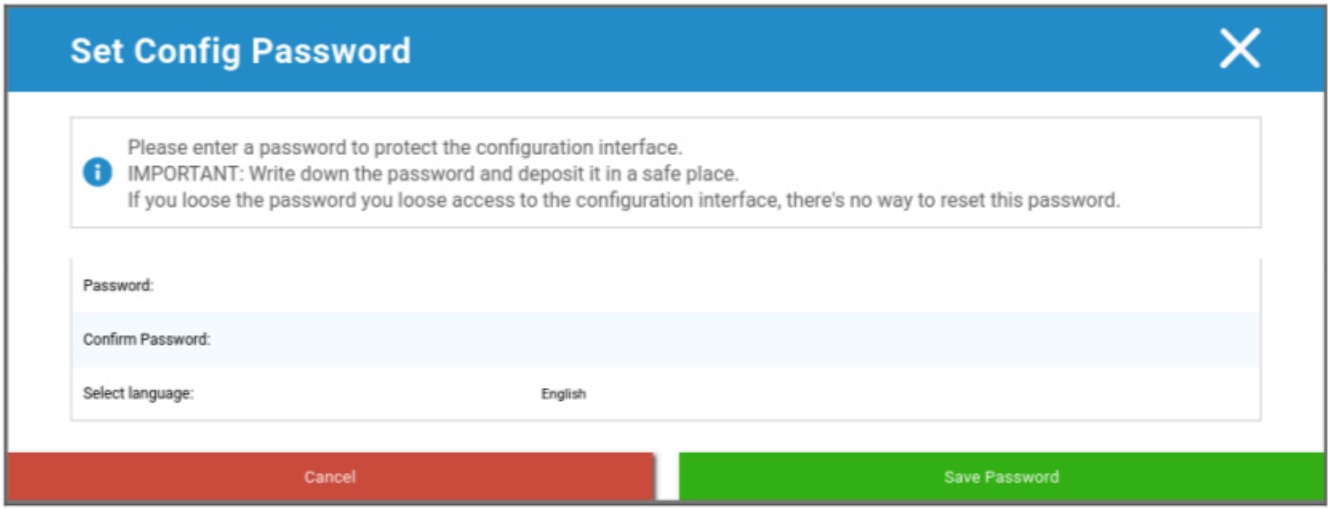
تكوين الجهاز الظاهري

هام: قبل البدء في تكوين الجهاز الظاهري يجب ضبط دقة العرض على 1280 × 800 بكسل على الأقل.

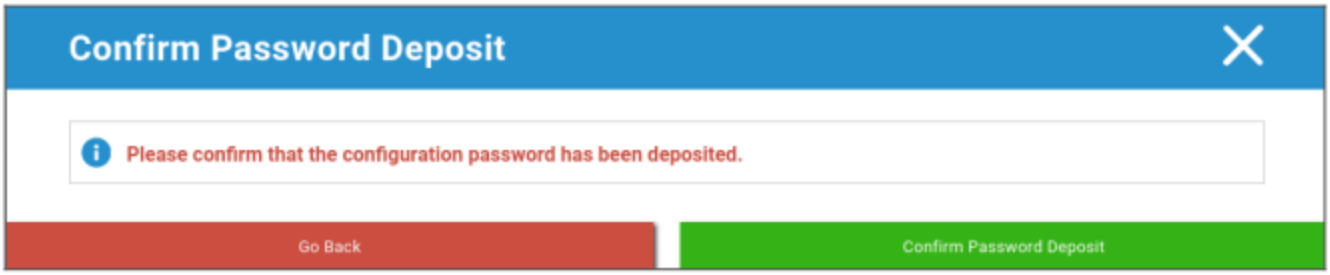
بعد الدخول بشوق إلى الجهاز، يجب أن يبدأ Firefox تلقائياً ويعرض واجهة التكوين.

التحضير

تحتاج أولاً إلى توفير كلمة مرور لواجهة التكوين. تُستخدم كلمة المرور هذه لتشفير جميع المعلومات والملفات التي يتم إدخالها في واجهة التهيئة. هنا يمكنك أيضًا تعيين اللغة التي يجب أن تُعرض بها الواجهة (يمكن تغييرها لاحقًا).

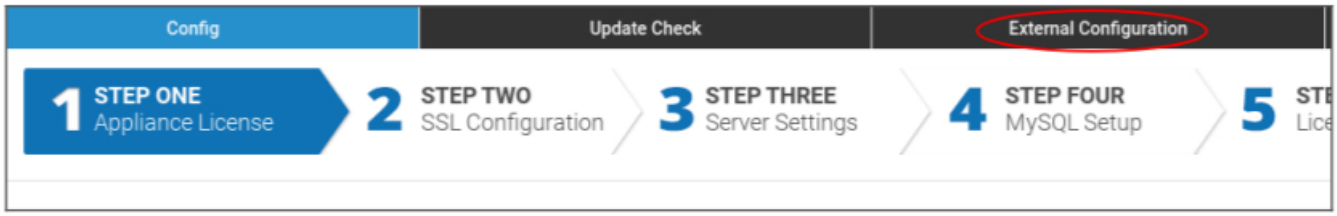


لا يمكن إعادة تعيين كلمة المرور إلا عن طريق دعم AppTec360، لذا تأكد من إيداعها في مكان آمن وتأكيد النافذة المنبثقة القادمة.



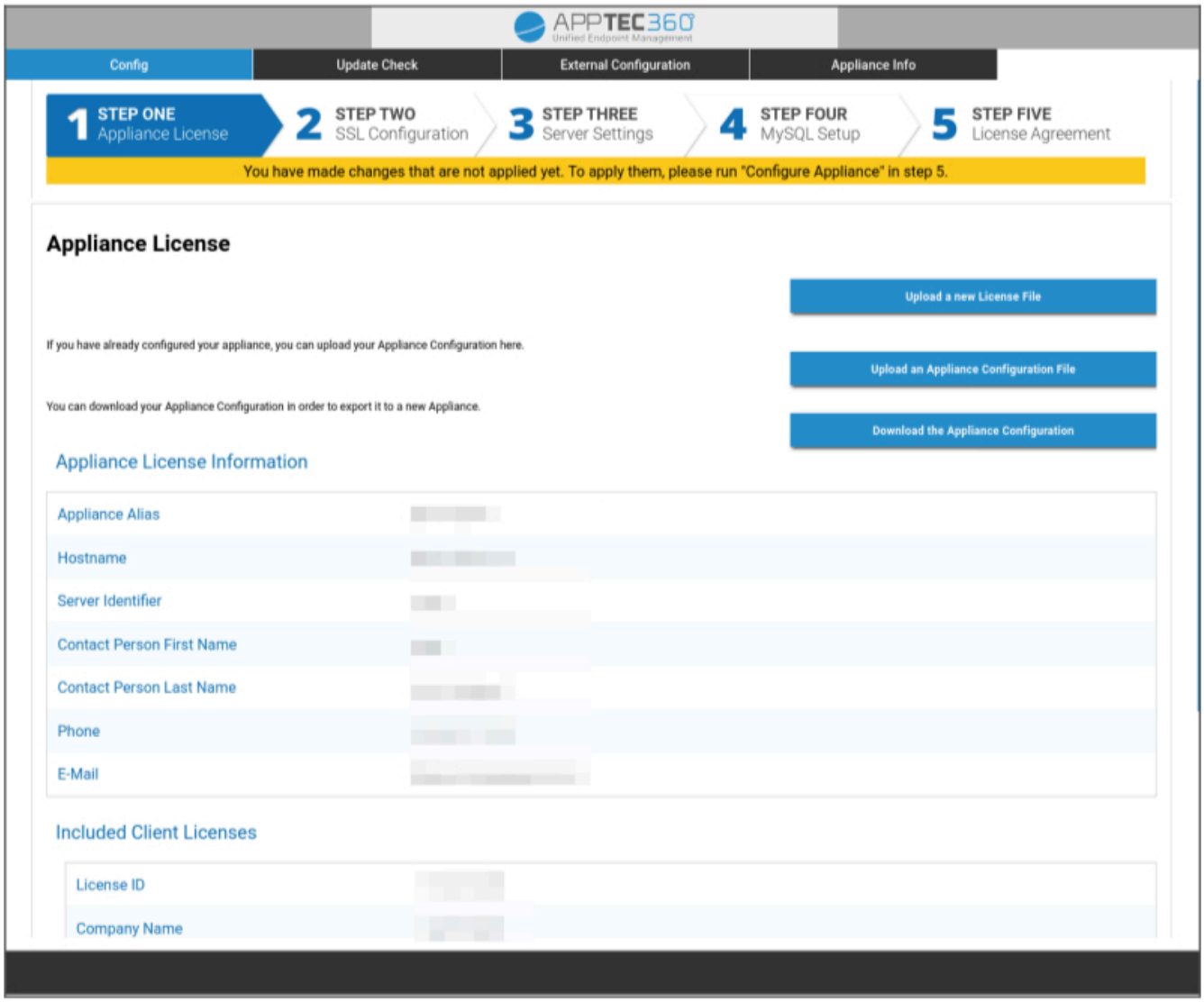
التهيئة من مضيف خارجي

لتيسير عملية الإعداد، يمكنك جعل صفحة التكوين قابلة للوصول إليها من بعيد. للقيام بذلك، اتبع الخطوات الواردة في "التهيئة من مضيف خارجي".



الخطوة الأولى – ترخيص الجهاز

1. يُرجى تحميل ملف الترخيص الذي استلمته من AppTec.
2. إذا تم تحميل ملف الترخيص بنجاح، يمكنك رؤية معلومات ترخيص الجهاز كما في لقطة الشاشة أدناه.



الخطوة الثانية – شهادة SSL

يمكنك إما استخدام الإعداد التلقائي للشهادة باستخدام Let's Encrypt أو توفير الشهادات بنفسك (راجع شهادة SSL لمزيد من المعلومات).

أوتوماتيكي

سيتم إنشاء الشهادة تلقائياً باستخدام خدمة Let's Encrypt.

يستخدم AppTec360 EMM تحدي HTTP-01 للتحقق من صحة المجال مما يعني أن منفذ HTTP يجب أن يكون مفتوحًا من الإنترنت للطلب الأول للشهادة. يمكن التحقق من صحة طلبات التجديد اللاحقة عبر HTTPS.

قم بتبديل أزرار الاختيار إلى "تلقائي (Let's Encrypt)" واضغط على "حفظ القيم". سيتم طلب الشهادة تلقائيًا عند تطبيق التكوين في الخطوة الخامسة - اتفاقية الترخيص. سيتم تجديد الشهادة تلقائيًا إذا لزم الأمر وستتلقى رسالة بريد إلكتروني إذا كانت الشهادة على وشك الانتهاء (مما يعني أن التجديد قد يكون فشل).

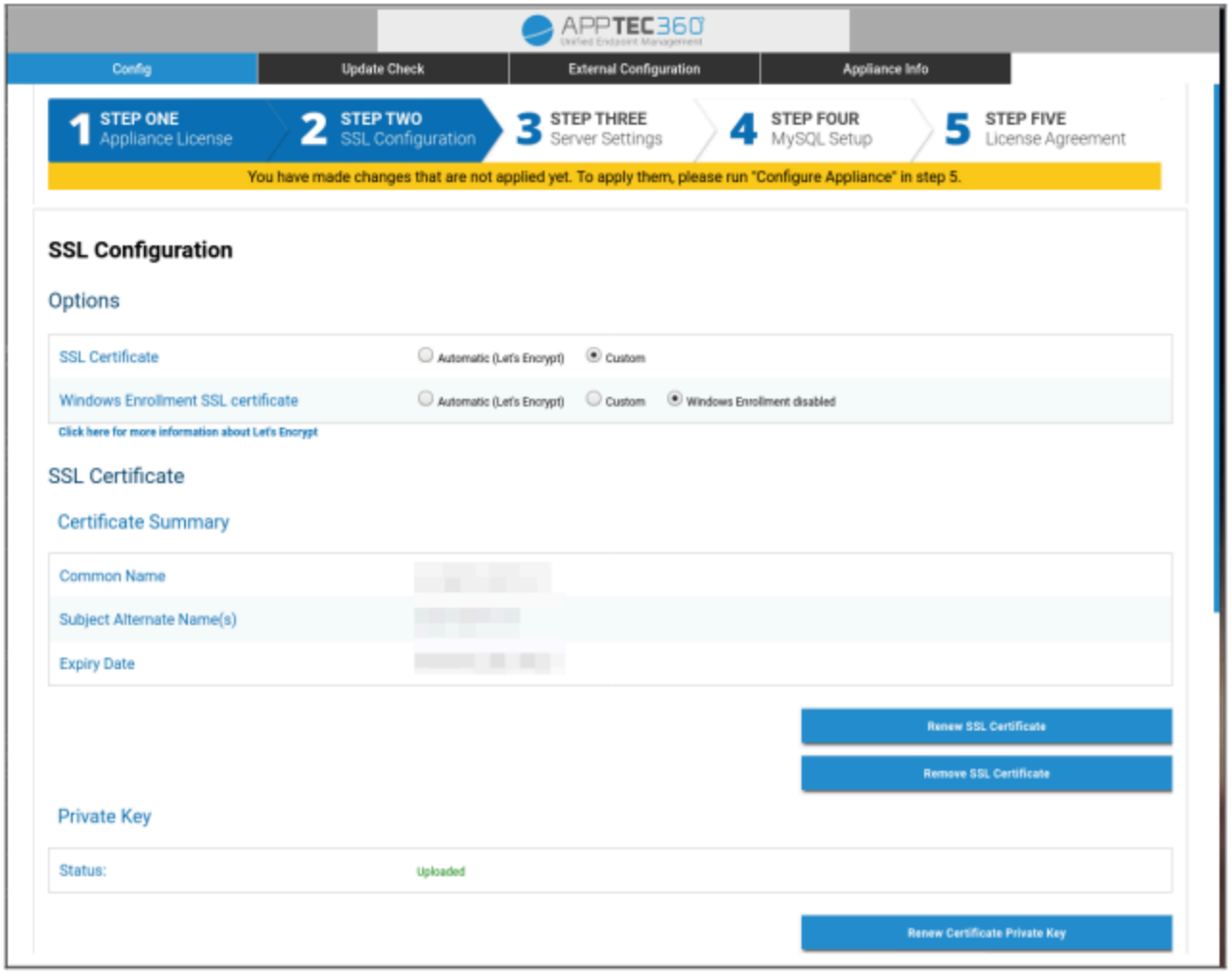
مخصص

1. قم بتحميل شهادة SSL-شهادة SSL لاسم المضيف المرخص لك. يمكنك رؤية اسم المضيف في الخطوة الأولى - ترخيص الجهاز.

2. يرجى أيضًا تحميل المفتاح الخاص للشهادة والشهادة الوسيطة إذا لزم الأمر.

هام: يجب ألا يكون المفتاح محميًا بكلمة مرور. إذا كان كذلك، يرجى إزالة كلمة المرور قبل التحميل.

تلميح: إذا كنت ترغب أيضًا في استخدام أجهزة ويندوز 10، فعليك تمكين "شهادة SSL لتسجيل ويندوز" وتحميل الشهادة والمفتاح الخاص والشهادة الوسيطة للنطاق الفرعي الخاص بك (الموضح في عنوان IP-عنوان IP وDNS Resolution) تحميل في أسفل الصفحة.



الخطوة الثالثة – إعدادات الخادم

1. يرجى إدخال عنوان بريد إلكتروني عالمي للدعم. سيتم استخدام هذا العنوان في رسائل البريد الإلكتروني للمستخدمين حتى يعرفوا بمن يتصلون في حالة وجود أي مشاكل تتعلق بأجهزتهم.

2. توفير إعدادات البريد الإلكتروني ليستخدمها النظام لإرسال رسائل البريد الإلكتروني. سيتم استخدام الإعدادات لإرسال رسائل البريد الإلكتروني إلى المستخدم وكذلك لإرسال تقارير الأخطاء وطلبات الميزات إلى"support@apptec360.com".بعد حفظ إعدادات البريد الإلكتروني تحتاج إلى التحقق منها بالنقر على "اختبار تكوين البريد الإلكتروني" واتباع التعليمات.

الخطوة الرابعة – إعداد MySQL

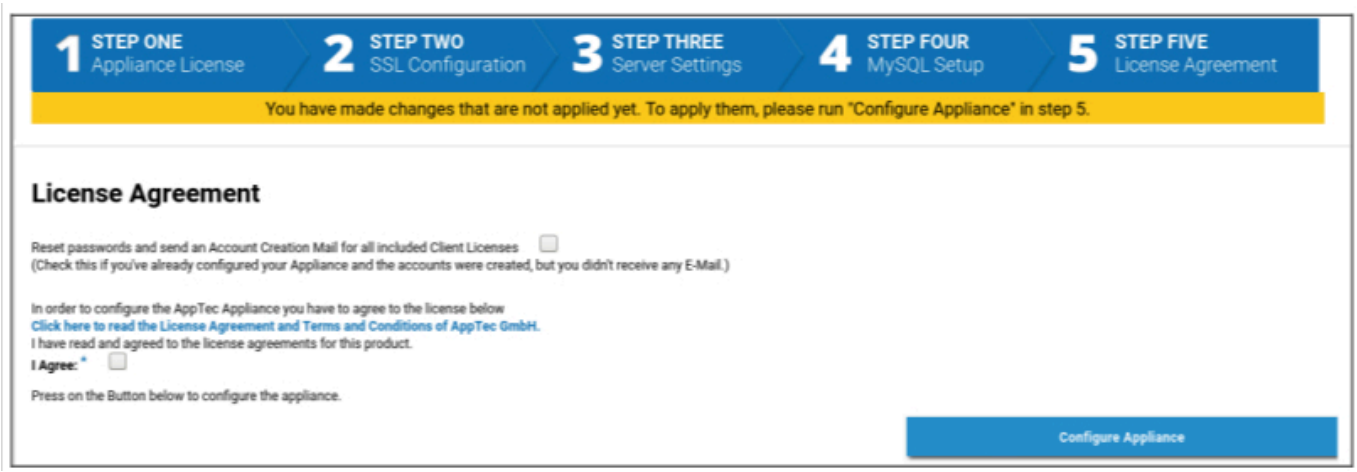
1. إذا كنت تريد استخدام قاعدة البيانات الداخلية يمكنك تخطي هذه الخطوة. وإلا يمكنك إدخال معلومات الاتصال لخادم قاعدة البيانات الخارجية.


1 STEP ONE Appliance License
2 STEP TWO SSL Configuration
3 STEP THREE Server Settings
4 STEP FOUR MySQL Setup
5 STEP FIVE License Agreement
You have made changes that are not applied yet. To apply them, please run "Configure Appliance" in step 5.
MySQL Setup
The MySQL connection has been successfully tested at April 7, 2021, 8:45 am.
If you change the settings after the initial configuration, you have to reconfigure your appliance by clicking on "Configure now" in step 5.
IP Address or Hostname
127.0.0.1
(Default: 127.0.0.1)
Username
AppTec
(Default: AppTec)
Password
(Default: AppTec)
Port
3306
(Default: 3306)

الخطوة الخامسة – اتفاقية الترخيص

1. يرجى قراءة اتفاقية الترخيص.
2. حدد "أوافق" واضغط على زر "تكوين الجهاز"، لتطبيق الإعدادات.

تلميح: ستحتاج إلى تشغيل "تكوين الجهاز" في كل مرة تقوم فيها بتغيير الإعدادات في الخطوات الخمس لتطبيق الإعدادات.



تهانينا!

لقد انتهيت من تكوين الجهاز الظاهري.

تم إرسال رسالة بريد إلكتروني تتضمن كلمة المرور الخاصة بك إلى العنوان الذي قدمته للحصول على الترخيص (تظهر في "تراخيص العميل المضمنة" في الخطوة الأولى - ترخيص الجهاز).

يمكنك الآن تسجيل الدخول إلى وحدة التحكم باستخدام كلمة المرور هذه وعنوان البريد الإلكتروني الذي استلمتها عليه.

لتسجيل الدخول إلى وحدة التحكم، يُرجى إدخال اسم المضيف لوحدة التحكم في شريط عنوان المتصفح.

يمكنك العثور على اسم المضيف الخاص بجهازك في الخطوة الأولى - ترخيص الجهاز.

استكشاف الأخطاء وإصلاحها

1. لم تتلق رسالة بريد إلكتروني عند تكوين الجهاز في الخطوة الخامسة - اتفاقية الترخيص:

تأكد من صحة إعدادات البريد الإلكتروني في الخطوة الثالثة - إعدادات الخادم. لإعادة إرسال كلمة المرور تحقق من "إعادة تعيين كلمات المرور وإرسال بريد إنشاء حساب لجميع تراخيص العميل المضمنة" في الخطوة الخامسة - اتفاقية الترخيص قبل تشغيل "تكوين الجهاز" مرة أخرى.

2. لقد تلقيت خطأً فيما يتعلق بـ Let's Encrypt أثناء التهيئة في الخطوة الخامسة - اتفاقية الترخيص:

تأكد من إمكانية الوصول إلى الجهاز من خلال اسم المجال الخاص به على المنفذ 80. يكتب برنامج Let's encrypt أيضًا سجلًا إلى "var/log/letsencrypt/" مما قد يساعد في استكشاف الأخطاء وإصلاحها.

التوصيات الأمنية

يوصى بتنفيذ الخطوات التالية لتأمين جهاز AppTec360 الخاص بك.

هذه ليست مجموعة كاملة من الإرشادات، إنها مجرد توصية لتكوين أساسي.

- تغيير كلمة المرور الخاصة بمستخدم AppTec360
- قم بتغيير كلمة المرور لمستخدمي "root MySQL"و "AppTec" وقم بتحديث الخطوة الرابعة - إعداد MySQL وفقًا لذلك
- تغيير منفذ خادم SSH الافتراضي
- قم بحظر المنفذ 80 في وحدة التحكم الخاصة بك وعدم السماح بحركة مرور HTTP الواردة، استخدم فقط HTTPS. بمجرد التهيئة، يمكن إجراء تكوين خارجي عبر HTTPS أيضًا.
- قم بتقييد الوصول إلى واجهة الإدارة على Ips معين فقط في أسفل الخطوة الثالثة - إعدادات الخادم
- تكوين جدار الحماية

الإعدادات العامة

نظرة عامة على الحساب

معلومات الحساب

لمحة عامة

هنا، يمكنك الاطلاع على نظرة عامة على حساب AppTec360 الخاص بك.

اسم الشركة	اسم شركتك
تاريخ الإنشاء	تاريخ إنشاء حسابك
نوع الترخيص	مدفوع = رخصة مدفوعة = رخصة مدفوعة مجاني = ترخيص غير مدفوع ملاحظة: ستظهر الحسابات الموجودة على جهاز OnPremise دائمًا على أنها مدفوعة لأسباب فنية
معرّف العميل	مُعرِّف حسابك (هذا ليس رقم العميل الخاص بك)
تاريخ انتهاء صلاحية الترخيص	تاريخ انتهاء صلاحية ترخيص AppTec360 الخاص بك
ترخيص صندوق المحتوى	مجاناً = ترخيص مجاني لـ 25 جهازاً مدفوع = ترخيص مدفوع لـ x جهاز
قاذفة	يوضح ما إذا كان يمكنك استخدام المشغل المخصص لنظام Android أم لا
الأجهزة	عدد التراخيص المستخدمة حالياً/إجمالي التراخيص
الاتصال بالشخص	جهة الاتصال المقدمة
الهاتف	رقم الهاتف المقدم
البريد الإلكتروني*	عنوان البريد الإلكتروني المقدم
المستخدم الجذر	المستخدمون الجذر القادرون على تسجيل الدخول
إصدار البرنامج	إصدار البرنامج الحالي

**ملاحظة: عنوان البريد الإلكتروني الموضح هنا هو عنوان البريد الإلكتروني الذي أدخلته لتسجيل الحساب. بناءً على هذا سيتم إنشاء مستخدم في شجرة المستخدم/الجهاز ويمكن تعديله. سيؤدي تعديل هذا المستخدم إلى تغيير عنوان البريد الإلكتروني الذي يجب عليك استخدامه لتسجيل الدخول ولكن ليس المعلومات الموجودة في النظرة العامة للحساب .*

تقرير الأخطاء

يمكن إرسال تقرير الأخطاء مباشرةً إلى الدعم للإبلاغ عن المشكلات أو الأخطاء ويتضمن معلومات وسجلات حول حسابك وإعدادك.

الموضوع	موضوع تقرير الخطأ. قم بتضمين رقم التذكرة إذا كنت تريد إضافة هذا إلى تذكرة دعم موجودة.
السلوك المتوقع	صِف بالتفصيل ما قمت به وما توقعت حدوثه
السلوك الفعلي	صف بالتفصيل ما حدث بالضبط. يرجى اقتباس رسائل الخطأ بالضبط. من المفيد أيضًا إضافة لقطات شاشة إلى المرفق.
في أي وقت واجهتك المشكلة؟	يُرجى تحديد الوقت الدقيق الذي تلقيت فيه رسالة/مشكلة محددة بالخطأ. في أفضل الأحوال تضمين الثواني أيضاً، على سبيل المثال 18:55:27
هل يمكن تكرار المشكلة؟ إذا كانت الإجابة بنعم، كيف (بالتفصيل)؟	صف كيف يمكنك إعادة إنتاج المشكلة بالتفصيل.
هل عملت هذه الميزة سابقاً كما توقعت؟ إذا كانت الإجابة بنعم، حتى متى؟	اتركها فارغة إذا كنت لا تعرف.
هل تم إجراء أي تغييرات محددة على النظام قبل ظهور هذه المشكلة؟ إذا كانت الإجابة بنعم، ما هي التغييرات (بالتفصيل)؟	اذكر دائمًا ما كان آخر تغيير أو إجراء قمت به قبل ظهور المشكلة، حتى لو كنت تعتقد أنه غير ذي صلة.
إذا كان ذلك ممكناً: ما هي طرازات الأجهزة وإصدارات نظام التشغيل المتأثرة؟	يرجى دائمًا تسمية إصدار نظام التشغيل بالضبط (على سبيل المثال iOS 14.7.1 أو Android 11)
إن أمكن: ما هو عنوان IP العام أو/و الرقم التسلسلي للجهاز؟	قم بتسمية جهاز واحد على الأقل، حتى لو كانت جميع الأجهزة متأثرة.
تضمين ملفات السجلات	تحقق من هذا لإرسال ملف السجل مع تقرير الخطأ. يوصى بذلك.
احضر حالة VPP الحالية من Apple وقم بتضمينها في تقرير الأخطاء	يتضمن معلومات حول تعيينات ترخيص VPP. لا تقم بتفعيل ذلك إلا إذا طلب منك الدعم القيام بذلك أو إذا كانت مشكلتك تتعلق بتعيين تراخيص VPP.
المرفقات	إرفاق أي ملف قد يكون مفيداً (مثل لقطات شاشة لرسالة خطأ)

طلب ميزة

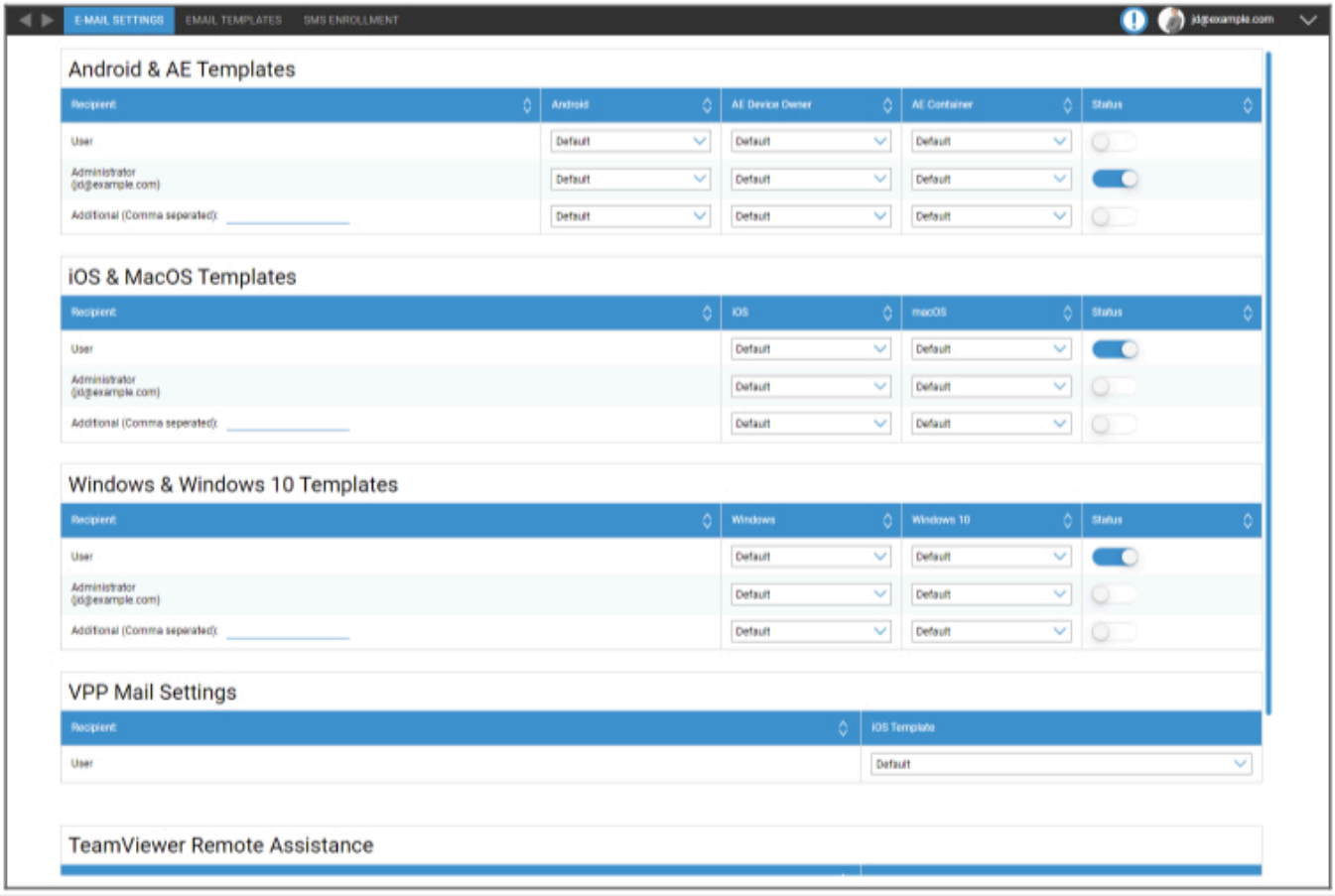
يمكن إرسال طلب ميزة مباشرةً إلى الدعم. يمكن أن يحتوي ذلك على طلب لميزة معينة أو تحسين ل

الملخص	نبذة مختصرة عن مشكلتك
الوصف	وصف تفصيلي لمشكلتك، يرجى التحديد قدر الإمكان
المرفقات	إرفاق الملفات بتقرير الأخطاء

التكوين العالمي

إعدادات البريد الإلكتروني

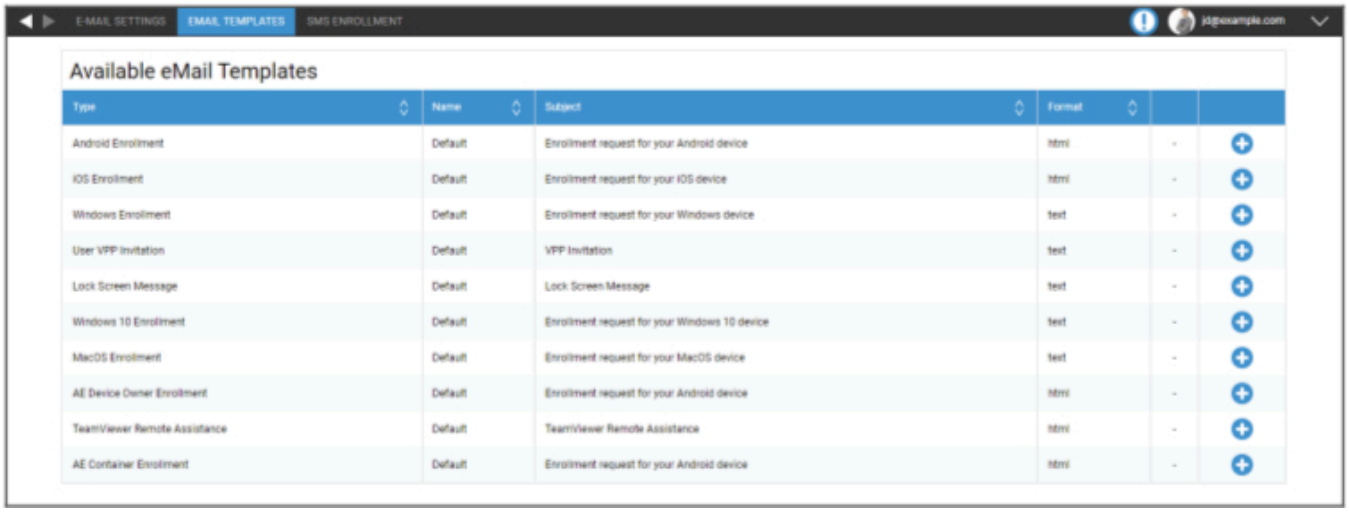
هنا يمكنك تحديد من الذي يحصل على بريد إلكتروني عند إنشاء طلب تسجيل والقالب النصي المستخدم لهذا البريد.



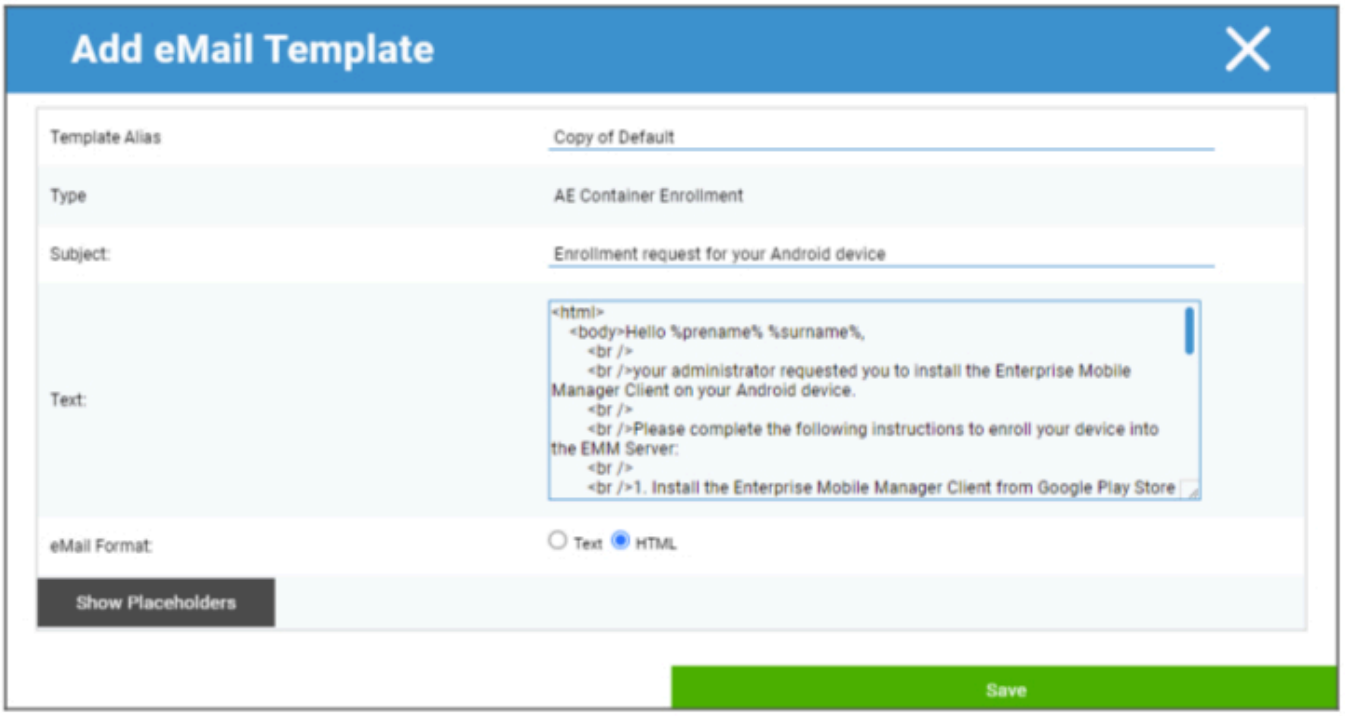
قوالب البريد الإلكتروني

هنا يمكنك إنشاء وتحرير القوالب الخاصة بك لسيناريوهات مختلفة. يمكن أن تكون في شكل نص عادي أو بتنسيق HTML. باستخدام HTML يمكنك التحكم بشكل أفضل في تنسيق النص الخاص بك.

لا يمكن تحرير القوالب الافتراضية أو مسحها.



يمكنك أيضًا استخدام العناصر النائبة كمتغير سيتم استبداله تلقائيًا. انقر على "إظهار العناصر النائبة" أثناء التحرير لرؤية العناصر النائبة المتاحة. الفئات المختلفة لها عناصر نائبة مختلفة.



التسجيل في الرسائل النصية القصيرة

هنا يمكنك إلغاء/تفعيل عملية التسجيل عبر الرسائل النصية القصيرة.

(افتراضي: معطل)

سترى أيضًا شاشة عرض تشير إلى عدد أرصدة الرسائل القصيرة التي لا تزال متاحة.

يجب شراء أرصدة الرسائل النصية القصيرة بشكل منفصل.

الخصوصية

الوصول إلى نظام تحديد المواقع العالمي (GPS)

هنا يمكنك حماية طريقة عرض GPS لكل جهاز باستخدام كلمة أو كلمتي مرور (مبدأ العيون الأربعة). ستتم مطالبتك بإدخال كلمة (كلمات) المرور الخاصة بك في كل مرة تحاول فيها الوصول إلى موقع الجهاز.

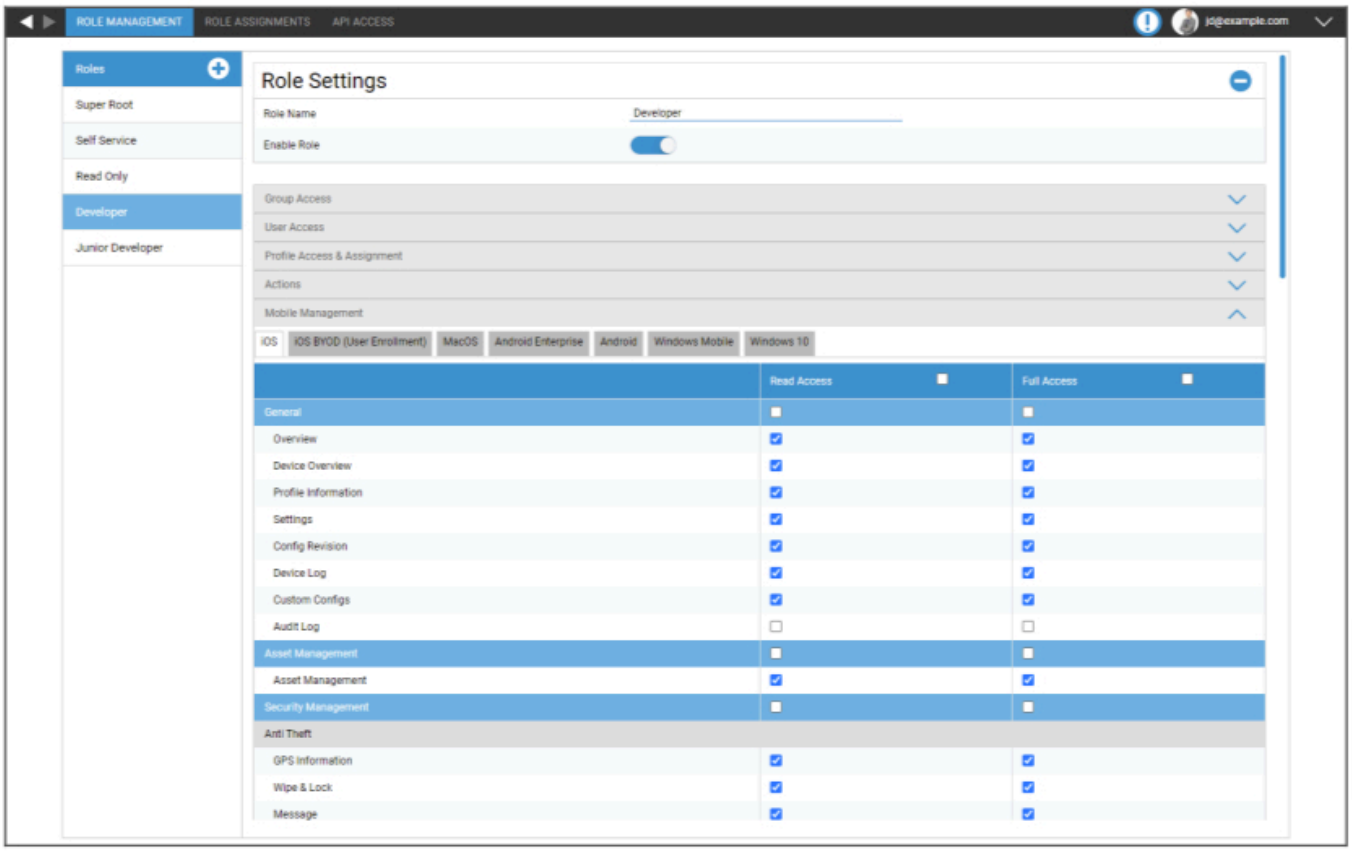
تقييد الوصول إلى إعدادات GPS	إيقاف التشغيل = الوظيفة متوقفة عن العمل ولا يلزم وجود كلمة مرور للتوطين
	تشغيل = الوظيفة قيد التشغيل ومطلوب كلمة مرور للتوطين
طريقة الحماية	استخدام كلمة مرور واحدة = استخدام كلمة مرور واحدة للتوطين
	استخدام كلمتي مرور = استخدام كلمتي مرور للتوطين
أدخل كلمة المرور (1)	أدخل كلمة المرور المختارة
تكرار كلمة المرور (1)	إعادة إدخال كلمة المرور المختارة
اختياري: أدخل كلمة المرور 2	أدخل كلمة المرور الثانية المختارة
اختياري: كرر كلمة المرور 2	إعادة إدخال كلمة المرور الثانية المختارة

ملاحظة: بعد تعيين رمز (رموز) المرور، عليك إدخاله مرة أخرى قبل أن يتم تمكينه بالكامل.

الوصول المستند إلى الدور

إدارة الأدوار

تحدد الأدوار ما يمكن للمستخدم رؤيته والقيام به عند تسجيل الدخول إلى وحدة تحكم الإدارة. هذا يسمح لك بإنشاء مستخدمين يمكنهم تسجيل الدخول ولكن لديهم وظائف محدودة.



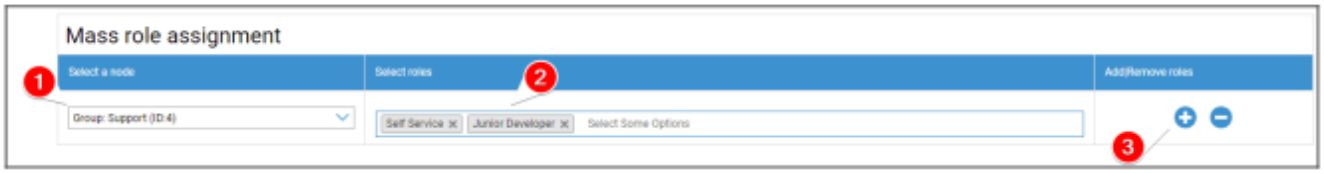
الدور الجذر الفائق هو الدور الافتراضي الذي يمكنه دائمًا رؤية كل شيء وتغييره. لا يمكن تغييره أو حذفه. دور الخدمة الذاتية قادر فقط على رؤية المستخدم والأجهزة الخاصة به. يمكنك الجمع بين الخدمة الذاتية والدور المخصص للسماح للمستخدمين على سبيل المثال بتسجيل الدخول وتسجيل الأجهزة بمفردهم ولمستخدمهم فقط.

يمكن تمكين الأدوار المخصصة يدوياً أو تعطيلها. يتم تعطيل الأدوار الجديدة بشكل افتراضي. يعمل المستخدمون الذين لديهم دور معطل كما لو لم يكن لديهم الدور. هذا يسمح لك على سبيل المثال بتقييد دور معين مؤقتًا من إجراءاتهم.

تنقسم جميع الأذونات بين "وصول للقراءة" و"وصول كامل". يتيح منح الدور صلاحية وصول للقراءة رؤية جزء معين من وحدة التحكم. يسمح منحهم حق الوصول الكامل للدور برؤية الجزء المحدد من وحدة التحكم وتغييره.

تعيينات الأدوار

هنا يمكنك الحصول على نظرة عامة على جميع المستخدمين الذين لديهم دور ومعرفة الدور الذي لديهم. يمكنك أيضًا تعيين دور لمستخدمين أو مجموعات كاملة هنا:

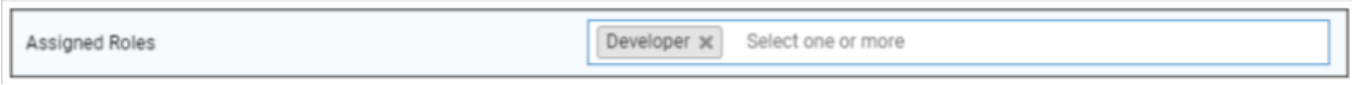


1. حدد المجموعة أو المستخدم الذي تريد إضافة أدوار أو إزالتها. يمكنك إما تحديد مستخدم واحد أو تحديد مجموعة. عند تحديد مجموعة، سيؤثر تغييرك على جميع المستخدمين داخل تلك المجموعة وجميع مستخدمي المجموعات الفرعية ضمن المجموعة المحددة.
2. حدد الدور الذي تريد إضافته أو إزالته. يمكنك تحديد دور واحد أو عدة أدوار.
3. Select what operation you want to perform. Clicking the “+” adds the selected roles if the user(s) did not have them already. Clicking the “-” removes the selected roles from the user(s). If you add roles to a user which did not yet have any role, it will automatically enable “Can Login” for the user.
4. حفظ لإنهاء العملية. سيتلقى المستخدمون الذين لم يكن لديهم دور في السابق وتم تعطيل "إمكانية تسجيل الدخول" تلقائيًا رسالة بريد إلكتروني تحتوي على رابط لتعيين كلمة مرور.

أسفل تعيين الأدوار الجماعية يمكنك العثور على نظرة عامة على الأدوار المعينة. يمكنك أيضًا تغيير الأدوار يدويًا هناك لمستخدمين محددين.

تعيين دور

لتعيين دور لمستخدم، عليك الانتقال إلى إدارة الأجهزة المحمولة، حيث تجد شجرة المجموعات والمستخدمين والأجهزة الخاصة بك. قم بتحرير المستخدم لتعيين دور. بدلاً من ذلك يمكنك استخدام الطريقة المذكورة أعلاه للمستخدمين الفرديين فقط أيضًا.



الوصول إلى واجهة برمجة التطبيقات

الوصول إلى واجهة برمجة تطبيقات AppTec360 REST API

تتطلب واجهة برمجة تطبيقات AppTec360 REST API رمزًا مميزًا للمصادقة (مفتاح واجهة برمجة التطبيقات) ومفتاحًا خاصًا يجب إنشاؤه في وحدة التحكم في الإدارة.

للقيام بذلك قم بتسجيل الدخول إلى AppTec360 EMM وانتقل إلى

الإعدادات العامة → الوصول المستند إلى الدور → الوصول إلى واجهة برمجة التطبيقات وإضافة مفتاح جديد.

عليك تحديد المستخدم الذي سيتم تطبيق أذوناته على مفتاح API.

يمكن تنزيل المفتاح الخاص مرة واحدة فقط. بعد بدء التنزيل سيتم حذف المفتاح، ويختفي زر "تنزيل".

إذا فقدت مفتاحك الخاص فعليك إنشاء مفتاح API جديد.

القواعد العامة

- تتوفر واجهة برمجة تطبيقات REST API أسفل عنوان URL الأساسي:

public/external/api/

- يجب إرسال جميع الطلبات عبر POST.
- تدعم واجهة برمجة تطبيقات REST API الطلبات عبر HTTPS فقط.
- يجب أن تحتوي الطلبات على العناوين التالية:

اسم العنوان	قيمة الرأس	الوصف
نوع المحتوى	تطبيق/جسون	ثابت
المصادقة	xyz...123	مفتاح API من علامة التبويب "الوصول إلى واجهة برمجة التطبيقات"
توقيع	توقيع مشفر Base64	توقيع الحمولة التي تم إنشاؤها باستخدام مفتاح خاص من علامة التبويب "الوصول إلى واجهة برمجة التطبيقات"

- يجب أن يكون نص الطلب كائن مشفر json يجب أن يحتوي على القيم التالية:

الحقل	قيمة مثال الحقل	الوصف
واجهة برمجة التطبيقات (api)	الإصدار2/الجهاز/قائمة الأجهزة	اسم واجهة برمجة التطبيقات
الوقت	1529662725	الطابع الزمني لنظام Unix (UTC) لجهاز العميل. الحد الأقصى للفرق الزمني المسموح به بين العميل والخادم هو 30 الدقائق.

- عند النجاح، تقوم واجهة برمجة التطبيقات بإرجاع البيانات المطلوبة (انظر الاستعلامات أدناه) ورمز حالة HTTP 200.
- في حالة حدوث خطأ، سيتراوح رمز حالة HTTP بين 4xx و5xx اعتمادًا على الخطأ وسيحتوي كائن الاستجابة على مصفوفة بمفتاح "أخطاء"، والذي يحتوي على قائمة برسائل الخطأ التي يمكن قراءتها من قبل البشر.
- إذا لم تكن هناك بيانات مطابقة لجهاز ما سيتم إرجاع مصفوفة فارغة.
- إذا كان معرّف الجهاز غير موجود، فستكون بيانات الإرجاع لاغية.

مثال على الطلب

```
POST /public/external/api HTTP/1.1
Host: myapptecemm.com
/ :Accept
Content-Type: application/jsonauth: 1234567890abcdefghijklmnopqrstuvwxyz
signature: a/bnOV466a0SiyVfsbpspZ+NxiTpmeF18NkfnOIq+OrEZDu9+VW7ESKziPXvw
kTM5B9j/t1WGN1mRcIKe80m8fDKPj+lr3BqoMJe7wGXift+uy6iS7Chpdz2iZA4KPxxU9Z
/GU2cdQ/SQceX57pi+ch7ApxBeVX2+lJapTwA6CfB0mJFaf4MPcg
7LZWkzKxKF7LNzNJHiy/vSpZcqjbXjpC4HWrX6j2uZG5eSP8kYcTR
+9VQfGtkX9pcyaNAwguR7zOOwMu/8L0oKq21/19rkabE4ZgUjtKS2
q+rh6mrP1g4BCZ7Xq/wvgZkaP+
==b0CStBdMRvj46i3enxCXcLQQ
Content-Length: 74
{api":"v2/device/listposition","time":1529665112,"params":{"ids": [10]}"}
```

الاستفسارات

قائمة بجميع الأجهزة

الوظيفة: إرجاع قائمة بجميع الأجهزة التي تحتوي على معرف الجهاز و IMEI و المسلسل
URI API: v2/device/listdevices
المعلمات الإلزامية: لا شيء
المعلمات الاختيارية: لا شيء

مثال على نص الطلب

}
","api": "v2/device/listdevices"
time": 1529662725"
{

مثال على نص الاستجابة

}
,[] :"errors"
]:"list"
,{"id":"10","serial":"987612345","imei":"899938455454" }
{"id":"11","serial":"619723118","imei":"713032378599" }
[
{

الحصول على قائمة بمواقع (GPS)

الوظيفة: إرجاع قائمة بجميع إدخالات سجل المواقع المخزنة لمعرفات الأجهزة
URI لواجهة برمجة التطبيقات: v2/device/listposition
معلمات إلزامية: "المعرفات" - مصفوفة معرفات الأجهزة
المعلمات الاختيارية: لا يوجد

مثال على نص الطلب

}
","api": "device/listposition"
} :"params"
ids": [10, 11]"
,{
time": 1529662725"
{

مثال على نص الاستجابة

}
,[] :"errors"
]:"list"
]:"10"
{"time":"1529632725","pos":"47.5572,7.5967"},
{"time":"1529642725","pos":"47.5572,7.5968"},
{"time":"1529652725","pos":"47.5573,7.5969"},
,[
,[]:"88"
[
{

الحصول على خريطة الأصول

الوظيفة:
إرجاع قائمة بجميع الأصول المحتملة المخزنة التي يمكن طلبها باستخدام الحصول على أي بيانات أصول.
يمكنك إما استخدام النموذج المقروء بشريًا أو علامة الأصول لطلب البيانات.
URI لواجهة برمجة التطبيقات: v2/device/getassetmap
المعلمات الإلزامية: لا شيء
المعلمات الاختيارية: لا شيء

مثال على نص الطلب

}
,"api": "v2/device/getassetmap"
time": 1529662725"
{

مثال على نص الاستجابة

تم اختصار هذا الرد لسهولة قراءته.

}
} :"AssetKeys"
,"UDID": "AT001"
,"Device Alias": "AT002"
,"OS Version WinMobile iOS MacOS": "AT003"
,"Model Name": "AT004"
,"Serial Number": "AT005"
,"Total Storage": "AT006"
,"Free Storage": "AT007"
,"IMEI": "AT008"
…
"apptecID": "APPTECID"
,{
[] :"errors"
{

الحصول على أي بيانات الأصول

الوظيفة: إرجاع قائمة ببيانات الأصول المطلوبة لمعرّفات الأجهزة
URI لواجهة برمجة التطبيقات: v2/device/getetassetdata
معلمات إلزامية: "المعرفات" - مصفوفة معرفات الأجهزة
المعلمات الاختيارية:
"مفاتيح الأصول" - مفاتيح بيانات الأصول المطلوب إرجاعها. إذا لم يتم تحديدها سيتم إرجاع جميع بيانات الأصول المتاحة
. يمكنك الحصول على قائمة بمفاتيح الأصول باستخدام الحصول على خريطة الأصول.

مثال على نص الطلب

}
,"api": "v2/device/getassetdata"
,time": 1529662725"
} :"params"
] :"ids"
26
,[
] :"assetkeys"
"imei"
[
{
{

مثال على نص الاستجابة

}
} :"result"
} :"26"
”imei": "349157642516427"
{
,{
[] :"errors"
{

مثال على كود برمجي في بايثون3

```
usr/bin/python/ !
import base64
from Crypto.Hash import SHA512
from Crypto.Signature import PKCS1_v1_5
from Crypto.PublicKey import RSA
import os
import time
import json
import urllib.request
import urllib.parse
import urllib.error
import http.client
"applianceDomain = "YOURAPPLIANCE.COM
"apiURL = "https://"+applianceDomain+"/public/external/api
"privateKeyPath = "/path/to/PrivateKey-XXXXXXXXXXX.pem
"apptecAPIAuthToken = "7eXXXXXXXXXXXXXXXXXXXXXXXXXXX20
currentTimestamp = int(time.time())
Get Devices #
requestData = {"api": "v2/device/listdevices", "time": currentTimestamp}#
Get Positions #
,requestData = {"api": "v2/device/listposition", "time": currentTimestamp#
{params":{"ids":[26]}"
Get AssetData #
,requestData = {"api": "v2/device/getassetdata", "time": currentTimestamp
{params":{"ids":[26], "assetkeys": ["imei"]}"
encode the request data to json #
print(json.dumps(requestData, indent=1))
jsonEncodedRequestData = json.dumps(requestData)
Sign the request data json with the API private key #
message = jsonEncodedRequestData.encode('utf-8')
print("Body:", message)
()digest = SHA512.new
digest.update(message)
```

```
Read private key from file #
:with open(privateKeyPath, "r") as myKeyFile
private_key = RSA.importKey(myKeyFile.read())
```

```
Load private key and sign message #
signer = PKCS1_v1_5.new(private_key)
signatureOfRequestData = signer.sign(digest)
)Base64EncodedSignature = base64.b64encode
signatureOfRequestData).decode("utf-8")

,"headers = {"Content-type": "application/json
{auth": apptecAPIAuthToken, "signature": Base64EncodedSignature"
print("Headers:", headers, "\n")

Send request to Server #
httpsClient = http.client.HTTPSConnection(applianceDomain, 443, timeout=10)
httpsClient.request("POST", apiURL, jsonEncodedRequestData, headers)

Get answer #
()response = httpsClient.getresponse
status = response.status
()data = response.read

:if data == False
print("Invalid answer from the server")
:else
print("Answer:")
print(json.dumps(json.loads(data), indent=1))
:if status != 200
print("http error: lastReceivedHttpCode")
print(status)
```

تكوين التفاح

شهادة APNS

هنا يمكنك تحميل شهادة APNS. هذا مطلوب لإدارة أجهزة iOS و MacOS.

ملاحظة: شهادة APNS صالحة لمدة عام واحد فقط. يجب تجديدها قبل انتهاء صلاحيتها. عملية التجديد مطابقة لعملية الإنشاء (انظر أدناه) ولا تستغرق سوى بضع دقائق قصيرة.

إذا نسيت تجديدها في الوقت المناسب، فلن تتمكن من إجراء تغييرات على أجهزتك المسجلة بالفعل **ويجب عليك تسجيل جميع الأجهزة مرة أخرى**.

الخطوة 1

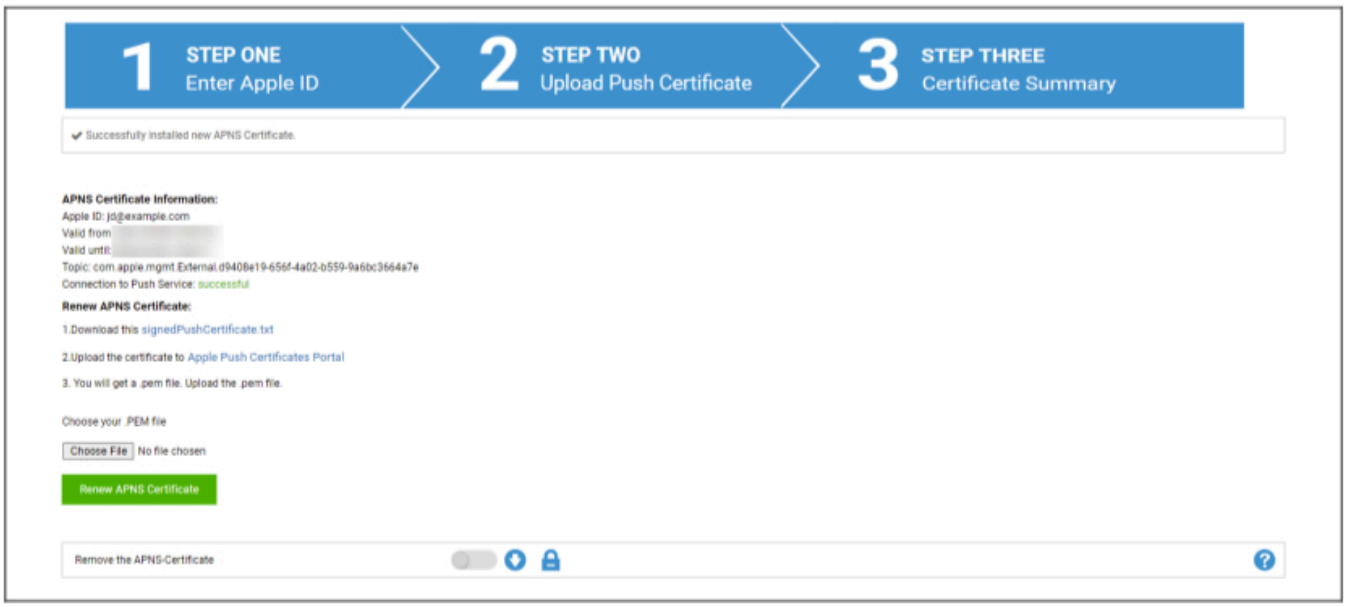
- أولاً، أدخل معرف Apple الذي تريد استخدامه لإنشاء شهادة APNS.

ملاحظة: يتم استخدام معرف Apple هذا فقط لإنشاء شهادة APNS. لا علاقة لمعرف Apple هذا بالأجهزة ولن تعرف الأجهزة عن معرف Apple هذا. بالإضافة إلى ذلك، تحتاج أيضًا إلى الوصول إلى معرف Apple هذا لتجديد شهادة APNS. لذلك يوصى باستخدام معرف Apple عام وتوثيق بيانات تسجيل الدخول. يتم إرسال تذكير إلى عنوان البريد المستخدم لمعرف Apple ID قبل انتهاء صلاحية شهادة APNS.

- انقر على "الخطوة التالية" للمتابعة.
- (اختياري) يمكنك أيضًا استعادة شهادة APNS المحذوفة مسبقًا إذا قمت بحذفها عن طريق الخطأ

الخطوة 2

- قم بتنزيل ملف signaturePushCertificate.txt الموقّع
- انتقل إلى https://identity.apple.com/pushcert/ وقم بتسجيل الدخول باستخدام معرف Apple من الخطوة 1
- انقر على "إنشاء شهادة"
- (اختياري) أدخل ملاحظة. يمكن أن يكون هذا مفيداً إذا كنت تدير عدة مستأجرين للتعرف عليهم بسهولة.
- انقر فوق "اختيار ملف" لتحديد ملف موقّعPushCertificate.txt الذي تم تنزيله مسبقًا
- انقر على "تحميل".
- سترى الآن التأكيد على أنك قمت بإنشاء شهادة APNS.
- انقر على "تنزيل" واحفظه.
- ارجع إلى وحدة تحكم الإدارة.
- انقر على "اختيار ملف" وحدد شهادة APNS التي تريد تحميلها.
- انقر على "تحميل"



الخطوة 3

لقد قمت الآن بإعداد شهادة APNS بنجاح ويمكنك الآن إدارة أجهزة iOS و MacOS.

في الخطوة 3 سترى في الخطوة 3 نظرة عامة على شهادة APNS المستخدمة حالياً.

لديك أيضًا خيار تجديد شهادة APNS باتباع الخطوات الموضحة على الشاشة. ضع في اعتبارك تجديدها قبل انتهاء صلاحيتها.

عند تجديد شهادة APNS، ضع في اعتبارك تسجيل الدخول باستخدام معرّف Apple الموضح في الخطوة 3 وكذلك تجديد الشهادة المستخدمة سابقاً وليس إنشاء شهادة جديدة. سترى "موضوع" شهادة APNS في الخطوة 3 وعند النقر على "i" في بوابة شهادة Apple Push Portal. هذا هو المعرف الفريد الذي يحدد الشهادة. سيساعدك هذا على تحديد الصحيح وتجديد الصحيح.

عندما تحصل على "خطأ: شهادة الدفع لها موضوع مختلف!" أثناء التجديد، فهذا يعني أنك قمت بتجديد شهادة أخرى أو قمت بإنشاء شهادة جديدة.

إذا كنت ترغب في تحميل شهادة جديدة، على سبيل المثال إذا لم يعد بإمكانك الوصول إلى معرف Apple المستخدم سابقاً، فعليك أولاً حذف الشهادة التي تم تحميلها حالياً.

على أي حال، يعني حذف شهادة APNS أنه لم يعد بإمكانك إجراء تغييرات للأجهزة المسجلة حاليًا حتى تقوم بتسجيلها مرة أخرى. لذا تأكد من أنك مستعد لذلك ولا تحذف الشهادة إلا إذا لم تكن هناك طريقة أخرى.

الوصول المُدار

هنا يمكنك تمكين تسجيل المستخدم لأجهزة iOS وأجهزة iPad المشتركة لأجهزة iOS.

تسجيل المستخدم

يتيح "تسجيل المستخدم" وضعاً خاصاً لأجهزة BYOD.

يجب إنشاء معرّف Apple مُدار لكل مستخدم في بوابة Apple Business Portal.

أثناء عملية التسجيل، سيُطلب من المستخدمين تقديم بيانات اعتماد Apple-ID الخاصة بهم.

يضمن "تسجيل المستخدم" أقصى درجات الأمان للمستخدم لأنه لا يسمح إلا بمجموعة محدودة من الإعدادات والقيود التي يمكن تهيئتها بواسطة جهاز إدارة الأجهزة المتعددة الوسائط.

المجال المُدار:

المجال المستخدم لتعيين عنوان البريد الإلكتروني للمستخدم إلى معرف Apple المُدار الخاص به (يجب أن يكون بصيغة: '@appleid.company.com').على سبيل المثال: john.doe@example.com سيتم تعيينه إلى john.doe@appleid.company.com

تحقق من "مدير أعمال Apple" لمعرفة المجال المُدار الخاص بك

جهاز iPad مشترك

جهاز iPad المشترك هو جهاز DEP مهيأ بملف تعريف DEP خاص.

يتيح ذلك لعدة مستخدمين تسجيل الدخول إلى الجهاز باستخدام معرف Apple المُدار الخاص بهم.

يجب إنشاء معرف Apple المُدار في Apple Business Portal أو Apple School Manager.

يُطلب من المستخدمين، الذين يقومون بتسجيل الدخول إلى جهاز iPad مشترك، تقديم بيانات اعتماد Apple-ID المدارة الخاصة بهم.

المجال المُدار:

المجال المستخدم لتعيين عنوان البريد الإلكتروني للمستخدم إلى معرف Apple المُدار الخاص به (يجب أن يكون بصيغة: '@appleid.company.com').على سبيل المثال: john.doe@example.com سيتم تعيينه إلى john.doe@appleid.company.com

تحقق من "مدير أعمال Apple" لمعرفة المجال المُدار الخاص بك

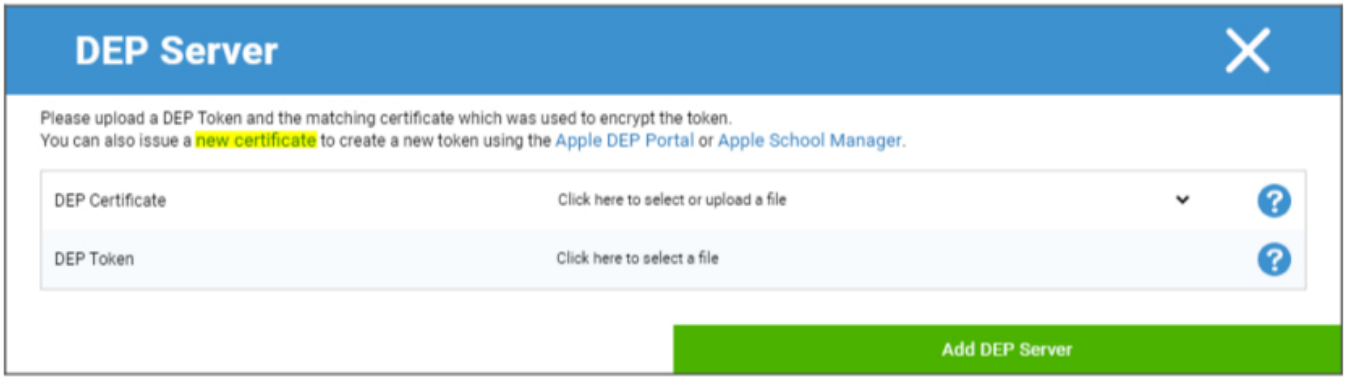
ديب

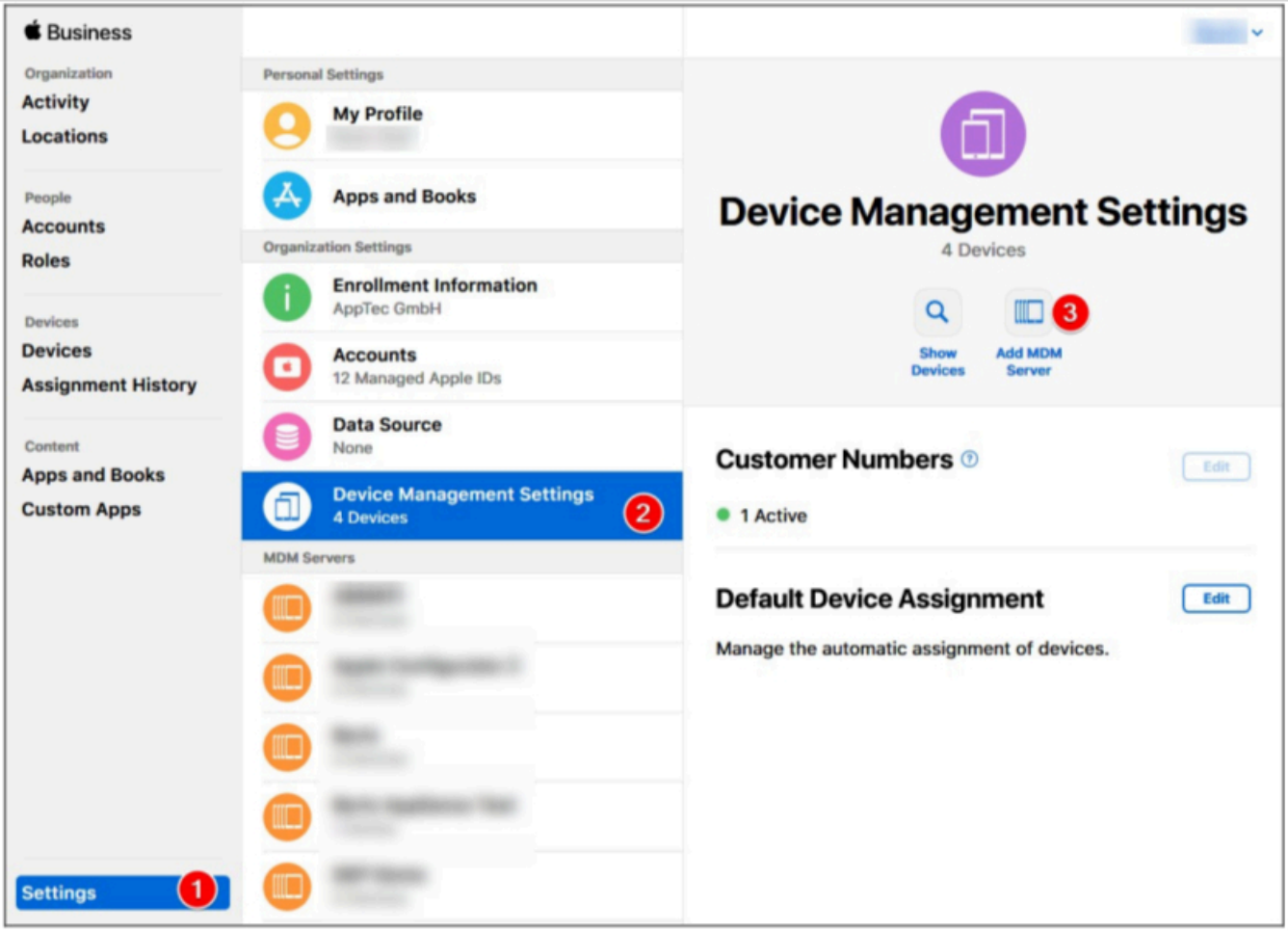
يتيح لك DEP (برنامج تسجيل الأجهزة) تسجيل الأجهزة بسهولة في MDM. عند استخدام برنامج DEP، سيتم توصيل الأجهزة تلقائيًا ببرنامج MDM عند إعداد الجهاز. يمكنك أيضًا تخطي جميع خطوات الإعداد تقريبًا والتي عادةً ما تكون إلزامية على نظام iOS.

ضع في اعتبارك أنك بحاجة إلى شراء الأجهزة من بائع يدعم DEP. لمزيد من المعلومات، اتصل بالبائع أو بشركة Apple.

مزيد من المعلومات حول DEP: https://www.apple.com/business/dep/

انقر على "+" لإضافة رمز DEP Token. في النافذة المنبثقة، انقر على "شهادة جديدة" في النص (المميز باللون الأصفر في الصورة أدناه). سيؤدي ذلك إلى إنشاء شهادة DEP وتنزيلها. بعد ذلك انتقل إلى Apple Business Manager(https://business.apple.com/) أو Apple School Manager(https://school.apple.com/).

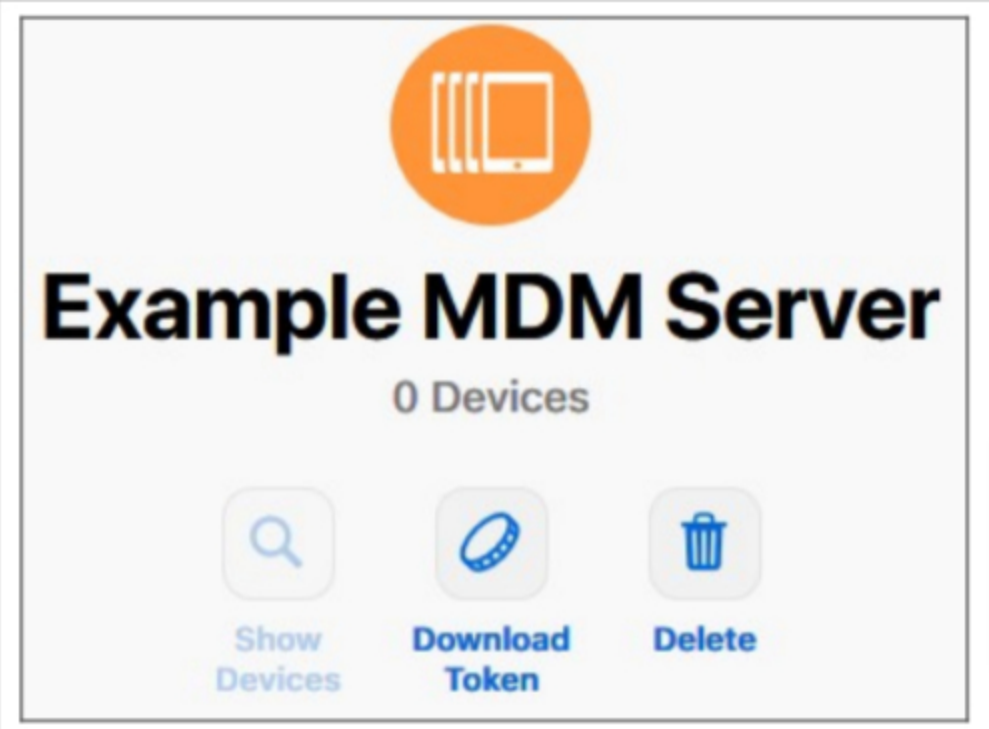




في مدير أعمال Apple Business Manager، اتبع الخطوات كما هو موضح في الصورة أعلاه. الإعدادات ← إعدادات إدارة الجهاز ← إضافة خادم MDM.

امنح الخادم أي اسم تريده وقم بتحميل شهادة DEP التي تم تنزيلها مسبقًا ضمن إعدادات خادم MDM → تحميل المفتاح العام وانقر على "حفظ".

سيكون لديك الآن خيار "تنزيل الرمز المميز". انقر على هذا الخيار واحفظه. الرمز المميز صالح لمدة عام واحد فقط. ولكن مجرد النقر على "تنزيل الرمز المميز" مرة أخرى، سيمنحك رمزًا جديدًا، مما يجعل تجديد الرمز المميز أمرًا سهلاً للغاية.



يمكنك الآن العودة إلى MDM، حيث قمت بتنزيل شهادة DEP مسبقاً. إذا لم تقم بإغلاق علامة التبويب، يجب أن تظل النافذة المنبثقة لإضافة خادم DEP مفتوحة ويجب أن تكون شهادة DEP محددة بالفعل. يمكنك الآن تحميل الرمز المميز في الحقل "رمز DEP Token" والنقر على خادم DEP.

في العمود "**الأجهزة**" سترى كمية الأجهزة التي تم تعيينها لخادم DEP هذا. سيتم إنشاء الأجهزة التي تمت إضافتها إلى خادم DEP هذا تلقائيًا في تجمع DEP في إدارة الأجهزة المحمولة.

يمكنك النقر على هذا الرقم للحصول على نظرة عامة على جميع أجهزة DEP وحالتها.

ملاحظة: استناداً إلى سير العمل أو التكوين في "مدير الأعمال"، قد يكون من الممكن أن تضطر إلى تعيين هذه الأجهزة يدوياً إلى خادم DEP Server. يمكنك أيضاً تعيين خادم DEP افتراضي في Apple Business Manager للأجهزة الجديدة.

في العمود "**ملفاتالتعريف**" ترى عدد ملفات تعريف DEP لديك. يمكنك أيضًا النقر على هذا الرقم للاطلاع على تفاصيل حول ملفات تعريف DEP الخاصة بك ويمكنك حذف ملفات التعريف القديمة/غير المستخدمة هنا. لا يمكن تغييرها حالياً. إذا أردت إجراء تغيير، فعليك إنشاء ملف تعريف جديد.

في العمود "**آخر مزامنة**"، يمكنك مزامنة خادم DEP يدويًا (على سبيل المثال إذا أضفت للتو جهازًا جديدًا إلى DEP) والاطلاع على تاريخ آخر مزامنة ناجحة.

في العمود "**ملف تعريف تلقائي**" يمكنك تعيين ملف تعريف DEP كملف تعريف تلقائي افتراضي. سيتم تعيين ملف التعريف هذا تلقائياً للأجهزة الجديدة. إذا لم تقم بتعيين ملف التعريف التلقائي، فسيتعين عليك تعيين ملف تعريف يدوياً للأجهزة الجديدة في كل مرة.

في العمود "**إضافة ملف تعريف**" يمكنك إضافة ملف تعريف DEP جديد. سيتلقى الجهاز هذا في بداية إعداد الجهاز. يحدد ملف تعريف DEP كيفية إعداد الجهاز وخطوات الإعداد التي سيتم تخطيها.

ملاحظة: بعد تسجيل الجهاز، لا يمكن تغيير هذه الإعدادات إلا من خلال إجراء إعادة ضبط المصنع وتسجيل الجهاز بملف تعريف جديد. هذا ينطبق بشكل خاص على "**قابل للإزالة**" و"**السماح بالاقتران**". في حالة "**السماح بالاقتران**"، يوصى بتشغيل "**السماح**بالاقتران"، حيث يمكن تعطيله عبر قيود MDM، ولكن لا يمكن تمكينه مرة أخرى إذا تم تعطيله في ملف تعريف DEP.

في العمود "**تعديل**" يمكنك تحميل رمز مميز جديد، على سبيل المثال عند تجديد الرمز المميز.

المهيئ وعنوان URL

عناوين URL للتسجيل في المجمع

هنا يمكنك إنشاء عنوان URL للتسجيل ورمز QR للتسجيل صالح لفترة محددة من التسجيل وحتى تاريخ محدد. وهذا يسمح لك بتسجيل أجهزة متعددة برابط واحد أو رمز QR واحد فقط.

ستكون الأجهزة المسجّلة باستخدام عنوان URL أو رمز الاستجابة السريعة هذا في تجمّع الأجهزة في إدارة الأجهزة المحمولة وعليك تعيينها يدويًا إلى مجموعة أو مستخدم بعد ذلك.

ملاحظة: هذا فقط للتسجيل اليدوي. لا تستخدم عنوان URL هذا إذا قمت بتسجيل الأجهزة عبر Apple Configurator

ملف تعريف MDM – مهيئ Apple

هنا يمكنك الحصول على عنوان URL الذي تحتاجه عند تسجيل الأجهزة عبر Apple Configurator. أثناء إعداد الأجهزة باستخدام أداة Apple Configurator، يمكنك إضافة الأجهزة إلى MDM في نفس العملية. تتطلب أداة Apple Configurator عنوان URL هذا لهذا الغرض.

ستكون الأجهزة المضافة عبر أداة Apple Configurator في تجمّع الأجهزة في إدارة الأجهزة المحمولة وعليك تعيينها يدويًا إلى مجموعة أو مستخدم بعد ذلك.

ستجد أيضًا ملف .mobileconfig هنا والذي يمكن استخدامه لتسجيل الأجهزة عبر Apple Configurator. على أي حال يوصى باستخدام عنوان URL.

تهيئة أندرويد

تهيئة أندرويد

إلغاء تثبيت الحماية	إذا تم تنشيط هذه الوظيفة، لا يمكن للمستخدم إلغاء تنشيط مسؤول الجهاز، دون إدخال كلمة المرور التي تم تعيينها من قبل مسؤول MDM. يتم تعيين كلمة المرور أثناء التسجيل، لذا يجب إعادة تسجيل الأجهزة لتحديث كلمة المرور. هناك خياران لإزالة مسؤولي الجهاز: 1. يدوياً على الجهاز ○ افتح تطبيق EMM على الجهاز ○ التبديل إلى علامة التبويب الحالة ○ اضغط على "إلغاء تثبيت الحماية" ○ أدخل كلمة المرور يمكنك استخدام المراجعة للحصول على كلمة المرور الصحيحة من "سجل كلمات المرور" في وحدة التحكم. ○ قم بالتمرير لأسفل وانقر على النقطة المضافة حديثًا، "انقر لإلغاء تثبيت تطبيق AppTec360 MDM" (لديك 20 ثانية لتنفيذ هذه المهمة) ○ قم بتأكيد الحوار "إلغاء تثبيت تطبيق AppTec360 MDM" بـ "موافق". سيؤدي ذلك إلى إلغاء تسجيل الجهاز من وحدة التحكم. ○ لإزالة التطبيق من الجهاز، قم بتأكيد الحوار "سيتم إلغاء تثبيت تطبيق AppTec360 MDM" باستخدام "UNINSTALL" 2. التلقائي (وحدة التحكم) ○ حدد الجهاز في وحدة التحكم ○ انقر على أيقونة الترس الأزرق واختر "مسح المؤسسة" ملاحظة: متوفر فقط مع نظام Android 4.x والإصدارات الأقل أو على الأجهزة المزودة بواجهة برمجة تطبيقات KNOX (أجهزة سامسونج)
إلغاء تثبيت كلمة المرور (المراجعة x)	كلمة المرور المحددة، والتي يمكن للمستخدم من خلالها إزالة مسؤول الجهاز

	المراجعة x = عداد، عدد المرات التي تم فيها تغيير كلمة المرور بالفعل من المهم كلمة المرور التي يحتاجها المستخدم، لأنه من المحتمل أن الجهاز لم يتصل بخادم AppTec360 وبالتالي لم يتم إرسال أحدث كلمة مرور بعد
سجل كلمات المرور	عند النقر على الزر الأزرق ("إظهار السجل")، يمكنك عرض كلمات المرور التي تم إنشاؤها مسبقًا
الحماية الموسعة لإلغاء التثبيت	يوفر هذا الخيار الحماية ضد الأجهزة غير الآمنة وطالما أن هذا الإعداد مفعل، فلا يمكن إلغاء تنشيط مسؤول الجهاز بسهولة
مطالبة المستخدم بإلغاء تثبيت التطبيقات المحظورة؟	إذا أمكن، لن يتم حظر التطبيقات المحظورة فحسب، بل سيتم إلغاء تثبيتها تلقائيًا أيضًا. سيُطلب من المستخدم إلغاء تثبيت التطبيقات المحظورة إذا لم يكن إلغاء التثبيت التلقائي ممكنًا.
حظر تطبيقات النظام الذكي	إذا تم تمكين القائمة البيضاء، يقوم عميل Android MDM بحظر جميع التطبيقات المثبتة من قبل المستخدم. قم بتمكين هذا الإعداد لحظر جميع تطبيقات النظام القابلة للتشغيل في وضع القائمة البيضاء.

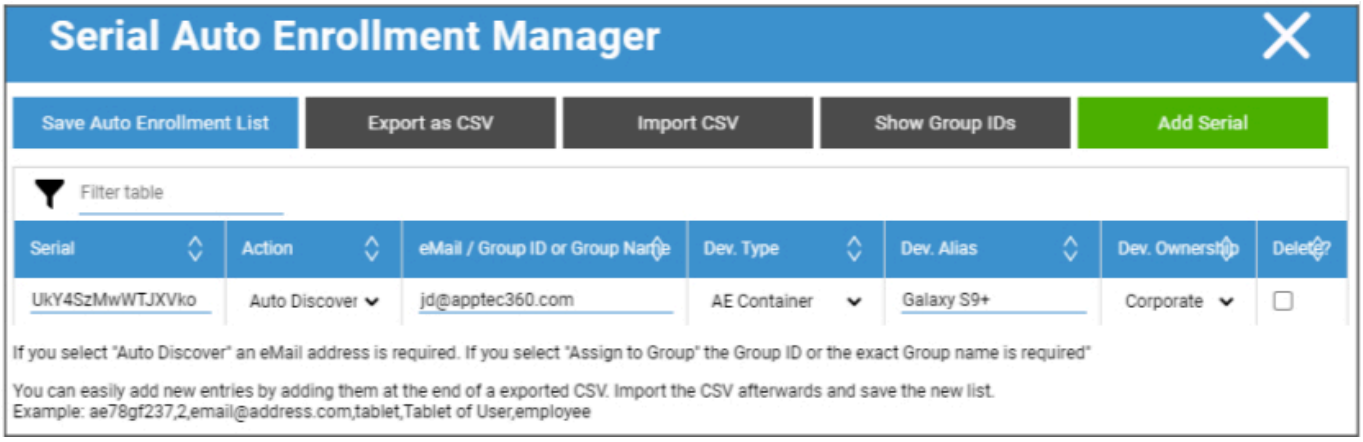
التسجيل التلقائي

يمكنك هنا تمكين ميزة التسجيل التلقائي لتسجيل أجهزتك تلقائياً عند فتح عميل AppTec360 MDM على الجهاز.

هام: طريقة التسجيل هذه مهملة ولم تعد تعمل على أندرويد 10 أو أعلى. على أي حال، عند استخدام Android 7 أو أعلى، يجب عليك تسجيل الأجهزة على أي حال على نظام Android Enterprise المُدار بالكامل. إذا كنت ترغب في استخدام حاوية Android Enterprise BYOD وكنت تستخدم Android 10 أو أعلى، فيجب عليك تسجيل الجهاز يدويًا عبر بيانات الاعتماد أو رمز الاستجابة السريعة أو الرسائل النصية القصيرة. على أي حال، لا يزال يتم استخدام قائمة التسجيل التلقائي لأتمتة عملية التسجيل على سبيل المثال تسجيل AE، وتسجيل Knox، وما إلى ذلك.

على أي حال، لا يزال يتم استخدام قائمة التسجيل التلقائي لأتمتة عملية التسجيل على سبيل المثال تسجيل AE، وتسجيل نوكس، وما إلى ذلك.

من خلال النقر على "Serial Manager" أو "IMEI Manager" يمكنك إضافة الرقم التسلسلي أو IMEI لأجهزتك على التوالي. ليس مطلوبًا القيام بالأمرين معًا بالنسبة لأجهزتك، يكفي واحد فقط.



يحدد **الإجراء** ما إذا كانت الأجهزة سيتم تسجيلها في التجمع، مستخدم أو مجموعة.

يمكنك أيضًا تصدير واستيراد ملف .csv وتصفية إدخالاتك حسب الكلمات الرئيسية.

أندرويد إنتربرايز

هنا يمكنك إعداد Android Enterprise. هذا ضروري لاستخدام جميع ميزات Android Enterprise.

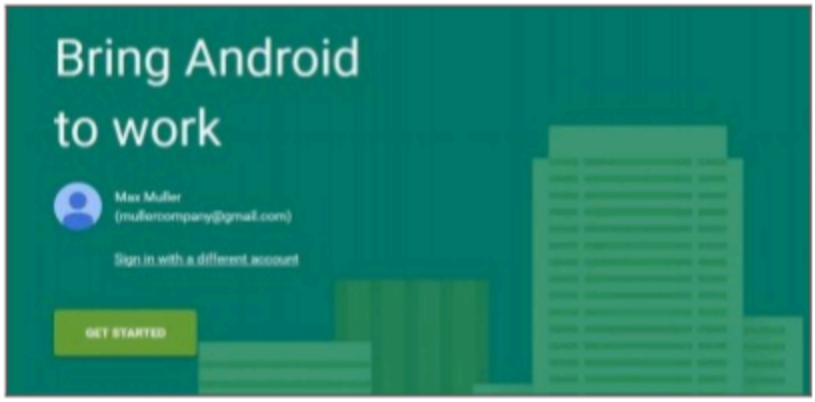
الطريقة الأولى: حساب المؤسسة على أندرويد (حساب جوجل)

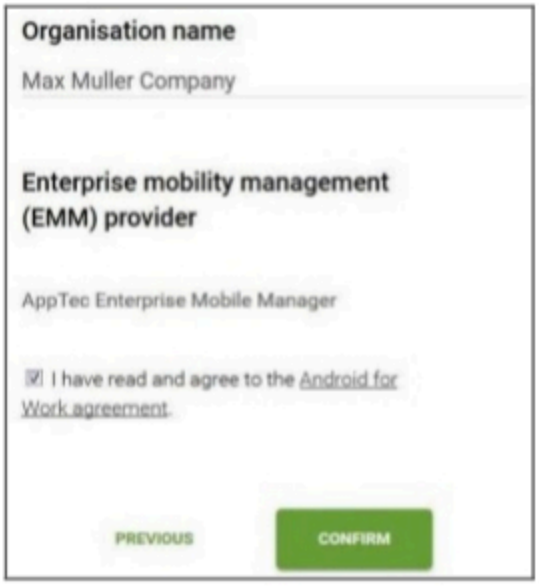
اضغط أولاً على "إعداد الإعداد"، ثم بعد لحظة قصيرة يجب أن يكون هناك زر "بدء الإعداد".

سيؤدي ذلك إلى نقلك إلى صفحة إعدادات جوجل للمؤسسات على نظام أندرويد.

قم بتسجيل الدخول باستخدام حساب Google الذي تريد استخدامه، إذا لم تكن قد سجلت الدخول بالفعل واضغط على "البدء".

يمكنك الآن إدخال اسم شركتك. بعد القيام بذلك، حدد خانة الاختيار واضغط على "تأكيد"





في الخطوة الأخيرة يمكنك إكمال تسجيلك ويجب أن تعود إلى وحدة التحكم. إذا نجح كل شيء يجب أن يبدو الأمر هكذا:

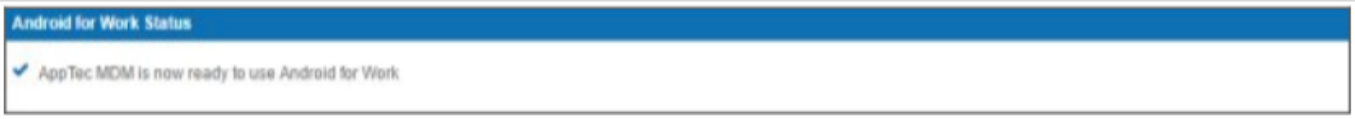
يمكنك الآن البدء في تهيئة حاوية Android Enterprise Container الخاصة بك.

الطريقة الثانية: حساب G-Suite

اضغط على "استخدام G-Suite" وقم بتسجيل الدخول إلى حساب مسؤول Google الخاص بك. هناك تنتقل إلى "الأمان" -> "إظهار المزيد" -> "إدارة موفر EMM لنظام Android" وإنشاء رمز مميز. ملاحظة: إذا كنت لا ترى إعدادات Android Enterprise في حساب G-Suite الخاص بك، فعليك الانتقال إلى "الحصول على المزيد من التطبيقات والخدمات" وإضافة إدارة جهاز Android. الآن أدخل الرمز المميز ونطاقك الأساسي في وحدة التحكم الخاصة بنا وانقر على "حفظ التغييرات". عند الانتهاء، انقر على "استخدام حساب Android Enterprise Account".

الآن يجب أن ترى زر "إنشاء حساب خدمة". اضغط عليه. قد تستغرق هذه العملية بضع لحظات.

إذا كان كل شيء يعمل، يجب أن يبدو هكذا:



يمكنك الآن البدء في تهيئة حاوية Android Enterprise Container الخاصة بك.

حماية إعادة ضبط المصنع

باستخدام حماية إعادة ضبط المصنع، يمكنك ربط جهازك بحساب جوجل من اختيارك، وهو ما يلغي أيضًا أي ربط موجود بحساب جوجل. لاستخدام حماية إعادة ضبط المصنع، عليك إعدادها هنا أولاً وتفعيلها في ملفاتك الشخصية بعد ذلك.

لإعداد حماية إعادة ضبط المصنع، انقر على "إعداد FRP" واتبع التعليمات التي تظهر على الشاشة.

ملاحظة: اقرأ الخطوات بعناية وقم بتنفيذها. نوصي بالقيام بذلك في نافذة متصفح متخفٍ جديد لتجنب تسجيل الدخول تلقائيًا إلى حساب Google الخاطئ. يمكنك قفل نفسك تمامًا خارج الجهاز، إذا كان يجب عليك إدخال معرّف خاطئ أو فقدت إمكانية الوصول إلى حساب Google المستخدم!

تسجيل AE

هنا يمكنك تفعيل وضع مالك جهاز Android Enterprise Ernollment. سيؤدي استخدام هذه الطريقة إلى تسجيل أجهزتك في وضع مالك جهاز أندرويد للمؤسسات. في هذا الوضع سيكون لديك التحكم الكامل في الجهاز.

تمكين تسجيل AE	تنشيط AE Enrollment تنبيه: إذا قمت بتعطيل AE Enrollment، ستتوقف رموز QR Codes الحالية وأجهزة مبرمج NFC التي تم تكوينها بالفعل عن العمل. إذا قمت بتمكين AE Enrollment مرة أخرى، فسيتعين عليك إعادة إرسال تكوينات دفع NFC / إنشاء رموز QR جديدة.
تمكين الاكتشاف التلقائي	عندما يقوم الجهاز بتسجيل نفسه عبر "التسجيل التلقائي"، سيحاول النظام تعيينه لمستخدم بناءً على المعلومات التي تم تعيينها في القائمة البيضاء للمسلسل / IMEI ("الإعدادات العامة"> "تكوين Android"> "التسجيل التلقائي").
حظر أجهزة غير معروفة	يُسمح فقط للأجهزة التي تم إدراجها في القائمة البيضاء في القائمة البيضاء للمسلسل / IMEI ("الإعدادات العامة"> "تكوين Android"> "التسجيل التلقائي") بالتسجيل.

ملاحظة حول الطريقة 1 و2: تشير "شاشة الترحيب" إلى الشاشة الأولى التي تراها بعد إعادة ضبط المصنع. قد تبدو هذه الشاشة مختلفة بناءً على إصدار و/أو طراز الجهاز الذي تستخدمه.

الطريقة 1: التسجيل برمز الاستجابة السريعة

(يتطلب نظام Android 7.0 أو أعلى) نوصي باستخدام هذه الطريقة دائمًا إذا كنت تستخدم نظام Android 7 أو أعلى.

1. إعادة ضبط المصنع للجهاز
2. قم بإنشاء رمز الاستجابة السريعة للتسجيل باستخدام إحدى الطريقتين التاليتين:
   - انقر في "الإعدادات العامة -> إعدادات أندرويد -> إعدادات أندرويد -> تسجيل AE" على "إنشاء رمز الاستجابة السريعة". اختر ما إذا كنت ترغب في تخطي تشفير التخزين و/أو يجب إزالة جميع تطبيقات النظام.
   - (بدلاً من ذلك) اختر جهازاً موجوداً. في "نظرة عامة على الجهاز" انقر على رمز الاستجابة السريعة المعروض هناك. اختر ما إذا كنت ترغب في تخطي تشفير التخزين و/أو يجب إزالة جميع تطبيقات النظام.
3. انقر الآن 6 مرات على شاشة الترحيب بجهازك. يجب أن يؤدي ذلك إلى بدء وضع تسجيل QR.
4. قم الآن بالاتصال بشبكة لاسلكية وانتظر لفترة قصيرة حتى يتم تثبيت قارئ رمز الاستجابة السريعة
5. والآن امسح رمز الاستجابة السريعة ضوئياً
6. هذا كل شيء. تم تسجيل جهازك الآن في وضع جهاز Android Enterprise Device Mode.
   - a. إذا كنت قد استخدمت رمز الاستجابة السريعة في "الإعدادات العامة"، يمكنك العثور على جهازك في "التجمع -> أجهزة مالك الجهاز AE". (تلميح: من الممكن أن تضطر إلى إعادة تحميل الموقع لرؤية الأجهزة). إذا قمت بتحديد "تمكين الاكتشاف التلقائي" ستجده في "تمكين الاكتشاف التلقائي".

- إذا استخدمت رمز الاستجابة السريعة لملف تعريف جهاز موجود، فسيتم تسجيل الجهاز في ملف التعريف هذا.

الطريقة 2: التسجيل في NFC

(يتطلب تقنية NFC وأندرويد 6.0 أو أعلى)

التحضير: أدخل معلومات الواي فاي الخاصة بك في "الإعدادات العامة -> إعدادات أندرويد -> إعدادات أندرويد -> تسجيل AE -> بيانات توفير NFC". استخدم الآن "جهاز NFC" للبحث عن الجهاز الذي سيصبح المبرمج. سيتم استخدام هذا الجهاز لإرسال معلومات التسجيل إلى الأجهزة الأخرى عبر NFC.

1. إعادة ضبط المصنع لجهازك
2. افتح تطبيق الاقتران بتقنية NFC من AppTec360 على المبرمج الخاص بك
3. اختر ما إذا كنت ترغب في تخطي تشفير التخزين و/أو يجب إزالة جميع تطبيقات النظام.
4. أمسك كلا الجهازين ظهراً لظهر
5. الآن يجب أن يكون تسجيل مؤسسة أندرويد إنتربرايز صارخًا
6. تجد الآن جهازك في وحدة التحكم
   - a. في المجمع، إذا لم تقم بتكوين الاكتشاف التلقائي
   - b. ضمن المستخدم، قمت بتكوينه للاكتشاف التلقائي
   - c. تلميح: من الممكن أن تضطر إلى إعادة تحميل الموقع لرؤية الأجهزة

الطريقة 3: حساب Google

(يتطلب أندرويد 5.1 أو أعلى)

(ملاحظة: إذا كنت تستخدم هذه الطريقة، فلن يتم تسجيل الجهاز تلقائيًا. بدلاً من ذلك عليك تسجيله يدوياً أو أتمتة العملية باستخدام التسجيل التلقائي).

1. إعادة ضبط المصنع لجهازك
2. تابع خطوات الإعداد حتى تتمكن من تسجيل الدخول باستخدام حساب جوجل
3. أدخل "afw#apptec" كاسم المستخدم/البريد الإلكتروني
4. اضغط على "التالي"
5. جهازك الآن هو جهاز أندرويد للمؤسسات

التسجيل في KNOX

هنا يمكنك تفعيل تسجيل KNOX Enrollment والعثور على المعلومات التي تحتاجها لإنشاء ملف تعريف تسجيل KNOX في بوابة نشر KNOX. تحتاج إلى حساب في بوابة KNOX للنشر لتكوين هذا الأمر واستخدامه.

(https://www.samsungknox.com/en/knox-deployment-program)

تمكين التسجيل في KNOX	تنشيط التسجيل في KNOX. تنبيه: إذا قمت بتعطيل KNOX Enrollment، ستتوقف ملفات تعريف MDM الحالية عن العمل. إذا قمت بتمكين KNOX Enrollment مرة أخرى، فسيتعين عليك تحديث حقل "بيانات JSON المخصصة" في ملف تعريف MDM الخاص بك
تمكين الاكتشاف التلقائي	عندما يقوم الجهاز بتسجيل نفسه عبر "تسجيل KNOX Enrollment"، سيحاول النظام تعيينه لمستخدم بناءً على المعلومات التي تم تعيينها في القائمة البيضاء للمسلسل / IMEI ("الإعدادات العامة"> "تكوين Android"> "التسجيل التلقائي").

1. تسجيل الدخول إلى بوابة التسجيل عبر الهاتف المحمول KNOX من سامسونج https://eukme.samsungknox.com/itadmin
2. الانتقال إلى "ملفات تعريف MDM"
3. انقر على "إضافة"
4. اختر "URI الخادم غير مطلوب لخادم MDM الخاص بي" وانقر على "التالي"
5. الآن قم بإنشاء ملف تعريف بالمعلومات الموضحة في وحدة تحكم الإدارة

الآن يمكن تثبيت ملف تعريف تسجيل KNOX هذا مباشرةً على الجهاز من قبل Samsung إذا حصلت على الأجهزة من Samsung مباشرةً.

وبدلاً من ذلك، يمكنك تنزيل تطبيق KNOX Deployment App، وتسجيل الدخول باستخدام حساب KNOX Deployment الخاص بك وإرسال ملف تعريف KNOX Enrollment Profile عبر تقنية NFC إلى أجهزة أخرى.

إذا كان الجهاز يحتوي على ملف تعريف KNOX Enrollment Profile مثبتًا، فسيتم تنزيل تطبيقنا وتسجيل الجهاز، إذا كان لديه اتصال إنترنت يعمل.

يمكن العثور على تسجيل الأجهزة عبر تسجيل KNOX Enrollment في "التجمع -> تسجيل KNOX"، أو ضمن المستخدم الذي حددته في الاكتشاف التلقائي.

عدم اللمس

باستخدام ميزة Zero-Touch، يمكنك تسجيل أجهزتك بسهولة دون الحاجة إلى لمسها أو تهيئة أي شيء على الجهاز نفسه. ما عليك سوى تشغيله ومتابعة التهيئة كالمعتاد وسيتلقى الجهاز جميع المعلومات حول كيفية الإعداد والاتصال بـ MDM تلقائيًا تمامًا.

لاستخدام ميزة Zero-Touch، عليك شراء أجهزتك من موزع يدعم ميزة Zero-Touch. يقوم الموزع نفسه أيضًا بإنشاء حساب لك في بوابة Zero-Touch. اتصل بالموزع للحصول على مزيد من المعلومات حول الإجراء أو إذا واجهتك مشاكل عند الوصول إلى بوابة Zero-Touch.

انقر على "بدء الإعداد" لبدء الإعداد. ستتم إعادة توجيهك إلى صفحة تسجيل الدخول حيث يتعين عليك تحديد حساب Google الخاص بك الذي يمكنه الوصول إلى بوابة Zero-Touch.

ملاحظة: من الممكن تحديد أي حساب. لذا تأكد من تحديد الحساب الصحيح في هذه الخطوة. إذا كنت لا ترى أجهزتك/التكوينات الخاصة بك، فمن المحتمل أنك استخدمت حسابًا خاطئًا.

بعد إكمال تسجيل الدخول، سيبدو الأمر كالتالي:

انقر على "+" لإضافة تهيئة وملء الحقول كما تظهر على الشاشة. إذا قمت بتمكين التكوين كتكوين افتراضي، فسيتم تعيينه للأجهزة الجديدة تلقائياً. لا يؤدي إنشاء أو تعيين تكوين افتراضي إلى تعيينه للأجهزة الموجودة بالفعل.

إذا لم يتم تعيين تهيئة للجهاز، فسيتم إعداده كجهاز عادي ولن يتصل بـ MDM. لذلك تأكد من أن أجهزتك قد تم تعيين تهيئة لها.

بعد أن تقوم بتوصيل حسابك، وتصبح أجهزتك مرئية ولديك تهيئة مخصصة لها، يمكنك البدء في إعداد الأجهزة.

يمكنك إضافة الأجهزة إلى قائمة التسجيل التلقائي حتى يتم تسجيلها في مجموعة أو مستخدم محدد تلقائياً. إذا لم تقم بتكوين أي شيء في قائمة التسجيل التلقائي، فسيتم تسجيل الأجهزة في مخزن الأسئلة.

تكوين الويندوز

تكوين الويندوز

هنا لديك الخيار لتمكين التكوينات التالية على جهاز الكمبيوتر الشخصي الذي يعمل بنظام Windows 10:

اتصال DM الفوري	
وقت إعادة المحاولة الأولي	ينشئ أول محاولة اتصال بالجهاز، تزداد هذه القيمة أضعافاً مضاعفة
إعادة محاولة الاتصال	يشير إلى عدد محاولات الاتصال التي يجب أن يقوم بها عميل DM، أثناء حدوث خطأ في الاتصال
الحد الأقصى لوقت النوم	يشير إلى الحد الأقصى لوقت السكون بعد حدوث خطأ في الاتصال
إعادة محاولة المزامنة الأولى	الفواصل الزمنية، التي يتصل فيها الجهاز بالخادم، بعد الاتصال الأول
فترة إعادة المحاولة الأولى	يتعلق ب "إعادة المزامنة الأولى" هنا يتم سرد الأوقات بالدقائق على سبيل المثال تحت "إعادة المزامنة الأولى" يتم إدراج القيمة "2" وتحت "الفاصل الزمني لإعادة المحاولة الأولى" يتم إدراج القيمة "4 دقائق"، وبهذه الطريقة يتصل الجهاز مرتين كل 4 دقائق، بعد الاتصال الأول
إعادة محاولة المزامنة الثانية	الفواصل الزمنية، التي يجب أن يتصل فيها الجهاز بالخادم، بعد إكمال "إعادة المزامنة الأولى"
الفاصل الزمني لإعادة المحاولة الثانية	نفس المبدأ المتبع في "فترة إعادة المحاولة الأولى" - إلا أنه ينطبق هنا على "إعادة المحاولة الثانية للمزامنة"
إعادة محاولة المزامنة المنتظمة	الفواصل الزمنية، لعدد المرات التي يجب أن يتواصل فيها الجهاز مع الخادم في المستقبل افتراضي: "لا نهائي" نوصي بعدم تغيير هذه القيمة، لأنك إذا قمت بإدخال "10"، سيتصل الجهاز بالخادم 10 أضعاف ثم يتوقف، وبالتالي ينقطع الاتصال بخادم AppTec360!
الفاصل الزمني لإعادة المحاولة المنتظمة	نفس مبدأ "الفاصل الزمني الأول/الثاني لإعادة المحاولة" - فقط هنا يتم تطبيق الإعدادات للمستقبل
الفاصل الزمني لإعادة المحاولة المنتظمة	نفس مبدأ "الفاصل الزمني الأول/الثاني لإعادة المحاولة" - فقط هنا يتم تطبيق الإعدادات للمستقبل

صندوق المحتوى

التكوين

هنا يمكنك تكوين ContentBox. يمكنك وضع ملفات للمجموعات في ContentBox والتي يمكن الوصول إليها باستخدام تطبيق ContentBox على الجهاز.

تمكين ContentBox	تمكين ContentBox. يمكن أن يؤدي تعطيل ذلك إذا كنت لا تستخدم ContentBox، إلى توفير الموارد على الأجهزة المحلية.
استخدام تثبيت ContentBox خارجي	يمكن أيضاً تشغيل ContentBox باستخدام Nextcloud الخاص بك.
عنوان URL	عنوان URL الكامل لكيان Nextcloud
المستخدم الجذر	المستخدم الجذر لحساب Nextcloud
كلمة المرور الجذرية	كلمة المرور الجذرية لحساب Nextcloud
أذونات مجلد المجموعة الافتراضية	أذونات مجلد المجموعة الافتراضية، يمكن تعديلها بشكل فردي حسب المجموعة (في إدارة الأجهزة المحمولة)
مشاركة مجلد المجموعة مع المجموعات الفرعية	إذا كانت نشطة، يمكن لكل مجموعة فرعية قراءة جميع مجلدات المجموعة الرئيسية، كما يمكن تكوينها بشكل فردي لكل مجموعة (إدارة الأجهزة المحمولة)
أذونات المجموعات الفرعية	أذونات المجموعات الفرعية يمكن تهيئتها بشكل فردي لكل مجموعة على حدة (إدارة الأجهزة المحمولة)
السماح بالمشاركة	السماح للمستخدم بمشاركة المحتوى عبر الروابط، ويمكن تهيئتها بشكل فردي لكل مجموعة على حدة
الحد الأقصى لحجم تحميل الملف بالميجابايت	الحد الأقصى لحجم الملف قياسي: 512 ميجابايت الحد الأقصى للتكوين: 2048
بيانات اعتماد WebDAV	
عنوان URL WebDAV	يمكنك أيضًا فتح ContentBox باستخدام WebDAV. يرجى عدم حذف المجلدات التالية، تحت أي ظرف من الظروف: /apptecgroups/ /apptecgroups/AppTecGroup-X
المستخدم الجذر	اسم المستخدم الجذري
كلمة المرور	كلمة مرور المستخدمين الجذر

تحدث المزامنة مع ContentBox تلقائياً. ومع ذلك، يمكنك إجراء مزامنة يدوية باستخدام "مزامنة صندوق المحتوى".

بالإضافة إلى ذلك، يمكنك هنا تنشيط/إلغاء تنشيط ContentBox على كل جهاز على حدة.

هذا مناسب فقط، إذا لم تكن قد قمت بترخيص ContentBox بشكل إضافي، فلا يزال لديك إمكانية الوصول إلى 25 جهازًا يمكنك اختبار ContentBox بها - هنا يمكنك تفعيل ذلك للأجهزة المعنية.

تكوين LDAP

نظرة عامة على LDAP

يمكنك هنا إنشاء اتصال بالدليل النشط عبر LDAP لاستيراد المستخدمين والمجموعات بشكل جماعي. يجب إجراء المزامنة يدوياً. يمكنك تكوين اتصالات LDAP متعددة بأنظمة مختلفة أو بتكوينات/مرشح مختلف.

اسم الخادم	اسم العرض للخادم
النوع	لا يتم حالياً دعم سوى الدلائل النشطة التي تدعم LDAP في الوقت الحالي
نطاق LDAP	نطاق LDAP الأساسي (على سبيل المثال: example.com)
مضيف LDAP	ضروري فقط في حالة عدم إمكانية الوصول إلى مضيف LDAP ضمن نطاق LDAP المحدد.
الميناء	اتركه فارغًا لاستخدام المنفذ القياسي (389 أو 636 لـ SSL)
اسم المستخدم	على سبيل المثال: CN=John,OU=U=Users,DC=EXAMPLE,DC=COM ملاحظة: تتطلب معظم الأنظمة اسم المستخدم بهذا التنسيق ولا تقبل "John" كاسم مستخدم
كلمة المرور	
تأكيد كلمة المرور	
أمان الاتصال	ملاحظة: عند استخدام SSL أو TLS، سيتم التحقق من شهادة الدليل النشط. إذا كانت موقعة ذاتيًا، يجب عليك إضافة المرجع المصدق الجذر إلى مخزن الثقة الخاص بالجهاز المحلي. إذا كنت على السحابة يجب أن يوفر Active Directory شهادة موثوق بها وإلا سيعمل الاتصال فقط بدون تشفير
المزامنة التلقائية.	تمكين المزامنة التلقائية لدليل LDAP في الفاصل الزمني المحدد في إعدادات LDAP العامة.
قاعدة DN	إذا كنت لا ترغب في مزامنة الدليل بأكمله، يمكنك تحديد OU هنا، على سبيل المثال OU=AndroidUsers,OU=Users,DC=EXAMPLE,DC=COM
عضو في	ستتم إضافة جميع المستخدمين المستوردين إلى المجموعة المحددة
المستخدمون المفعلون فقط؟	عند التمكين، سيتم النظر في السمة userAccountControl، ولن يتم استيراد المستخدمين الذين لا يحملون هذه السمة.
مرشح LDAP	يمكنك استخدام عامل تصفية LDAP لتصفية المستخدمين الذين يتم استيرادهم
فلتر Regex	يمكنك استخدام عامل تصفية Regex لتصفية المستخدمين الذين يتم استيرادهم
اختبار الاتصال	اختبار الاتصال عند حفظ التكوين
إعادة تعيين بنية الدليل عند المزامنة؟	إذا كان صحيحاً سيتم نقل جميع إدخالات LDAP إلى موقعها الأصلي في شجرة LDAP. يوصى بتمكينه.

إعادة استيراد المستخدمين والمجموعات المحذوفة؟	عند التمكين، سيتم إعادة إنشاء المستخدمين والمجموعات التي تم حذفها. يوصى بتمكينه.
مزامنة عمليات الحذف؟	عند التمكين، سيتم حذف المجموعات والمستخدمين عند حذفهم على خادم LDAP. كما سيتم حذف أجهزة المستخدمين المحذوفين.

أسفل قائمة تكوينات LDAP الخاصة بك يمكنك تحديد الفترة التي تتم فيها مزامنة النظام تلقائياً. يستخدم فقط تكوينات LDAP للمزامنة التلقائية التي تم تنشيط الخيار وفقاً لذلك.

إدارة التطبيقات

قاعدة بيانات التطبيق الداخلي

أندرويد

هنا يمكنك تحميل تطبيقات Android التي قامت شركتك بتطويرها وتوزيعها لاحقاً في إدارة الأجهزة المحمولة في ملفات تعريف الأجهزة أو المجموعات.

يرجى العلم أننا ننصح بتوزيع التطبيقات بهذه الطريقة فقط، والتي لا تتوفر في متجر Google Play.

انقر على "+" لتحميل ملف APK للتطبيق الذي تريد تحميله. تنسيق APK هو الوحيد المدعوم حاليًا.

يمكن زيادة حد التحميل على الأجهزة المحلية في الخطوة 3 من تكوين الجهاز. إذا كنت ترغب في زيادة حد التحميل على السحابة، يُرجى الاتصال بالدعم للحصول على مزيد من المعلومات.

انتبه إلى أن ملفات APK عادةً ما تكون أصغر قليلاً من محتواها. من الممكن أن يفشل التحميل بسبب ذلك، حيث يتم تفريغ ملف APK في العملية. على سبيل المثال من الممكن أن يفشل ملف APK بحجم 95 ميغابايت مع حد تحميل 100 ميغابايت. في هذه الحالة، قم بزيادة حد التحميل كما هو مذكور أعلاه.

كما ننصح أيضًا بنقل ملف APK يدويًا أولاً إلى جهاز اختبار واحد (على سبيل المثال عبر USB) ومحاولة تثبيته يدويًا باستخدام تطبيق الملفات الخاص بالجهاز. إذا لم ينجح ذلك لأي سبب من الأسباب، فسيفشل أيضًا عبر MDM.

تحديث الهدف

باستخدام ميزة "تحديث الهدف" يمكنك اختيار إصدار التطبيق الذي يجب تثبيته أو الإصدار الذي يجب تحديث التطبيق إليه إذا قمت بتفعيل "التحديث المستمر" للتطبيق.

إذا لم تقم بتحديد هدف التحديث، فسيتم استخدام الإصدار الأعلى.

ضع في اعتبارك أن Android لا يمكنه تخفيض إصدار التطبيقات. انتبه أيضًا إلى أن "رمز الإصدار" يحدد ما إذا كان الإصدار أعلى أو أقل أو نفس الإصدار أم لا. لذا تأكد من زيادة هذا الإصدار بشكل صحيح في تطبيقك عند إنشاء تحديث.

iOS

هنا يمكنك تحميل تطبيقات iOS التي قمت بتطويرها وتوزيعها لاحقًا في إدارة الأجهزة المحمولة في ملفك الشخصي للجهاز أو المجموعة.

انقر على "+" لتحميل تنسيق IPA للتطبيق الذي تريد تحميله. يتم دعم تنسيق IPA فقط في الوقت الحالي.

يمكن زيادة حد التحميل على الأجهزة المحلية في الخطوة 3 من تكوين الجهاز. إذا كنت ترغب في زيادة حد التحميل على السحابة، يُرجى الاتصال بالدعم للحصول على مزيد من المعلومات.

تحديث الهدف

باستخدام ميزة "تحديث الهدف" يمكنك اختيار إصدار التطبيق الذي يجب تثبيته أو الإصدار الذي يجب تحديث التطبيق إليه إذا قمت بتفعيل "التحديث المستمر" للتطبيق.

إذا لم تقم بتحديد هدف التحديث، فسيتم استخدام الإصدار الأعلى.

نظام التشغيل MacOS

هنا يمكنك تحميل تطبيقات MacOS التي قمت بتطويرها وتوزيعها لاحقًا في إدارة الأجهزة المحمولة في ملفك الشخصي للجهاز أو المجموعة.

انقر على "+" لتحميل PKG للتطبيق الذي تريد تحميله. يتم دعم تنسيق PKG فقط في الوقت الحالي.

يمكن زيادة حد التحميل على الأجهزة المحلية في الخطوة 3 من تكوين الجهاز. إذا كنت ترغب في زيادة حد التحميل على السحابة، يُرجى الاتصال بالدعم للحصول على مزيد من المعلومات.

تحديث الهدف

باستخدام وظيفة "تحديث الهدف"، يمكنك اختيار إصدار التطبيق الذي يجب تثبيته أو الإصدار الذي يجب تحديث التطبيق إليه إذا قمت بتفعيل "التحديث المستمر" للتطبيق.

إذا لم تقم بتحديد هدف التحديث، فسيتم استخدام الإصدار الأعلى.

ويندوز 10

هنا يمكنك تحميل تطبيقات Windows 10 وتوزيعها لاحقًا في إدارة الأجهزة المحمولة في ملفك الشخصي للجهاز أو المجموعة.

انقر على "+" لتحميل APPX أو APPXBUNDLE أو MSI للتطبيق الذي تريد تحميله. يتم دعم تنسيق APPX أو APPXBUNDLE أو MSI فقط في الوقت الحالي.

يمكنك أيضًا تحميل وتحديد التبعيات للتطبيق، والتي سيتم توزيعها وتثبيتها تلقائيًا قبل تثبيت التطبيق المطلوب.

يمكن زيادة حد التحميل على الأجهزة المحلية في الخطوة 3 من تكوين الجهاز. إذا كنت ترغب في زيادة حد التحميل على السحابة، يُرجى الاتصال بالدعم للحصول على مزيد من المعلومات.

تحديث الهدف

باستخدام وظيفة "تحديث الهدف"، يمكنك اختيار إصدار التطبيق الذي يجب تثبيته أو الإصدار الذي يجب تحديث التطبيق إليه إذا قمت بتفعيل "التحديث المستمر" للتطبيق.

إذا لم تقم بتحديد هدف التحديث، فسيتم استخدام الإصدار الأعلى.

حزمة Win32 (.exe)

يمكنك أيضًا توزيع ملفات .exe/مثبتات ملفات .exe على أجهزتك.

اسم الحزمة	الاسم الذي سيتم عرضه في MDM
الوصف	الوصف الموضح في آلية إدارة الأجهزة المتعددة الوظائف
ملف الحزمة	يُسمح فقط بملفات .zip. ضع الملفات التي تريد نشرها في هذا الملف المضغوط.
سياق النشر	**النظام**: يتم تشغيل أمر التثبيت بامتيازات النظام وهو أعلى من "المستخدم". أيضًا عند استخدام "النظام"، لا تحتوي العملية على واجهة مستخدم، لذلك ستكون صامتة ولا يمكن الوصول إلى ملف تعريف المستخدم، مثل متغيرات البيئة مثل %AppDat%. **المستخدم**: يمكن لأمر التثبيت الوصول إلى ملف تعريف المستخدم ويمكنه عرض واجهة المستخدم إذا لزم الأمر. ملاحظة: قد تعمل بعض العمليات في سياق واحد فقط. على سبيل المثال: إذا تم تثبيت برنامج ما في AppData، فسيعمل فقط عند تحديد "المستخدم"
أمر التثبيت	الأمر المستخدم لتثبيت البرنامج. على سبيل المثال، أمر التثبيت لملف مضغوط يحتوي على "setup.exe" في جذره، والذي يدعم المعلمة "/s" للتثبيت الصامت، سيكون أمر التثبيت "setup.exe /s". انتبه إلى أن البرامج المختلفة قد يكون لها معلمات مختلفة.
أمر إلغاء التثبيت	الأمر المطلوب تشغيله لإلغاء تثبيت البرنامج عبر MDM. عادةً ما يشير هذا الأمر إلى برنامج إلغاء التثبيت. على سبيل المثال "C:\Program Files\ExampleSoftware\uninstall.exe".
المتطلبات	
ملاحظة: يجب استيفاء جميع المتطلبات المحددة لتثبيت البرنامج. وإلا فلن يتم تثبيته. قد تكون بعض الحقول إلزامية. إذا لم يتم تعيين أي قيمة لأحد المتطلبات، فسيتم تجاهل المتطلب.	
بنية نظام التشغيل	بنية نظام التشغيل
الحد الأدنى لإصدار نظام التشغيل	الحد الأدنى لإصدار نظام التشغيل
الحد الأدنى للمساحة الخالية على القرص (ميغابايت)	الحد الأدنى للمساحة الخالية على القرص (ميغابايت)
الحد الأدنى للذاكرة الفعلية (ميغابايت)	الحد الأدنى للذاكرة الفعلية (ميغابايت)
الحد الأدنى لعدد المعالجات المنطقية	الحد الأدنى لعدد المعالجات المنطقية

الحد الأدنى لسرعة وحدة المعالجة المركزية (ميجاهرتز)	الحد الأدنى لسرعة وحدة المعالجة المركزية (ميجاهرتز)
المتطلبات الإضافية	يمكنك أيضًا تحديد القواعد يدويًا أو تحميل برنامج نصي هنا لإجراء عمليات تحقق إضافية من المتطلبات إذا كنت ترغب في ذلك.
قواعد الكشف	
طريقة الكشف	يمكنك هنا تحديد كيفية اكتشاف ما إذا كان التطبيق مثبتًا على الجهاز أم لا. سيتم تشغيل أوامر التثبيت فقط عندما تكتشف هذه القواعد أن التطبيق غير مثبت. يتم تشغيل أوامر إلغاء التثبيت فقط عندما تكتشف هذه القواعد أن التطبيق غير مثبت. **تحديد القواعد يدوياً**: يتيح لك تحديد قاعدة واحدة أو أكثر يدويًا للتحقق على سبيل المثال من وجود ملف أو مجلد أو MSI أو مفتاح تسجيل معين. إذا كانت جميع قواعد الكشف المحددة صحيحة، فسيتم اعتبار التطبيق موجوداً. **استخدام البرنامج النصي**: قم بتحميل البرنامج النصي الخاص بك مع عمليات التحقق الخاصة بك. إذا أرجع البرنامج النصي "$TRUE"، فسيتم اعتبار التطبيق موجودًا.
قواعد الكشف	

إعدادات التطبيق

إعدادات تطبيق iOS

هنا يمكنك تحديد الإعدادات الافتراضية لإضافة تطبيق إلى التطبيقات الإلزامية أو متجر تطبيقات المؤسسة.

ملاحظة: هذا يحدد فقط ما يتم تحديده افتراضيًا عند إضافة التطبيقات. لا يؤدي هذا إلى تغيير الإعدادات الحالية للتطبيقات التي تمت إضافتها بالفعل في التطبيقات الإلزامية أو متجر تطبيقات المؤسسة.

مواكبة آخر المستجدات	يحافظ على تحديث التطبيق تلقائياً. يُرجى العلم أن الأمر قد يستغرق ما يصل إلى 7 أيام بعد إصدار التحديث حتى يتم تحديث التطبيق.
التجاوز عند عدم الإدارة	إذا كان التطبيق مثبتًا بالفعل على أنه غير مُدار (من قبل المستخدم) فسيتم تجاوز التطبيق وإدارته بواسطة إدارة تطبيقات MDM.
إزالة التطبيق عند إزالة ملف تعريف MDM	إلغاء تثبيت التطبيق عند إزالة MDM.
منع النسخ الاحتياطي لبيانات التطبيق	يمنع النسخ الاحتياطي لبيانات التطبيق.

إعدادات تطبيق أندرويد

هنا يمكنك تحديد الإعدادات الافتراضية لإضافة تطبيق إلى التطبيقات الإلزامية أو متجر تطبيقات المؤسسة.

ملاحظة: هذا يحدد فقط ما يتم تحديده افتراضيًا عند الإضافة. لا يؤدي ذلك إلى تغيير إعدادات التطبيقات التي تمت إضافتها بالفعل في التطبيقات الإلزامية أو متجر تطبيقات المؤسسة.

مواكبة آخر المستجدات	يحافظ على تحديث التطبيق تلقائياً. متاح فقط للتطبيقات الداخلية.
تحديث عميل AppTec360 AppTec360 EMM المتحكم به	في حالة التمكين، يمكن للمسؤولين تحديد هدف التحديث لعميل AppTec360 EMM Client. ستظهر قائمة بجميع الإصدارات المتوفرة من عميل AppTec360 EMM في "الإعدادات العامة" → "إدارة التطبيقات" → "قاعدة بيانات التطبيقات الداخلية" → "Android".

تطبيقات الطرف الثالث

أندرويد

هنا يمكنك تعيين رمز التفعيل الخاص بك لـ Ikarus.

اضبط هذا على "استخدام رمز التفعيل" وأدخل رمز التفعيل الخاص بك هنا.

ملاحظة: بعد إدخال الرمز وحفظه، لا تتم إضافة الرمز بعد إلى الملف الشخصي الذي يتم إرساله إلى الجهاز. عليك إجراء أي تغيير في ملف التعريف الخاص بك حتى تتم إضافة الرمز إلى ملف التعريف. على سبيل المثال: قم بتغيير أي مفتاح في الملف الشخصي من إيقاف التشغيل ← تشغيل ← إيقاف التشغيل - احفظ ← تعيين الآن.

iOS

هنا يمكنك إدخال ترخيص SecurePIM الخاص بك. بعد إدخال الترخيص، اضغط على "حفظ التغييرات" ويمكنك استخدام خيارات SecurePIM.

VPP / KNOX Premium

يتيح لك برنامج الشراء المجمع (VPP) من Apple توزيع التطبيقات المدفوعة والمجانية بسهولة على أجهزتك. يوصى بذلك بشدة لأنك لا تحتاج إلى معرف Apple على الأجهزة، ولا يتعين على المستخدمين تأكيد التثبيت (تحت الإشراف)، ولن يضطر المستخدمون إلى إدخال كلمة مرور معرف Apple، ويمكنك توزيع التطبيقات المدفوعة بسهولة دون شرائها على كل جهاز مرة أخرى.

لاستخدام VPP يجب عليك التسجيل في مدير أعمال Apple Business Manager.

تراخيص VPP

هنا يمكنك الحصول على نظرة عامة على تطبيقات VPP الخاصة بك، وعدد التراخيص المستخدمة وعدد التراخيص المتاحة.

سيتيح لك النقر على العجلة معرفة الأجهزة التي تم تعيين ترخيص لها وحالة هذا التعيين.

يؤدي النقر فوق تحديث ذاكرة التخزين المؤقت لبرنامج VPP التي تقارن التراخيص المعينة في MDM مع التراخيص المعينة من جانب Apples. يمكن أن يؤدي ذلك إلى حل مشاكل الترخيص في بعض الحالات.

رمز VPP المميز

يمكنك هنا تحميل رمز VPP المميز الخاص بك، والذي يمكن العثور عليه في مدير أعمال Apple Business Manager في الإعدادات → التطبيقات والكتب. يمكنك تحميل عدة رموز VPP Tokens.

يمكنك تجديد الرمز المميز ببساطة عن طريق تنزيل رمز جديد في مدير أعمال Apple، والنقر على عجلة "تعديل" وتحميل الرمز الجديد.

يحدد "وضع VPP" كيفية التعامل مع تعيين الترخيص. بناءً على السيناريو الخاص بك، عليك استخدام أوضاع مختلفة:

يجب استخدام "استنادًا إلى الجهاز" عند تسجيل الأجهزة عبر رمز الاستجابة السريعة أو الرابط أو أداة تهيئة Apple أو DEP.

"المستند إلى المستخدم" مطلوب إذا كانت الأجهزة مسجلة مع تسجيل المستخدم أو كجهاز iPad مشترك.

إذا قمت بتمكين "الإدارة التلقائية للتراخيص"، فسيتم تلقائيًا تعيين تراخيص Apple VPP للمستخدمين الذين يتم نقلهم من مجموعة إلى أخرى استنادًا إلى ملف تعريف المجموعة التي تم نقلهم إليها.

لن يتم إلغاء تراخيص Apple VPP الحالية من المجموعة التي انتقلوا منها.

سيتم تلقائياً تعيين تراخيص Apple VPP للمستخدمين الجدد الذين تمت إضافتهم إلى مجموعة ما استناداً إلى ملف تعريف المجموعة المعنية.

مفتاح KNOX Premium Key

هنا يمكنك إدخال مفتاح KNOX Premium الخاص بك لاستخدام حاوية KNOX من سامسونج.

يرجى الانتباه إلى أن هذا لم يعد مدعومًا منذ Android 10. استخدم حاوية Android Enterprise Container بدلاً من ذلك.

إعدادات متجر التطبيقات

المنطقة واللغة

هنا يمكنك تعيين اللغة والمنطقة الافتراضية للبحث عن التطبيق في إدارة التطبيقات.

يرجى الانتباه إلى أن الإعداد الخاص بـ iTunes يحدد أيضًا كيفية حصول النظام على معلومات حول تطبيقات معينة. إذا واجهت تطبيقات في قوائمك يتم عرضها بطريقة غريبة (مثل أيقونة مفقودة) فربما تكون قد حددت منطقة لا يتوفر فيها التطبيق المحدد.

متجر AE Play

هنا يمكنك العثور على جميع خيارات متجر Play Store لأجهزة Android Enterprise للموافقة على التطبيقات أو تحميل التطبيقات الخاصة إلى متجر Play أو إنشاء تطبيقات الويب الخاصة بك.

التطبيقات المعتمدة

هنا يمكنك الحصول على نظرة عامة على جميع التطبيقات التي وافقت عليها.

تطبيقات متجر Play ستور

سيؤدي ذلك إلى تحميل إطار iFrame يعرض متجر Play. ابحث عن أي تطبيق تريده، وانقر عليه ووافق عليه. أثناء الموافقة على التطبيق يمكنك أيضًا تحديد إلغاء الموافقة إذا تغيرت الأذونات المطلوبة. نوصي بترك هذه الإعدادات افتراضية عند الموافقة على التطبيقات.

بعد الموافقة على التطبيق، يمكنك إضافته إلى ملفاتك الشخصية.

سيتغير زر "الموافقة" إلى "إبطال الموافقة" بعد الموافقة، بحيث يمكنك دائمًا إزالة التطبيقات إذا لم تعد بحاجة إليها بعد الآن.

التطبيقات الخاصة

هنا يمكنك تحميل تطبيقك الخاص كتطبيق خاص على متجر Google Play. يتيح لك ذلك توزيع التطبيق من خلال خدمات Google وتحديثه من خلالها. ويتميز هذا أيضًا بميزة أنه يمكن تثبيت تطبيقاتك الخاصة دون الحاجة إلى تأكيد المستخدم، وهو أمر ضروري عادةً.

تطبيقات الويب

هنا يمكنك إنشاء تطبيقات ويب، وهي روابط لصفحات ويب معينة يمكن تعيينها مثل التطبيقات.

يمكنك أيضًا إعطاء هذه الأيقونة أيقونة مخصصة وتحديد كيفية عرضها بالضبط.

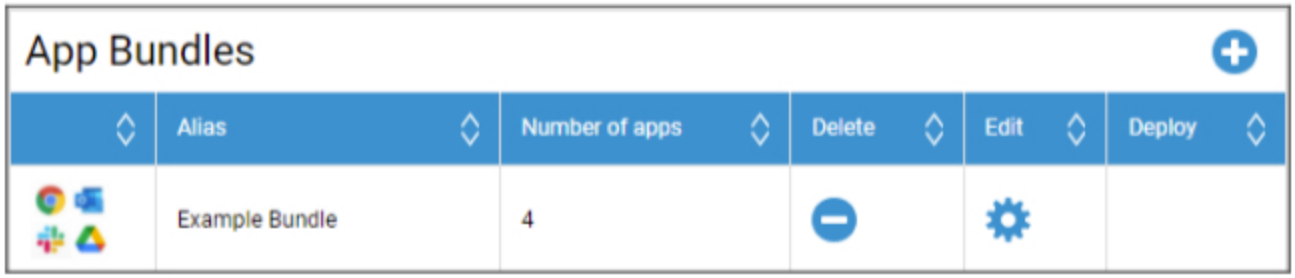
تخطيط المتجر

يحدد تخطيط المتجر كيفية عرض التطبيقات في متجر Play أو إذا كانت معروضة أصلاً.

ضع في اعتبارك أنه إذا كنت تريد عرض التطبيقات في متجر Play ليقوم المستخدم بتثبيتها يدويًا، فيجب إضافتها هنا في التخطيط **و** في الملف الشخصي إلى متجر Play للمؤسسات. إذا أضفت تطبيقًا إلى واحد منهما فقط، فلن يتم عرضه.

باقة التطبيقات

باستخدام حزم التطبيقات، يمكنك تحديد مجموعات من التطبيقات التي يمكن تعيينها لملفات تعريف الجهاز أو المجموعة بنقرة واحدة.



انقر على "+" لإنشاء حزمة تطبيقات جديدة. بعد إنشاء حزمة تطبيقات، يمكنك النقر على "تعديل" لإضافة تطبيقات من مصادر مختلفة إلى الحزمة.

يمكن إضافة حزمة إلى الملفات الشخصية مثل كل التطبيقات الأخرى. عند إضافة التطبيقات، سيكون لديك علامة تبويب إضافية باسم "حزم التطبيقات" حيث توجد حزمك.

إذا أجريت أي تغيير على حزمة تطبيقات سيظهر زر في العمود "نشر". سيتيح لك ذلك دفع هذه التغييرات إلى جميع الملفات الشخصية التي تحتوي على هذه الحزمة. لذا ضع في اعتبارك أنه يجب عليك القيام بذلك يدويًا بعد إضافة أو إزالة التطبيقات في الحزمة.

جهاز التحكم عن بُعد

برنامج TeamViewer

موصل برنامج TeamViewer

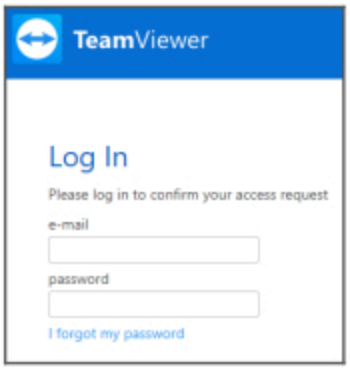
ملاحظة: في الإصدار التجريبي المجاني على نسختنا السحابية لن تتمكن من ربط حساب TeamViewer الخاص بك. سيكون لديك حساب تجريبي مجاني مرتبط تلقائيًا بدلاً من ذلك.

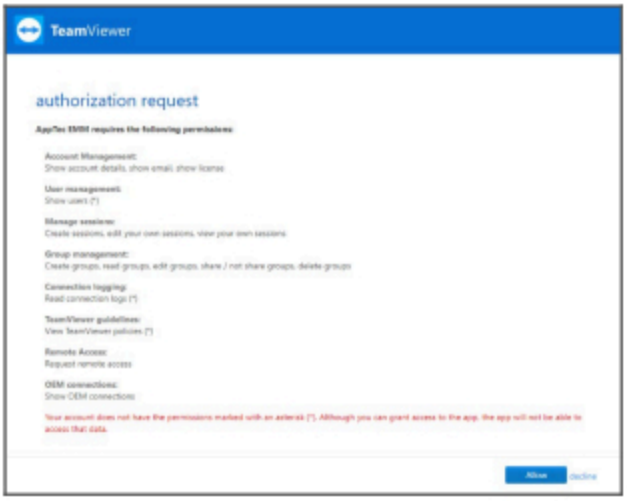
انتقل إلى الإعدادات العامة -> التحكم عن بعد -> برنامج TeamViewer. هنا يمكنك ربط حساب TeamViewer الخاص بك مع وحدة التحكم أو الاطلاع على معلومات حول حسابك المتصل حاليًا. يمكنك أيضًا عرض جميع الجلسات النشطة حاليًا إذا انتقلت إلى "الجلسات النشطة".

لربط حسابك انقر على "بدء الإعداد".

سيؤدي القيام بذلك إلى توجيهك إلى صفحة جديدة حيث يتعين عليك تسجيل الدخول باستخدام حساب TeamViewer الخاص بك.

بعد تسجيل الدخول، يجب عليك تفويض AppTec360 MDM باستخدام هذا الحساب. بعد تأكيد ذلك، عليك الانتظار بضع ثوانٍ ثم يتم توصيل الحساب.


TeamViewer
Log In
Please log in to confirm your access request
e-mail
password
I forgot my password


TeamViewer
authorization request

تثبيت برنامج TeamViewer QuickSupport

أضف تطبيق "TeamViewer QuickSupport" إلى التطبيقات الإلزامية في ملف تعريف جهازك أو ملف تعريف المجموعة وانقر على "تعيين الآن". انتظر حتى يتم تثبيت التطبيق على الجهاز.

إذا حاولت الوصول إلى جهاز لم يتم تثبيت التطبيق عليه، فسيتم تثبيته أو سيُطلب منك تثبيته بناءً على تكوين الجهاز.

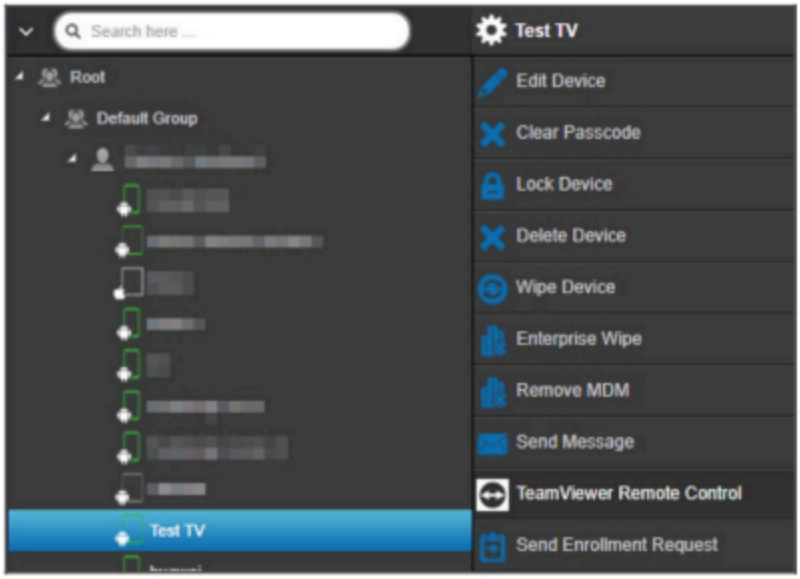
التحكم عن بُعد في جهازك

للتحكم بجهازك عن بُعد، حدد الجهاز، وانقر على العجلة واختر "TeamViewer Remote Control"

إذا كانت هناك جلسة عمل نشطة بالفعل، يمكنك إما استخدام الجلسة القديمة أو إنشاء جلسة عمل جديدة.

تأكد من أنك تريد إنشاء جلسة TeamViewer جديدة.

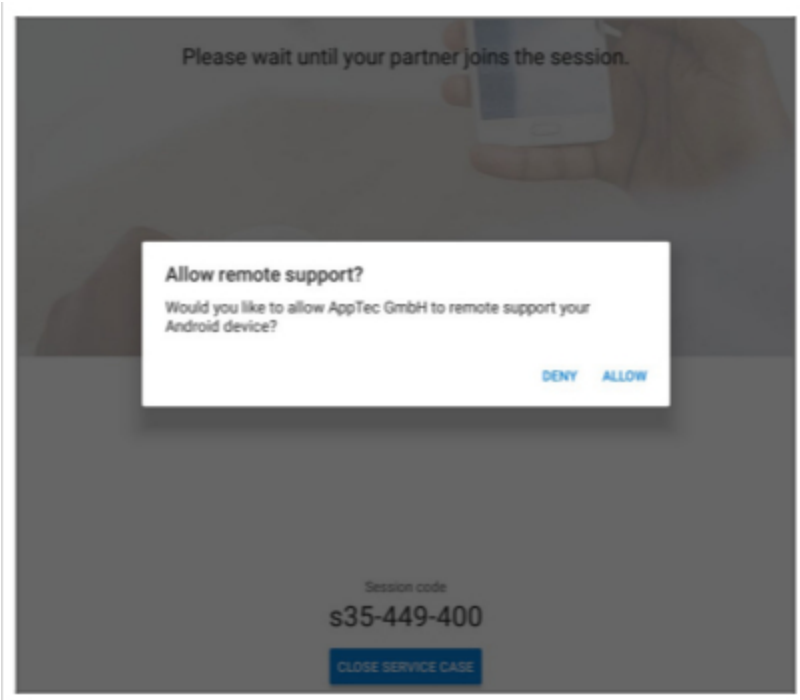
بعد بضع ثوانٍ سيظهر لك رابط لجلسة TeamViewer الخاصة بك. يمكنك النقر على "ابدأ" لفتح هذا الرابط في نافذة جديدة.


Search here ...
Root
Default Group
Test TV
Test TV
Edit Device
Clear Passcode
Lock Device
Delete Device
Wipe Device
Enterprise Wipe
Remove MDM
Send Message
TeamViewer Remote Control
Send Enrollment Request


Remote Control
Supporter URL: https://get.teamviewer.com/v13/
Click on "Start" to open the TeamViewer Remote Control in a new window.
Cancel
Start

سيؤدي هذا الرابط إلى فتح برنامج TeamViewer المثبت لديك وتوصيلك بجهازك.

عليك الآن تأكيد الاتصال على الجهاز نفسه للتحكم به عن بُعد.

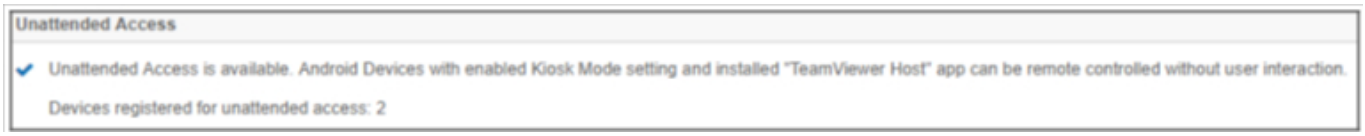


إذا كنت تستخدم نظام iOS فستتلقى رسالة في عميل AppTec360 MDM Client. باستخدام هذا الرابط سينضم الجهاز إلى الجلسة عن بُعد. اعتمادًا على إعدادات الإشعارات الخاصة بالجهاز، من الممكن ألا تتلقى إشعارًا ويتعين عليك فتح عميل AppTec360 MDM يدويًا.

في بعض أجهزة Android (مثل Samsung)، يلزم تثبيت تطبيق إضافي كإضافة على بعض أجهزة Android (مثل Samsung). سيعلمك تطبيق TeamViewer على الجهاز بذلك، إذا كان ذلك ضروريًا على جهازك.

الوصول غير المراقب

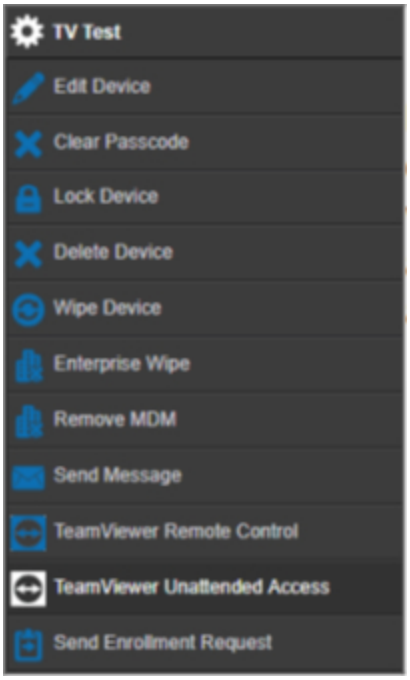
ملاحظة: الوصول غير المراقب ممكن فقط على أجهزة Android.



لا يمكنك الاتصال بأجهزتك، دون قبول الاتصال على الجهاز، إلا إذا كان حساب TeamViewer الخاص بك يستخدم ترخيص "Tensor" أو "Corporate".

يمكنك التحقق من ذلك، بعد ربط حسابك، في "الإعدادات العامة"

لاستخدام الوصول غير المراقب، يجب عليك تثبيت تطبيق "TeamViewer Host" وتفعيل "تمكين الوصول غير المراقب" ضمن "وضع الكشك والمشغل" في ملفك الشخصي. يرجى العلم أن هذا ممكن فقط إذا كنت تستخدم وضع الكشك.



يمكنك الآن تحديد الوصول غير المراقب إذا قمت بتحديد جهازك والنقر على العجلة. سيؤدي ذلك إلى توصيلك بجهازك دون الحاجة إلى أي تأكيد على الجهاز نفسه. يرجى الانتباه إلى أن الأمر قد يستغرق بعض اللحظات حتى تحصل على الرابط للوصول إلى جهازك.

سبلاش توب

إذا قمت بتمكين خيار Splashtop، سترى خيارات تكوين Splashtop في ملفاتك الشخصية.

لاستخدام Splashtop، عليك تعيين Splashtop Streamer (com.splashtop.streamer.csrs) كتطبيق إلزامي في ملفك الشخصي. بعد ذلك يمكنك تمكين تكوين Splashtop في ملفك الشخصي في "التحكم عن بعد". سيؤدي تمكين هذا إلى تهيئة تطبيق Splashtop Streamer. إذا كنت تستخدم تطبيق Splashtop Streamer ولكن ليس مع تطبيق MDM، فيجب عليك ترك هذا الأمر مغلقاً.

في ملفك الشخصي ضمن "التحكم عن بعد" عليك أيضًا تعيين رمز النشر. انتقل إلى https://my.splashtop.com وقم بتسجيل الدخول إلى حساب Splashtop الخاص بك. انقر على "إضافة كمبيوتر" وانسخ رمز النشر المكون من 12 رقمًا من الصفحة الناتجة.

بدون رمز النشر لا يمكن التحكم عن بُعد في النشر عن بُعد.

بعد القيام بذلك، يمكنك النقر بزر الفأرة الأيمن على جهازك وبدء جلسة عمل عن بُعد بالنقر على "Splashtop Remote Control"

إدارة بطاقة SIM

استيراد CSV مجمّع CSV

يعرض هذا نظرة عامة على بطاقات SIM المخصصة لك وجميع المعلومات المتعلقة بها. يساعدك هذا في الحصول على جميع المعلومات، ليس فقط حول أجهزتك ولكن أيضًا حول بطاقات سيم الخاصة بك في نظام واحد.

ملاحظة: هذه إدارة/توثيق يدوي. من غير الممكن الحصول على هذه البيانات تلقائيًا من الأجهزة بسبب آليات الخصوصية/الأمن الخاصة بأنظمة التشغيل.

يمكنك أيضًا استيراد هذه القائمة واستيرادها بصيغة CSV.

الناقل والتعريفة

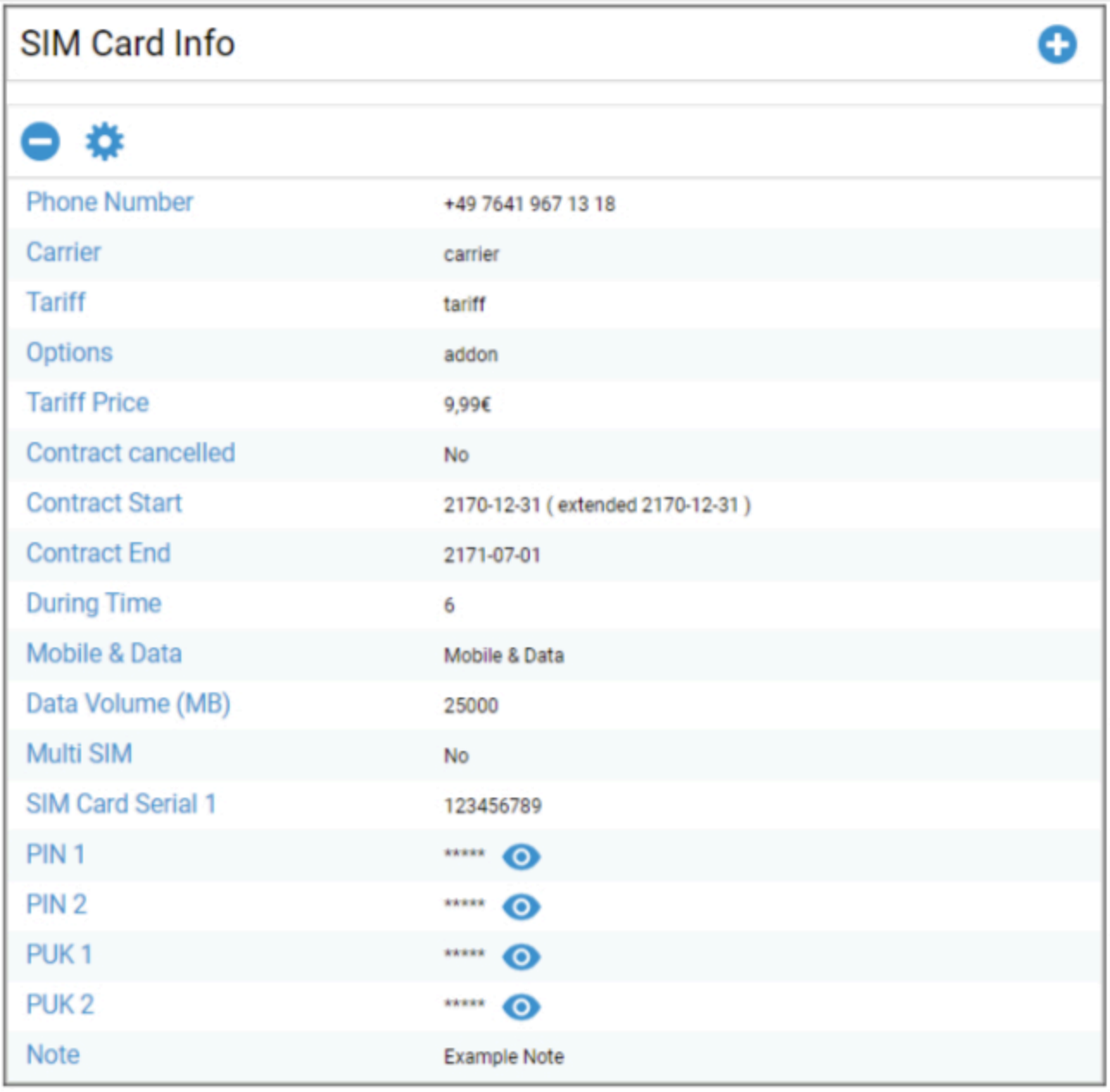
لإضافة بطاقة SIM، انقر أولاً على الزر لإضافة ناقل واحد أو عدة ناقلات.

بعد ذلك انقر على "+" في "معلومات التعريفة" لإضافة تعريفة إلى شركة نقل.

اختياريًا يمكنك إضافة الوظائف الإضافية الاختيارية أدناه إذا كان لديك شيء من هذا القبيل.

أعد هذا كل ما تحتاجه لإضافة بطاقة Sim فعلية. يتم تعيين بطاقات Sim حالياً لمستخدم. لذلك انتقل إلى إدارة الهاتف المتحرك، واختر مستخدمًا وانتقل إلى "نظرة عامة على بطاقة Sim Card.

هنا ترى بطاقات سيم الخاصة بهذا المستخدم. إذا كانت هناك واحدة، يمكنك تعديلها أو إزالتها. يمكن أن يكون لدى المستخدمين بطاقات سيم متعددة.

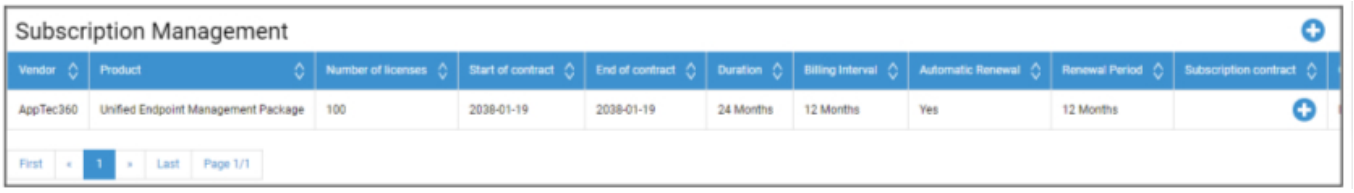


انقر على "+" لإضافة بطاقة SIM وإضافة جميع المعلومات التي تحتاجها. سيتم أيضًا إدراج بطاقات سيم هذه في قائمة جميع بطاقات سيم الخاصة بك في الإعدادات العامة → إدارة بطاقة سيم.

إدارة الاشتراكات

إدارة الاشتراكات

يمكنك هنا توثيق الاشتراكات الجارية وتفاصيلها وكذلك تخزين ملفات مختلفة، مثل العقد الموقع وخطاب الإنهاء وما إلى ذلك. يمكنك أيضًا إعداد تذكيرات تذكرك بالبريد قبل انتهاء الاشتراك وربما تمديده تلقائيًا.



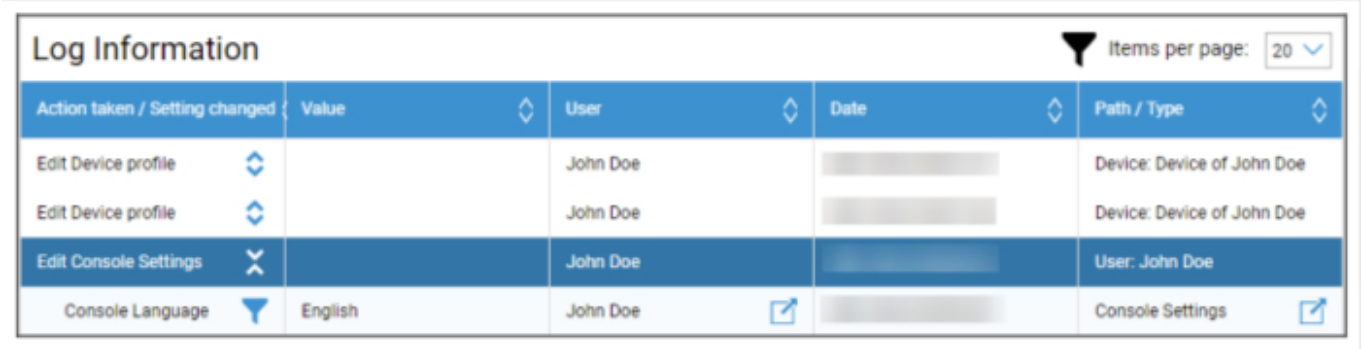
انقر على "+" في الأعلى لإضافة اشتراك. يمكنك إضافة أي عدد تريده من الاشتراكات.

انقر على "+" في الحقول المختلفة لتحميل الملفات المتعلقة بهذا الاشتراك. يمكنك من الناحية الفنية تحميل أي نوع من الملفات ولكن اعلم أنه لا يمكن معاينة كل نوع ملف في المتصفح.

سجل التدقيق العام

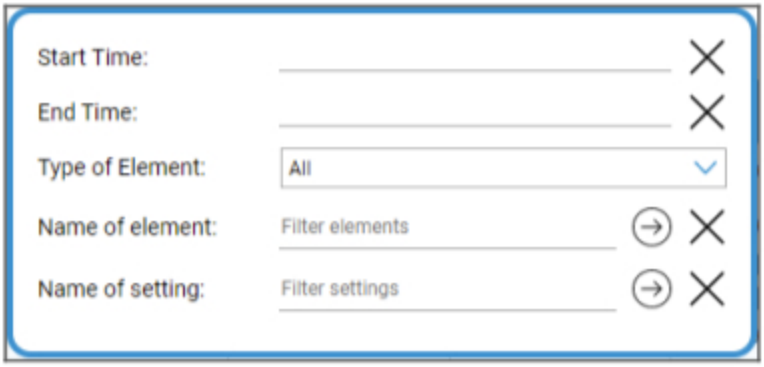
سجل التدقيق

هنا لديك سجل تدقيق عام يعرض جميع التغييرات التي تم إجراؤها. بينما يعرض سجل التدقيق في مستخدم أو مجموعة فقط التغييرات وفقًا لهذا المستخدم أو المجموعة، فإن هذا يعرض كل تغيير تم إجراؤه في أي مكان في وحدة التحكم.



يمكنك معرفة ما تم تغييره ومن قام بالتغيير ومتى وأين. في بعض الحالات يمكنك أيضًا توسيع الإدخال لرؤية المزيد من التفاصيل.

من الممكن النقر على المستخدم أو على الإدخال في "المسار/النوع" للوصول إلى الموقع الذي تم فيه التغيير.



في أعلى اليمين، يمكنك أيضًا تحديد عامل تصفية يمكن أن يساعدك في العثور على تغييرات معينة في بيئة تحدث فيها العديد من التغييرات.

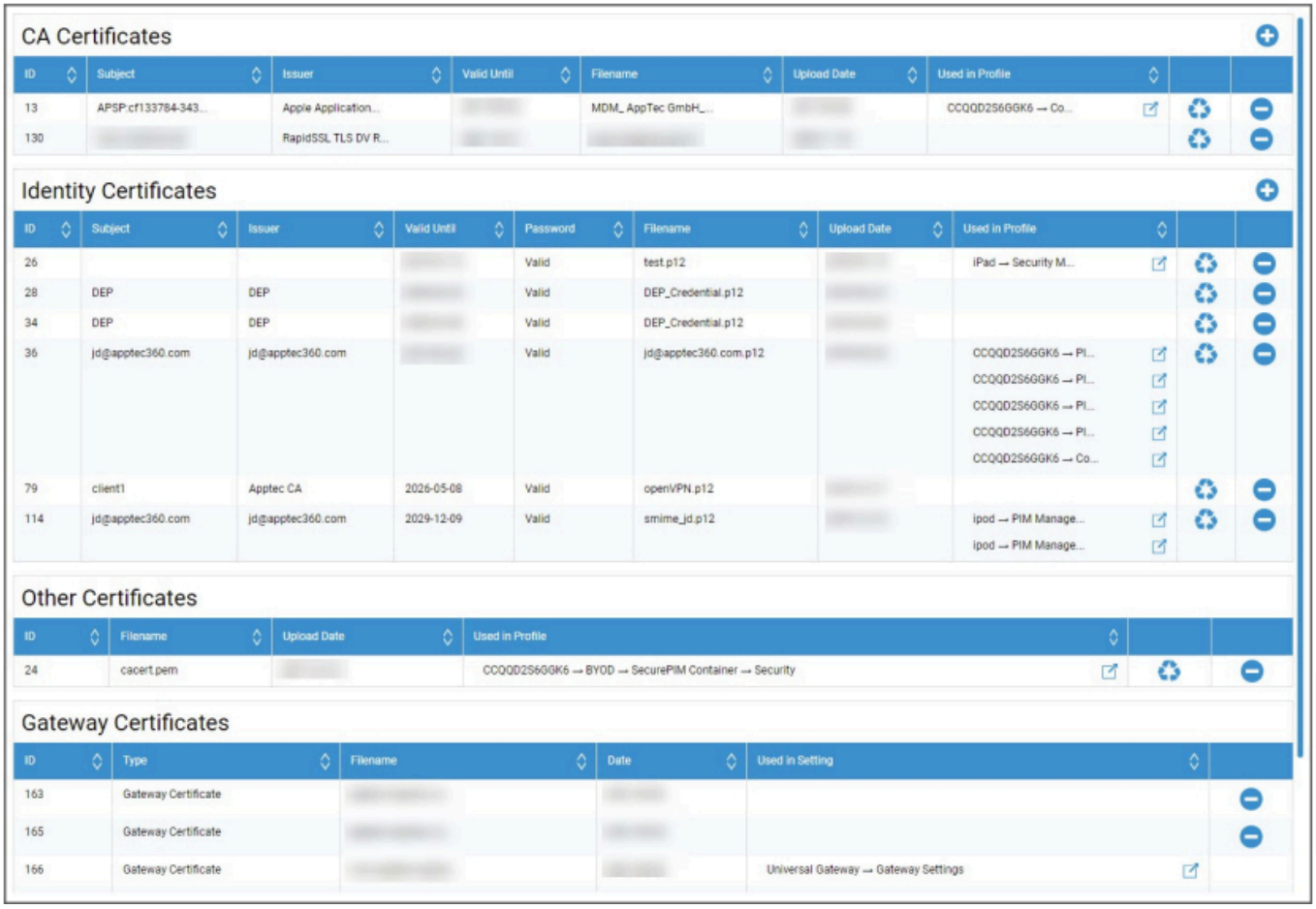
إعدادات سجل التدقيق

تحدد "فترة الاحتفاظ بسجلات التدقيق" مدة الاحتفاظ بسجلات التدقيق قبل حذفها.

إدارة الشهادات

ستحصل هنا على نظرة عامة على جميع الشهادات التي تم تحميلها واستخدامها في وحدة التحكم. هذه مجرد نظرة عامة. لا يزال يتم إجراء التكوين الفعلي لشهادات Wi-Fi على سبيل المثال في ملف التعريف في الموقع المقابل.

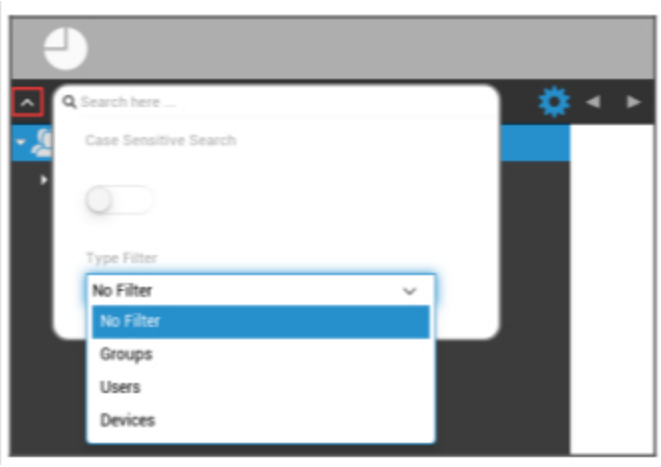
يمكنك هنا أيضًا إزالة الشهادات أو تحديثها، والتي ستنعكس تلقائيًا في الملفات الشخصية المتأثرة. انقر على المعلومات الموجودة في "مستخدمة في الملف الشخصي" لمعرفة أين لا تزال أي شهادة معينة بالضبط.



إدارة الهاتف المحمول

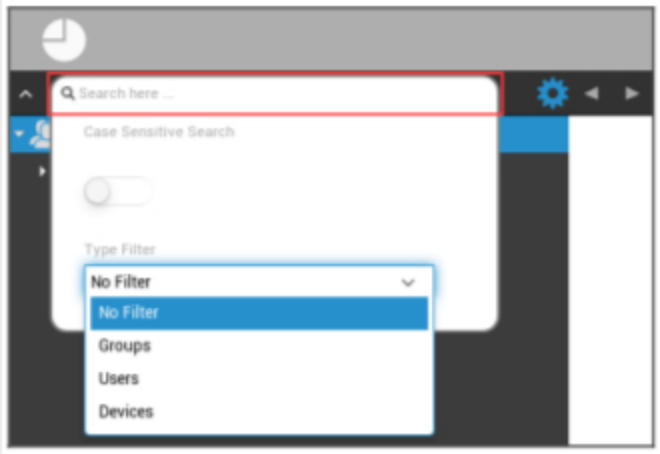
شاشة إدارة الهاتف المحمول

فلتر الجهاز



بنقرة واحدة في الزاوية العلوية اليسرى من الشاشة، يمكنك العثور على مجموعة متنوعة من الفلاتر لعرض الأجهزة.

نافذة البحث



تسمح لك نافذة البحث بالبحث في جميع الأجهزة و/أو المستخدمين باستخدام كلمة رئيسية محددة.

معدات الخيارات

بعد النقر على الرمز المعني، يتم عرض قائمة بالخيارات المتاحة لك.

هذه تتغير مع كل نافذة حالية ويتم شرحها في الفصول المعنية.

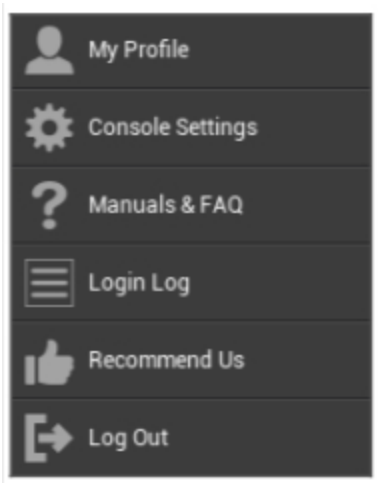
أسهم التنقل

بنقرة على السهم الأيسر، سيتم نقلك إلى الصفحة السابقة.

بعد ذلك، بنقرة على السهم الأيمن، سيتم نقلك إلى الصفحة التي غادرتها للتو.

إعدادات حساب الإدارة-الإدارة

يؤدي النقر على عنوان البريد الإلكتروني كما هو موضح أعلاه إلى عرض القائمة التالية:



ملفي الشخصي	تحرير تفاصيل حساب المدراء
إعدادات وحدة التحكم	تكوين إعدادات وحدة التحكم لحساب المسؤولين
الكتيبات والأسئلة الشائعة	عرض صفحة "الكتيبات والأسئلة الشائعة" في "الإعدادات العامة"
سجل تسجيل الدخول	الوصول إلى "سجل تسجيل الدخول"
أوصي بنا	عرض صفحة "التوصية بنا" في "الإعدادات العامة"
تسجيل الخروج	تسجيل الخروج من وحدة تحكم MDM

معلومات المستخدم

هنا يمكنك تعديل تفاصيل الحساب الخاص بالمشرف الذي قام بتسجيل الدخول حالياً.

اسم المستخدم	اسم المستخدم و/أو عنوان البريد الإلكتروني للحساب
الاسم	الاسم الأول للمسؤولين
الاسم العائلي	الاسم العائلي للمسؤولين
اسم تسجيل الدخول	اسم تسجيل دخول المسؤولين
عنوان البريد الإلكتروني	عنوان البريد الإلكتروني للمسؤولين
عنوان البريد الإلكتروني البديل	عنوان البريد الإلكتروني البديل للمسؤولين
صورة	صورة الملف الشخصي
رقم الهاتف	رقم هاتف المسؤولين
رقم الهاتف المحمول	رقم الهاتف المحمول للمسؤولين
تمديد الهاتف	امتداد الهاتف
الموقع	الموقع
المنصب	المنصب في الشركة
مجموعة المستخدمين	حدد مجموعة المستخدمين التي تريد تعيين حساب المسؤول إليها
تعليق	أدخل تعليقاً
أدخل كلمة مرور جديدة	أدخل كلمة المرور لتغيير كلمة المرور
كرر كلمة المرور الجديدة	كرر كلمة المرور الجديدة للتأكيد

يرجى ملاحظة أنه يمكن أيضًا تقديم وصول الإدارة كحساب مستخدم محلي في بنية التسلسل الهرمي. بدون إنشاء مسؤول إضافي، لا ينبغي حذف هذا الحساب دون إنشاء مسؤول إضافي!

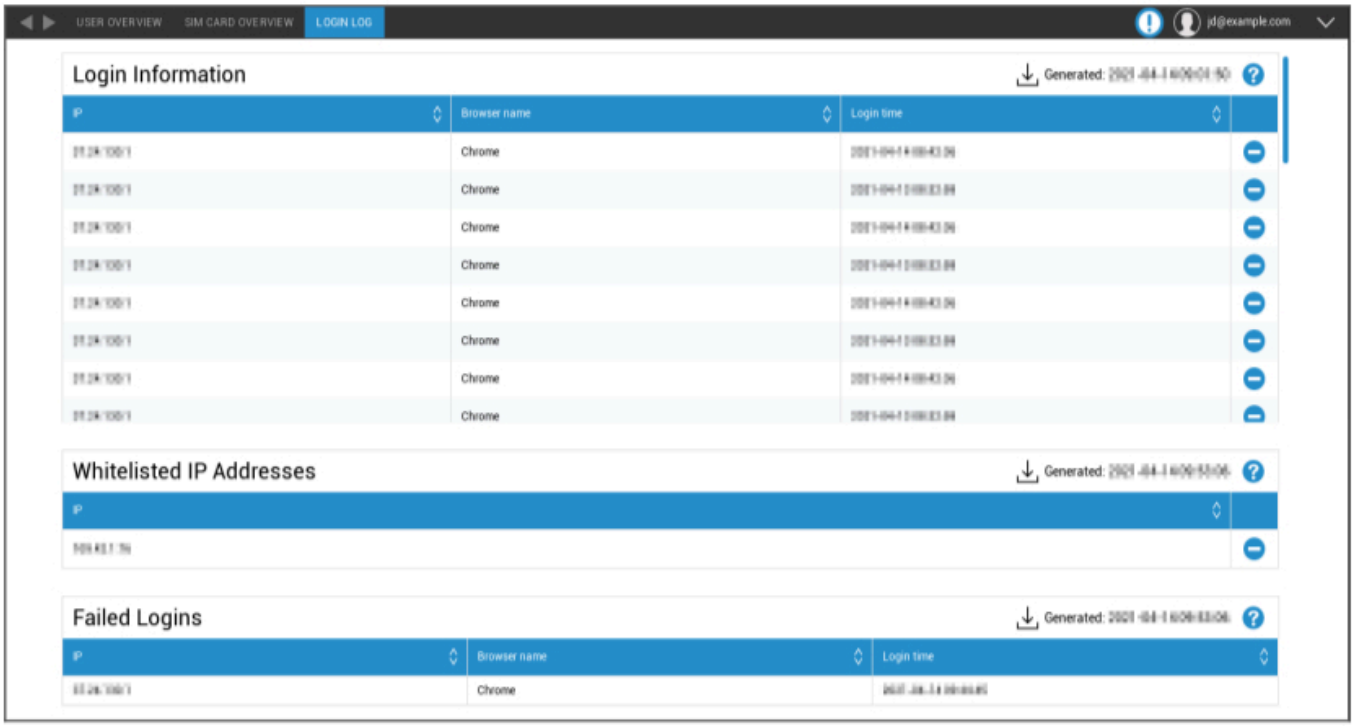
إعدادات وحدة التحكم

هنا يمكنك تكوين إعدادات وحدة التحكم التالية لحساب المسؤولين:

خيارات عرض دليل المستخدم الدليل	تحديد كيفية تصنيف المستخدمين في الشجرة
خيارات عرض جهاز الدليل	تحديد كيفية تسمية الأجهزة في الشجرة
مهلة الجلسة	إذا لم يفعل المستخدم أي شيء في الوقت المحدد، فسيتم تسجيل خروج المستخدم. القيمة الافتراضية هي 60 دقيقة. يرجى تسجيل الخروج وتسجيل الدخول مرة أخرى بعد تغيير هذا الإعداد.
المنطقة الزمنية	اختر المنطقة الزمنية المستخدمة
تنسيق الوقت	اختر كيفية عرض الطوابع الزمنية
لغة وحدة التحكم	اختر اللغة التي يجب عرض وحدة التحكم بها. تتوفر الإنجليزية والألمانية.
اللون الرئيسي	يمكنك تعيين اللون الذي سيتم استخدامه كأساس لنظام ألوان وحدة التحكم. يمكنك إما استخدام منتقي الألوان، أو إدخال لون بترميز HTML HEX. تعمل مُشكِّلات RGB مثل "وردي" و"أصفر" أيضًا.
حفظ الأمر	تركيبة المفاتيح لتشغيل الحفظ دون الضغط على زر "حفظ".
استخدام المصادقة الثنائية	تمكين استخدام المصادقة الثنائية عند تسجيل الدخول. سوف تتلقى رسالة بريد إلكتروني عند تسجيل الدخول تحتوي على رمز يجب عليك إدخاله لتسجيل الدخول.
مهلة المصادقة الثنائية العامل	قم بتعيين فترة زمنية لن تتم خلالها مطالبتك بمصادقة ثنائية بعد مصادقة ناجحة بالفعل.
إرسال رمز التحقق عبر	سيتم إرسال رمز التحقق إلى الخيارات المحددة. ستظهر رسالة الجهاز في تطبيق AppTec360 MDM على جميع أجهزة Android و iOS التي تخصك.
إرسال رسالة تسجيل الدخول بعد تسجيل الدخول	في حالة التمكين، سيتم إرسال بريد إلكتروني لكل تسجيل دخول من عنوان IP غير مدرج في القائمة البيضاء. يحتوي البريد الإلكتروني على معلومات حول تسجيل الدخول (مثل عنوان IP، المتصفح).

سجل تسجيل الدخول

هنا يمكنك الاطلاع على المعلومات المتعلقة بتسجيلات الدخول لحساب المسؤول الذي تم تسجيل دخوله حالياً.



معلومات تسجيل الدخول	قائمة تحتوي على عمليات تسجيل الدخول لحساب المسؤول الذي تم تسجيل دخوله حاليًا والتي تم تسجيلها بواسطة وحدة التحكم. تعرض هذه القائمة جميع عمليات تسجيل الدخول الناجحة في آخر 30 يوماً.
عناوين IP المدرجة في القائمة البيضاء	هذه قائمة بجميع عناوين IP المدرجة في القائمة البيضاء. إذا قمت بتسجيل الدخول من عنوان IP مدرج هنا فلن تصلك رسالة تسجيل الدخول. يمكنك إضافة عنوان IP إلى هذه القائمة من خلال النقر على الزر المجاور لإدخال في قائمة "معلومات تسجيل الدخول" أعلاه. يمكنك إزالة عنوان IP من هذه القائمة عن طريق النقر على الزر الموجود بجوار إدخال في هذه القائمة أو في قائمة "معلومات تسجيل الدخول" أعلاه.
عمليات تسجيل الدخول الفاشلة	هذه قائمة بجميع محاولات تسجيل الدخول الفاشلة في آخر 30 يوماً. إذا فشلت في إدخال كلمة المرور الصحيحة 3 مرات على الأقل خلال 20 دقيقة سيظهر إدخال في هذه القائمة. سيتم إبلاغك أيضاً بمحاولات تسجيل الدخول الفاشلة عبر البريد الإلكتروني.

الإدارة المؤسسية (العقدة الجذرية) في إدارة الهاتف المحمول

عند وصولك إلى العقدة الجذرية (المجموعة الأولى)، يمكنك إجراء مجموعة متنوعة من الإعدادات الخاصة بشركتك، فيما يتعلق بإدارة الهاتف المحمول.

إنشاء مجموعة فرعية	إنشاء مجموعة فرعية
إعادة تسمية العقدة الجذر	إعادة تسمية العقدة الجذرية (مثل اسم شركتك)
التسجيل الجماعي	تسجيل أجهزة/مستخدمين متعددين في نفس الوقت
التعيين الجماعي	تعيين ملف تعريف للمجموعات المعنية، بنظرة واحدة
إدارة التطبيقات السريعة	إرسال طلبات (إلغاء) التثبيت (التثبيت) للتطبيق إلى أجهزة المجموعات المعنية
استيراد مستخدم CSV	استيراد المستخدمين من CSV إلى المجموعة المعنية

إنشاء مجموعة فرعية

باستخدام "إنشاء مجموعة فرعية" يمكنك إنشاء مجموعة فرعية إضافية.

يمكنك تحديد المجموعة الفرعية التي يجب تعيين المجموعة الفرعية تحت أي مجموعة فرعية.

(بشكل افتراضي، يتم إنشاء مجموعة جديدة يتم تعيينها كمجموعة فرعية في العقدة الجذر)

إعادة تسمية العقدة الجذر

هنا يمكنك إعادة تسمية اسم الجذر الخاص بك. من الشائع استخدام اسم الشركة في هذه الحالة.

التسجيل الجماعي

باستخدام "التسجيل الجماعي" يمكنك تسجيل العديد من الأجهزة والمستخدمين.

يمكنك تحديد الطريقة التي يجب أن يتلقى بها المستخدم التسجيل مباشرة (البريد الإلكتروني؛ البريد الإلكتروني البديل؛ الرسائل النصية القصيرة)

اعتمادًا على الجهاز الذي سيستقبله المستخدم (iOS، Android، Windows Phone)، يمكنك وضع علامة على ذلك مباشرةً هنا.

يمكن هنا أيضًا التمييز بين ما إذا كان هاتفًا ذكيًا أو جهازًا لوحيًا، ويمكنك هنا أيضًا تحديد ما إذا كان هاتفًا ذكيًا أو جهازًا لوحيًا، حيث يجب عليك تحديده بشكل صحيح، مع وضع علامة اختيار.

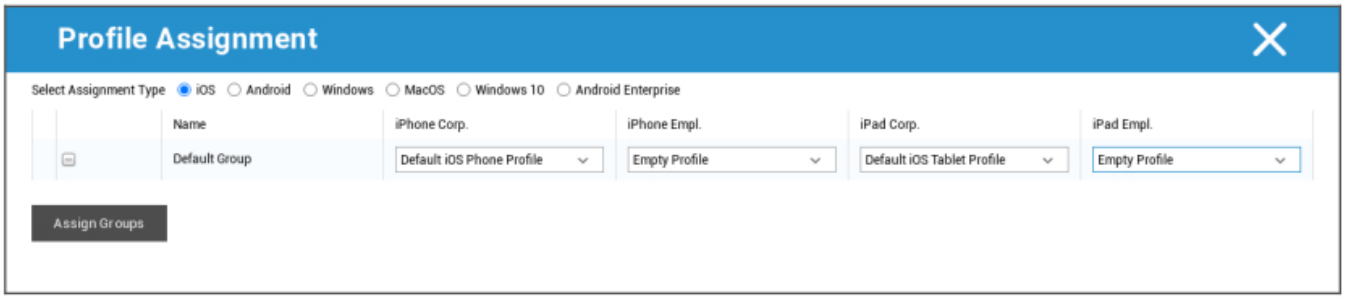
كخطوة أخيرة، يمكنك تحديد ما إذا كان الجهاز المعني خاصاً بالشركة أو خاصاً (BYOD).

باستخدام "تصدير كملف CSV"، يمكنك تصدير المعلومات كملف بيانات CSV. في المقابل، يمكنك أيضًا استيراد ملف بيانات CSV باستخدام "استيراد CSV"، يجب أن يبدو الملف مثل المثال أدناه:

فيليب ريس؛ philipp.reis@apptec360.com؛ pr@apptec360.com؛ +41 61 511 3210 511 3210

التعيين الجماعي

ضمن "التعيين الجماعي" يمكنك تعيين ملف تعريف لجميع المجموعات، وينقسم هذا إلى iOS - أندرويد - ويندوز - ماك أو إس - ويندوز 10 - أندرويد إنتربرايز

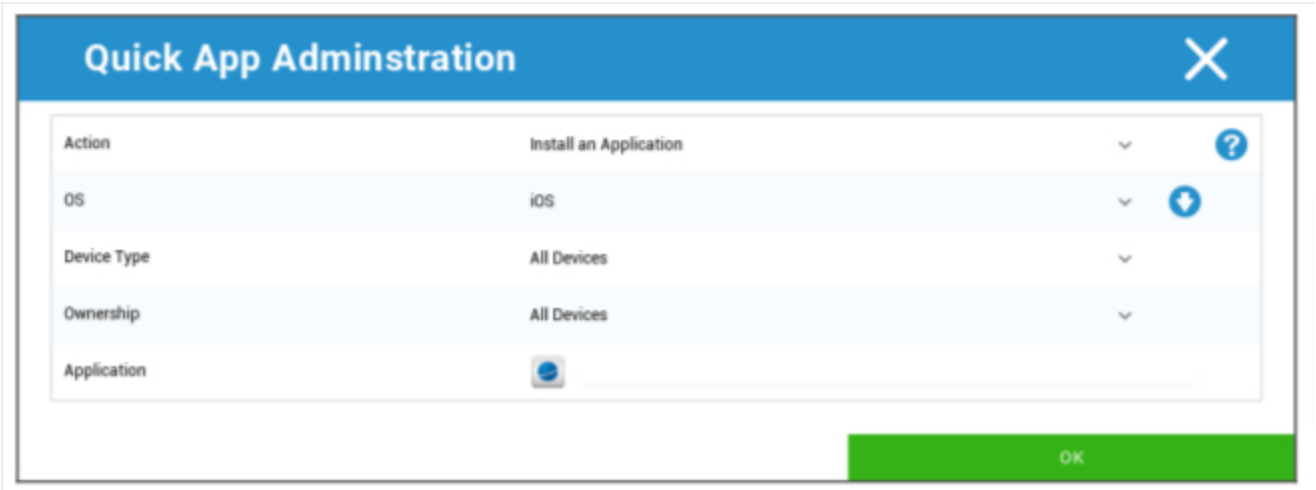


ويندوز - ماك أو إس - ويندوز 10 - أندرويد إنتربرايز

إدارة التطبيقات السريعة

ضمن إدارة التطبيقات السريعة، يمكنك إرسال طلبات التثبيت أو إلغاء التثبيت لتطبيق محدد إلى نظام تشغيل من اختيارك.

يمكنك أيضاً تحديد ما إذا كان يجب إرسال الطلب إلى جميع أنواع الأجهزة في نظام التشغيل المحدد أو إلى نوع جهاز محدد فقط.



استيراد مستخدم CSV

استيراد المستخدمين من CSV إلى المجموعة المعنية.

باستخدام "تنزيل قالب CSV"، يمكنك تصدير ملف قالب CSV، والذي يمكن ملؤه (أو يمكن استخدامه كمرجع).

يمكنك أيضًا استخدام الخيارين "إظهار معرفات الأدوار" و"إظهار معرفات المجموعات" كمرجع لإنشاء ملف CSV الخاص بك.

يمكن تحميل ملف CSV إلى MDM باستخدام "تحميل CSV".

كخطوة أخيرة، يمكنك بدء الاستيراد بالنقر على "بدء الاستيراد".

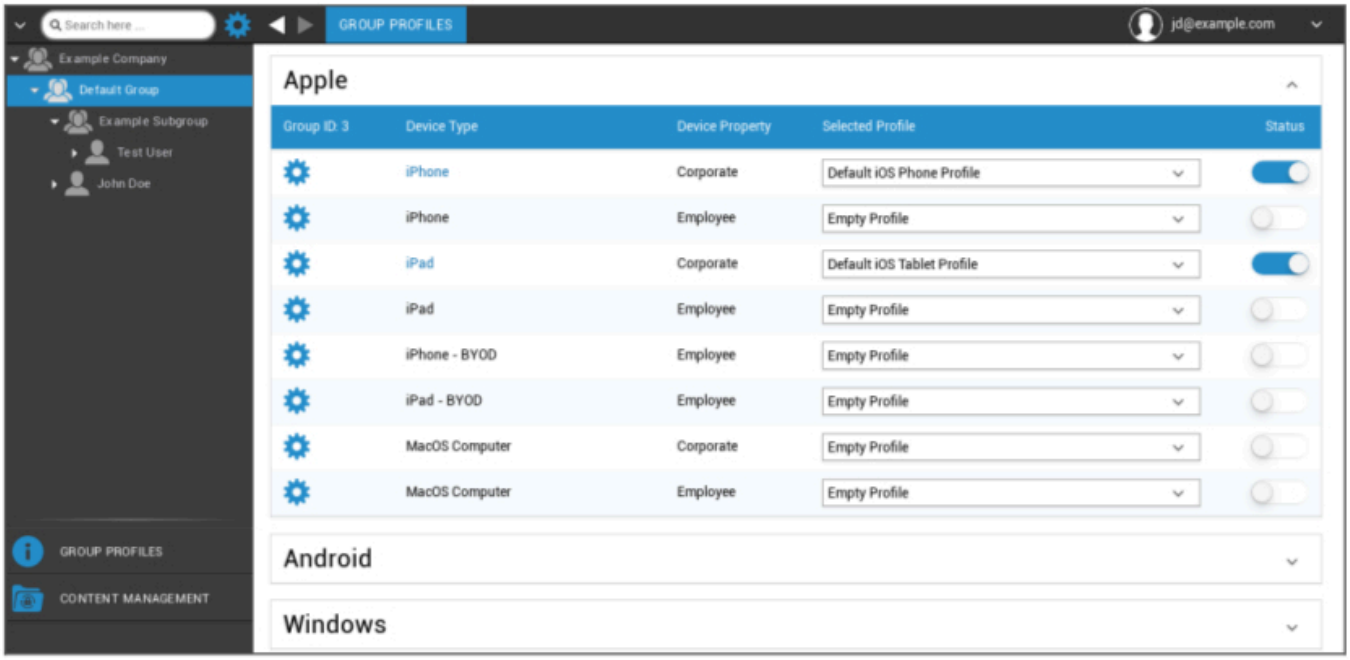
إدارة المجموعة في إدارة الأجهزة المحمولة

بنقرة واحدة على النظرة العامة تعرض ملفات تعريف التكوين المختلفة للأنظمة الأساسية المعنية.

يحتوي ملف تعريف واحد على جميع خيارات الإعدادات التي يمكن إنشاؤها باستخدام AppTec360 مسبقاً على جهاز المستخدم النهائي. على كل منصة يمكنك إنشاء ملفات تعريف لأجهزة الشركات (الشركات) أو أجهزة "أحضر جهازك الخاص" (الموظف).

من أجل التفريق بين التكوينات لمجموعات الأجهزة، على سبيل المثال بناءً على الموقع أو الوظيفة، يُنصح بإنشاء عدة مجموعات فرعية.

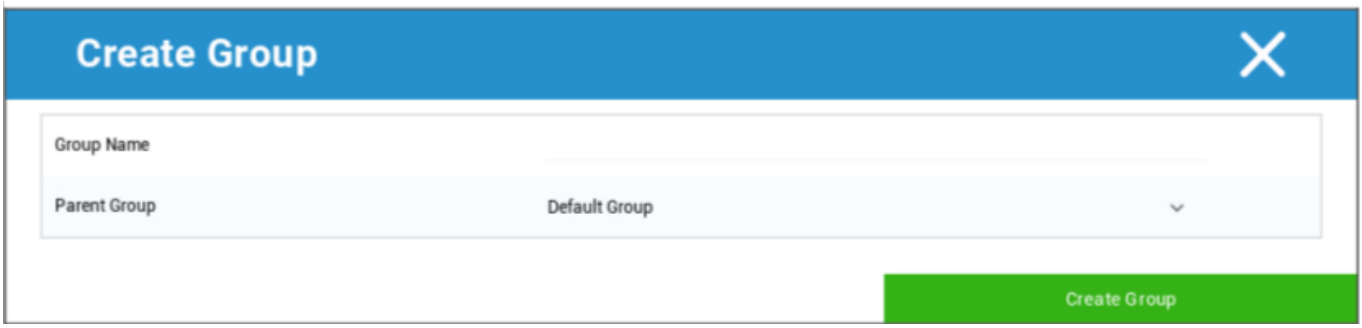
يرجى ملاحظة إدارة الملف الشخصي في إدارة الأجهزة المحمولة



باستخدام قائمة الترس يمكنك إعداد مجموعة متنوعة من الإعدادات للمجموعة (الفرعية) المعنية.

إنشاء مجموعة فرعية	إنشاء مجموعة فرعية للمجموعة (الفرعية) المعنية
تحرير المجموعة المحددة	تحرير المجموعة المحددة
حذف المجموعة المحددة	حذف المجموعة المحددة
التسجيل الجماعي	تسجيل العديد من الأجهزة/المستخدمين في وقت واحد للملف الشخصي المحدد
التعيين الجماعي	تعيين ملفات التعريف إلى المجموعة المحددة حالياً
إنشاء مجموعة فرعية	إنشاء مجموعة فرعية للمجموعة (الفرعية) المعنية
إنشاء مستخدم	إنشاء مستخدم للمجموعة (الفرعية) المعنية

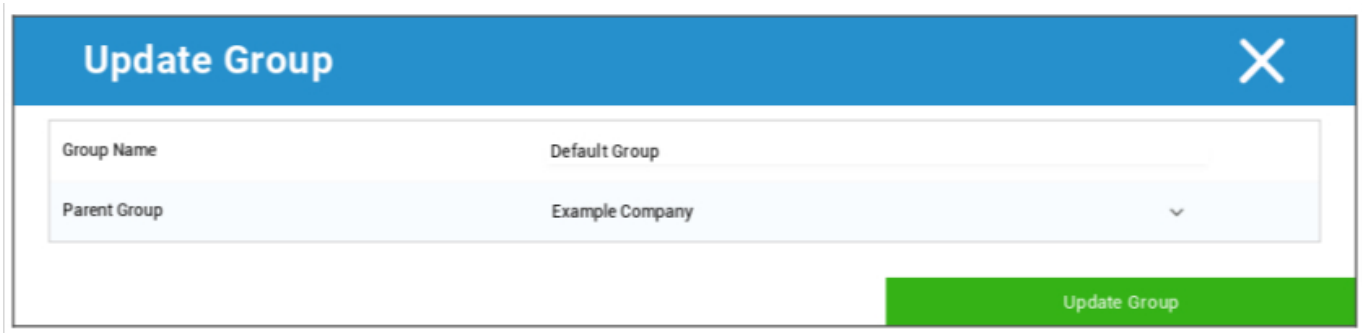
إنشاء مجموعة فرعية



باستخدام "إنشاء مجموعة فرعية"، يمكنك إنشاء مجموعة فرعية إضافية.

يمكنك تحديد المجموعة الفرعية التي سيتم تعيين المجموعة الفرعية تحت أي مجموعة فرعية (كإعداد افتراضي، يتم تعيين المجموعة الفرعية إلى المجموعة المحددة حاليًا).

تحرير المجموعة المحددة



هنا يمكنك تعديل الملف الشخصي - هنا، يمكن هنا تعديل الإعدادات التالية:

- يمكن تغيير اسم المجموعة
- يمكن تغيير مجموعة الوالدين

حذف المجموعة المحددة

ضمن "حذف المجموعة المحددة" يتم سرد جميع المستخدمين والأجهزة الموجودة في المجموعة المعنية. هنا، لديك خيار حذفها.

بالنسبة لمستخدم واحد يمكنك تنفيذ أوامر الحذف التالية:

حذف المستخدم	تم حذف المستخدم
نقل مستخدم إلى مجموعة:	يمكنك نقل المستخدم إلى مجموعة أخرى (العمود التالي، على سبيل المثال: المشرفون)

بالنسبة لجهاز واحد يمكنك تنفيذ أوامر الحذف التالية:

المسح والحذف	مسح الجهاز وحذفه
حذف من النظام	إزالة الجهاز فقط من AppTec

المرجع: التسجيل الجماعي

المرجع: التعيين الجماعي

إنشاء مستخدم

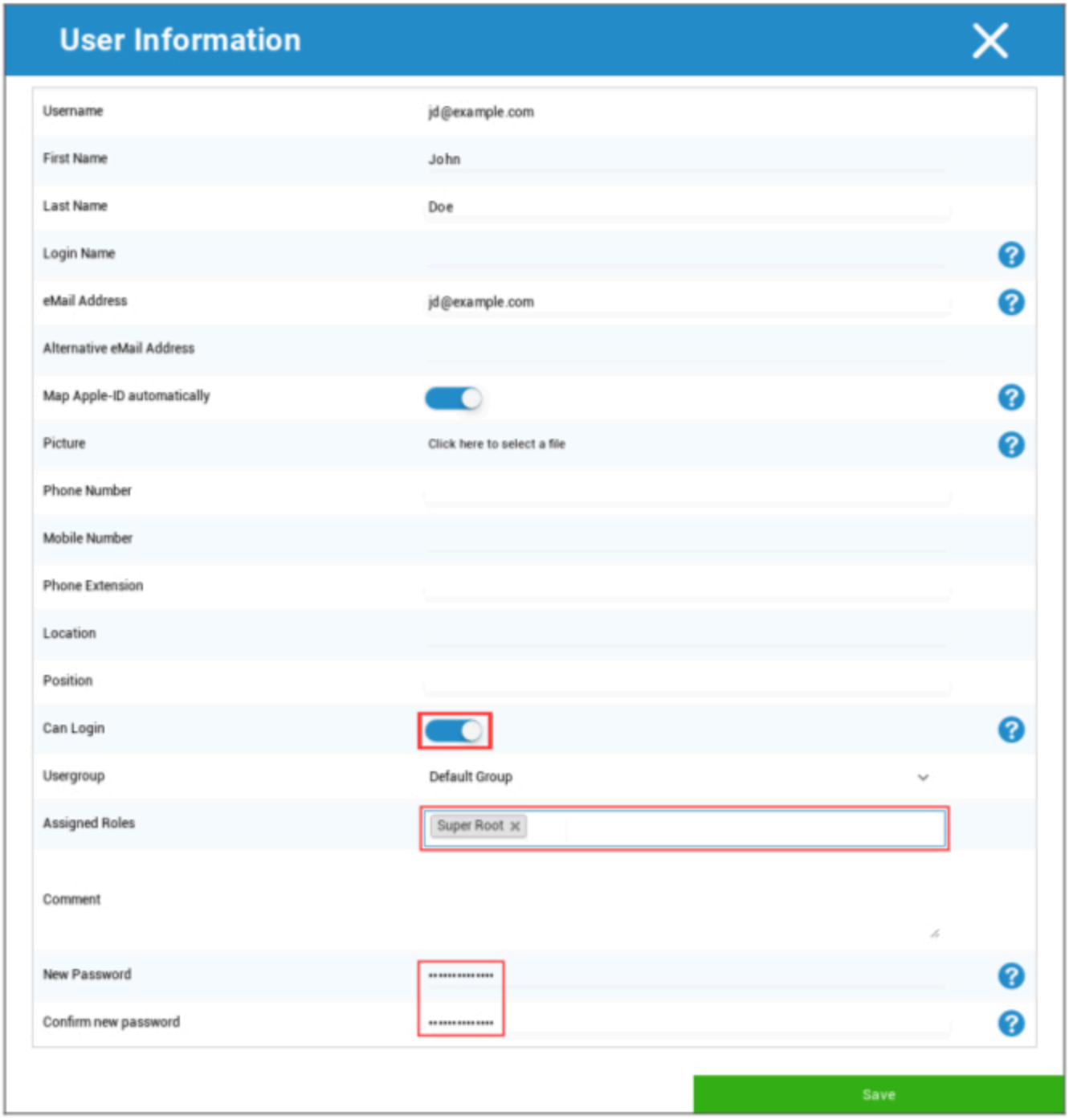
باستخدام "إنشاء مستخدم"، يمكنك إضافة مستخدم جديد.

إنشاء مستخدم-مسؤول-مستخدم جديد

يمكنك تعيين مستخدم كمستخدم مسؤول-مستخدم. سيمنحه القيام بذلك صلاحيات تسجيل الدخول إلى وحدة التحكم وكذلك تغيير المستخدمين/المجموعات/الأجهزة.

إنشاء مستخدم عادي أو استخدام مستخدم موجود. اختر المستخدم الذي تريد منحه صلاحيات المسؤول، وانقر على العجلة واختر "تعديل المستخدم":

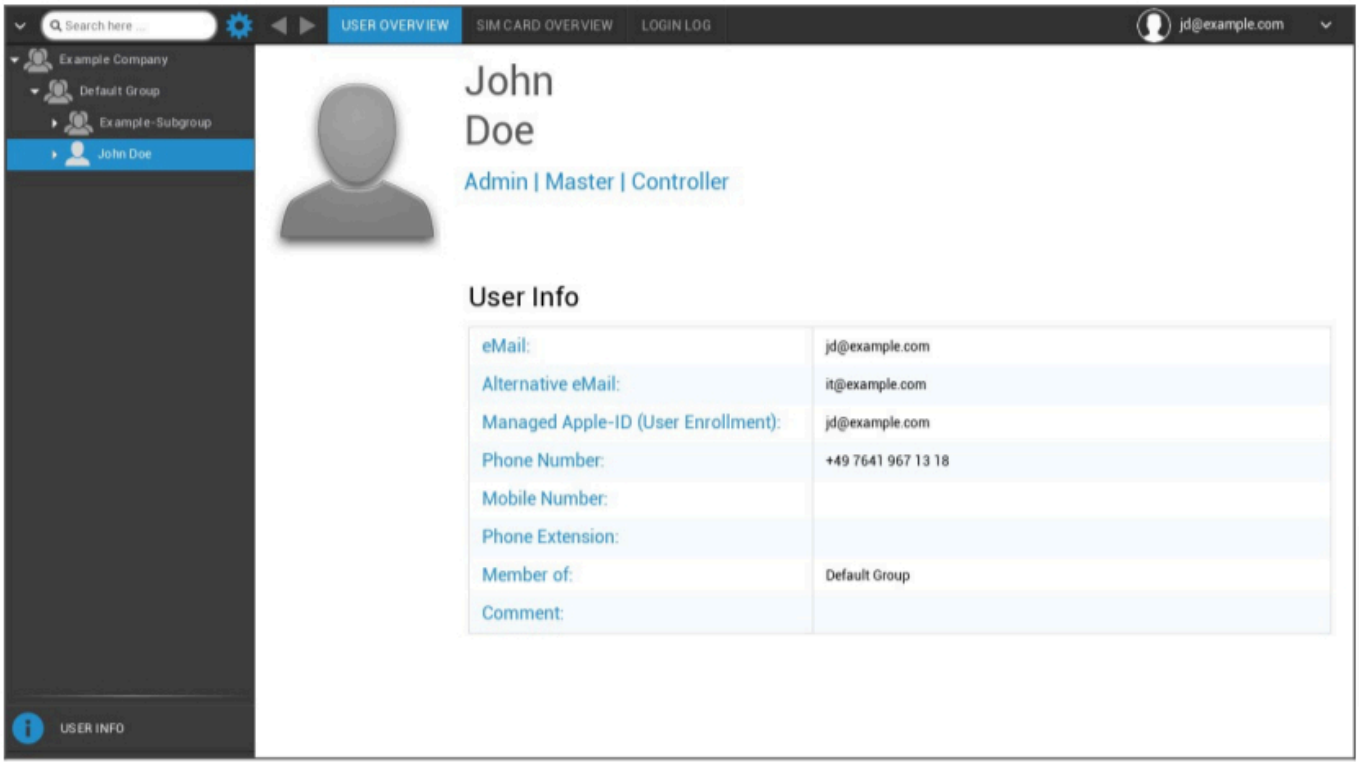
قم بتنشيط مفتاح "إمكانية تسجيل الدخول"، وقم بتعيين دور "الجذر الفائق" للمستخدم وقم بتعيين كلمة مرور.



احفظ هذا ويمكن للمستخدم الآن تسجيل الدخول باسم المستخدم وكلمة المرور.

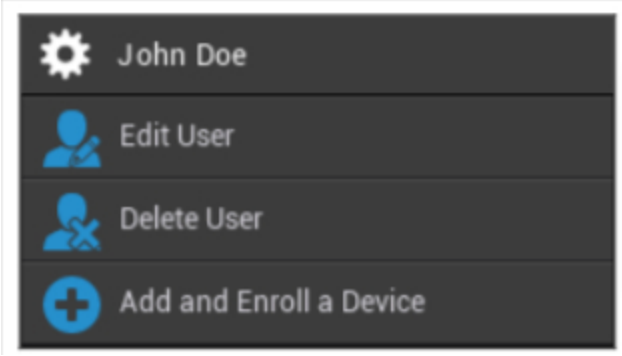
إدارة المستخدم في إدارة الهاتف المحمول

عند تحديد مستخدم معين، سترى النظرة العامة التالية:



ستتلقى نظرة عامة على جميع المعلومات التي أدخلتها سابقاً في "إنشاء مستخدم".

باستخدام الترس المثبت في الأعلى، يمكنك إجراء التكوينات التالية:



اسم المستخدم	اسم المستخدم المستخدم المحدد
تحرير المستخدم	تحرير معلومات المستخدم
حذف المستخدم	حذف المستخدم • الحذف من النظام = ستتم إزالة الجهاز من AppTec

	• المسح والحذف = ستتم استعادة الجهاز إلى إعدادات المصنع وإزالته من AppTec
إضافة جهاز وتسجيله	تسجيل جهاز للمستخدم المحدد

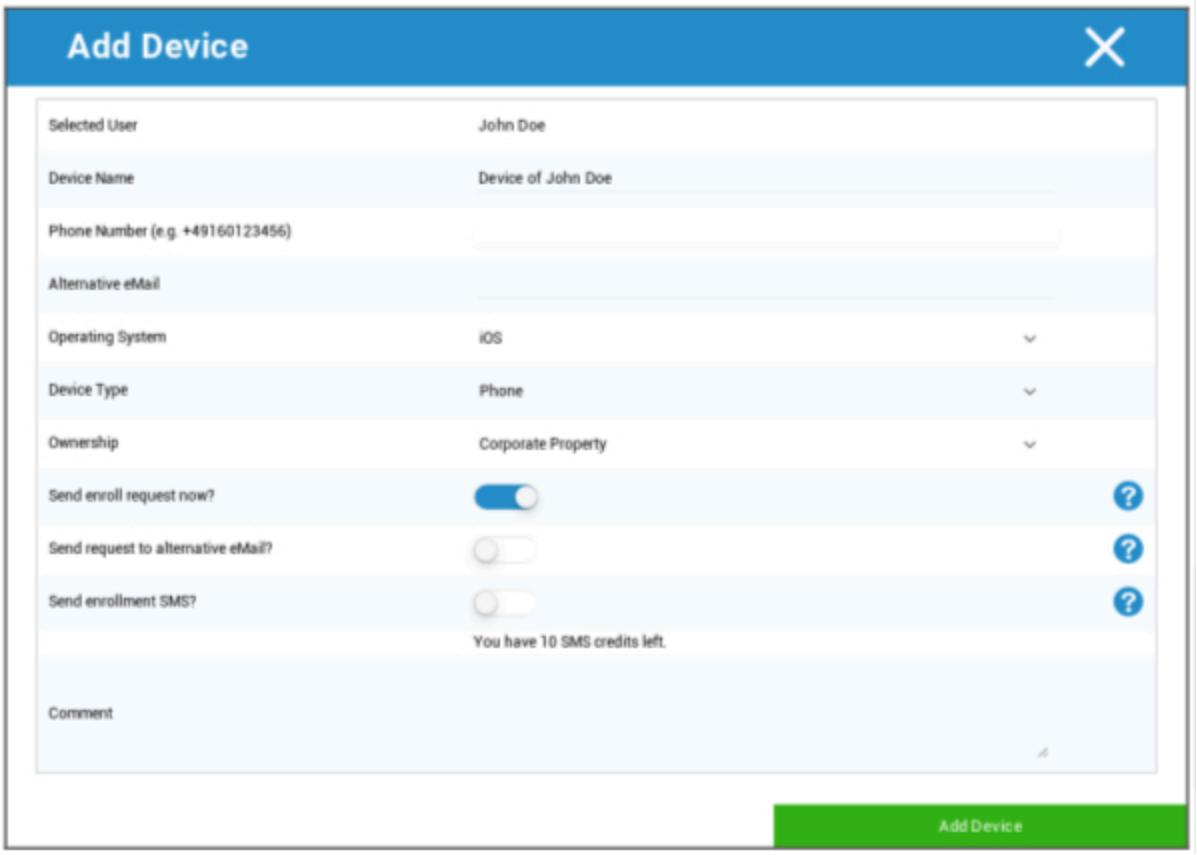
يرجى ملاحظة أنه يمكن أيضًا تقديم وصول الإدارة كحساب مستخدم محلي في بنية التسلسل الهرمي. بدون إنشاء مسؤول إضافي، لا ينبغي حذف هذا الحساب دون إنشاء مسؤول إضافي!

إضافة جهاز وتسجيله

هنا يمكنك تحديد جهاز للاستخدام المحدد.

بدلاً من ذلك يمكنك تسجيل الأجهزة في مجموعة مباشرةً. للقيام بذلك، انقر على المجموعة، ثم انقر على العجلة وحدد "إضافة جهاز وتسجيله".

يجب أن ترى النظرة العامة التالية:



بناءً على نوع الجهاز الذي تريد تسجيله، يجب عليك إجراء التكوينات التالية:

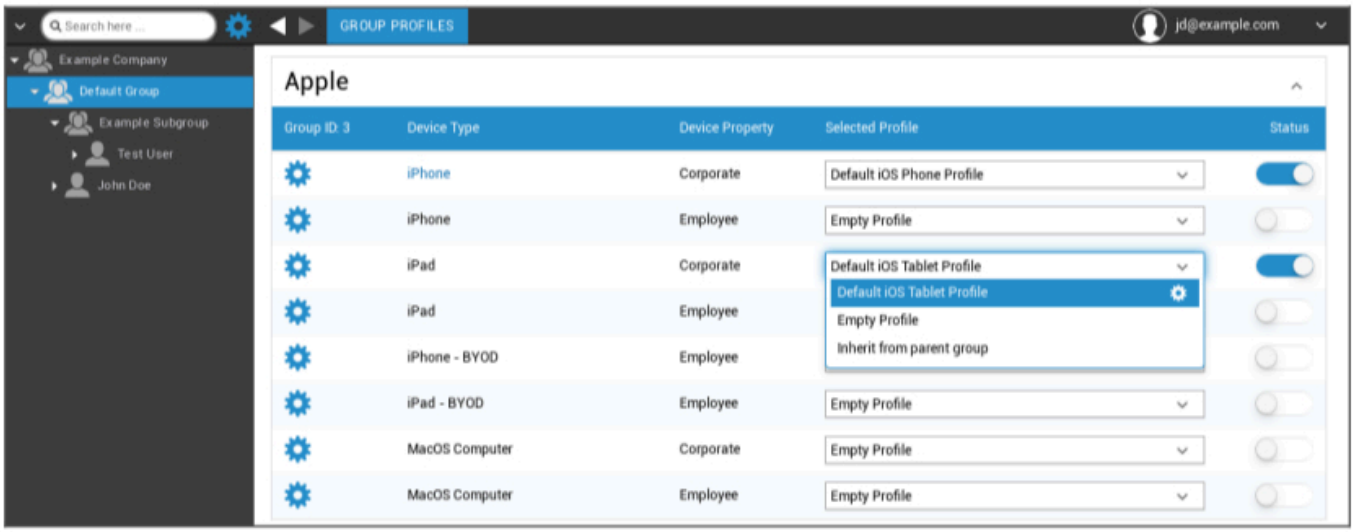
المستخدم المختار	المستخدم المحدد (سيتم تعبئته تلقائياً)
اسم الجهاز	سيتم تعبئته تلقائيًا (جهاز "اسم المستخدم") - ومع ذلك، يمكن تغييره
رقم الهاتف	رقم الهاتف، سيتم تعبئته تلقائيًا (طالما تم توفيره من قبل المستخدم) - هنا يمكن إضافته أو تغييره
البريد الإلكتروني البديل	البريد الإلكتروني البديل، سيتم ملء البريد الإلكتروني البديل تلقائيًا (طالما تم توفيره من قبل المستخدم) - هنا، ومع ذلك، يمكن إضافته أو تغييره
مالك الجهاز	ممتلكات الشركات = جهاز الشركات ممتلكات الموظف = جهاز BYOD
اختر نظام التشغيل	هنا، يمكنك الاختيار بين أنظمة التشغيل التالية: • iOS • نظام التشغيل iOS BYOD (تسجيل المستخدم) • نظام التشغيل MacOS • أندرويد إنتربرايز • أندرويد • ويندوز موبايل • ويندوز 10
إرسال طلب التسجيل؟	يتم إرسال البريد الإلكتروني على الفور إلى عنوان البريد الإلكتروني الرئيسي ويُطلب من المستخدم توصيل جهازه
إرسال طلب إلى بريد إلكتروني بديل؟	إرسال البريد الإلكتروني بشكل إضافي أو حصري (في حال تم إلغاء تفعيل "إرسال طلب التسجيل؟") إلى عنوان البريد الإلكتروني البديل (البريد الإلكتروني يختلف عن البريد الإلكتروني "العادي" لطلب التسجيل)
إرسال رسالة نصية قصيرة للتسجيل؟	إرسال طلب تسجيل عبر رسالة نصية قصيرة (يجب إدخال "رقم الهاتف")

بعد إرسال طلب التسجيل، سيتم عرض الجهاز (باللون الأحمر) على الفور.

بمجرد أن يتم توصيل الجهاز بنجاح، سيتم وضع علامة خضراء على الجهاز بعد فترة وجيزة من ذلك ويكون بذلك جاهزاً لتلقي القيود والتطبيقات وما إلى ذلك.

إدارة الملفات الشخصية في إدارة الهاتف المحمول

بعد النقر على مجموعة، ستتلقى نظرة عامة على جميع الأنظمة الأساسية للأجهزة التي سيتم تهيئتها والملفات الشخصية المعينة على التوالي.



	تنفيذ التكوين لملف التعريف المحدد
نوع الجهاز	نوع الجهاز و/أو طراز الجهاز
خاصية الجهاز	مالك الجهاز (الشركة = ملكية الشركة، الموظف = جهاز الموظف الخاص)
نبذة مختارة	ملف التعريف المحدد (يفتح الترس حوار تكوين ملف التعريف)
الحالة	تشغيل/إيقاف تشغيل (يتم تنشيط/إلغاء تنشيط الملف الشخصي)

عند تحديد الترس ستتلقى الخيارات التالية:

إنشاء ملف تعريف

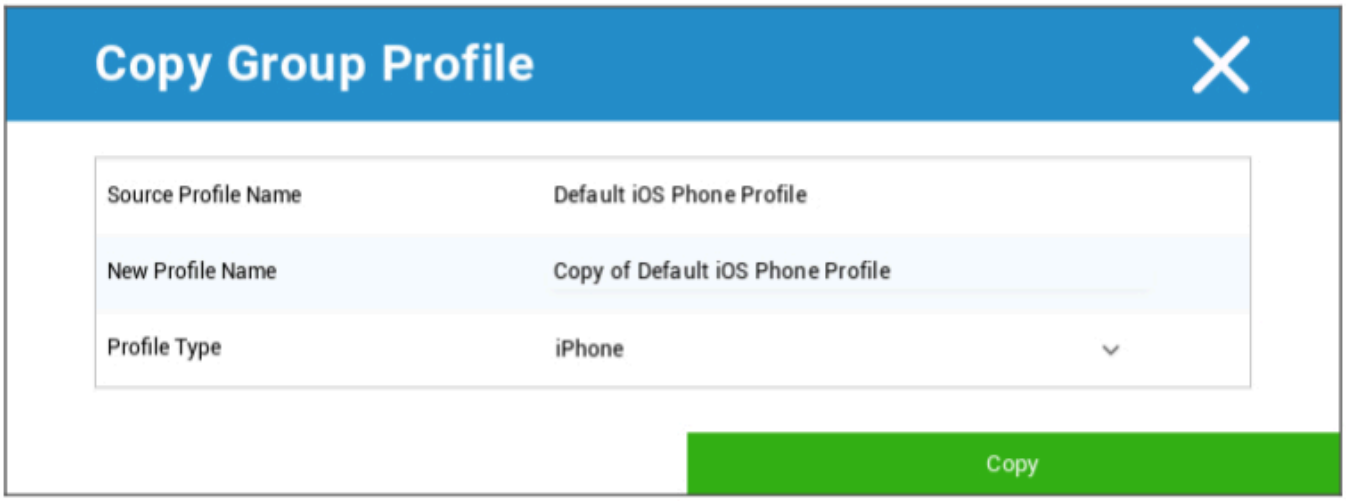
يمكنك إنشاء وتكوين ملف تعريف جديد لكل إدخال و/أو منصة. بعد النقر على هذه النقطة الفرعية، سيتم إنشاء الملف الشخصي على الفور ويمكنك البدء بتهيئة نظام iOS و Android و Windows Phone على الفور.

تعديل الملف الشخصي

بعد النقر على "تعديل الملف الشخصي"، ستصل إلى شاشة عرض التكوين للملف الشخصي المعني، حيث يمكنك ضبط التكوينات.

ملف تعريف النسخ

بمساعدة وظيفة "نسخ ملف التعريف"، يمكنك نسخ الإعدادات/الإعدادات من ملف تعريف موجود بالفعل وإضافتها إلى ملف تعريف جديد.

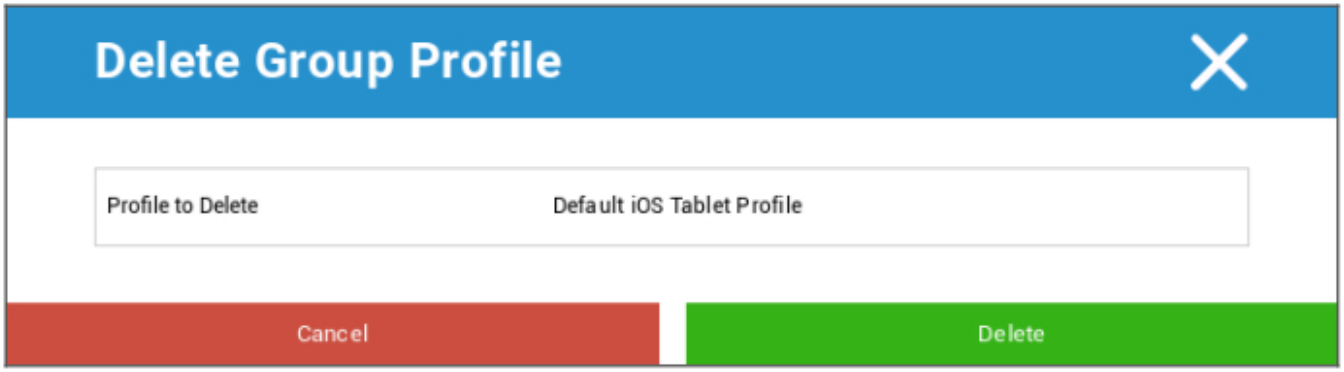


اسم الملف الشخصي للمصدر	اسم الملف الشخصي المراد نسخه
اسم الملف الشخصي الجديد	اسم الملف الشخصي الجديد
نوع الملف الشخصي	نوع الملف الشخصي (هاتف/جهاز لوحي)

بمجرد النقر على "نسخ"، سيتم إنشاء ملف التعريف ويمكن الآن تعيينه إلى المجموعة

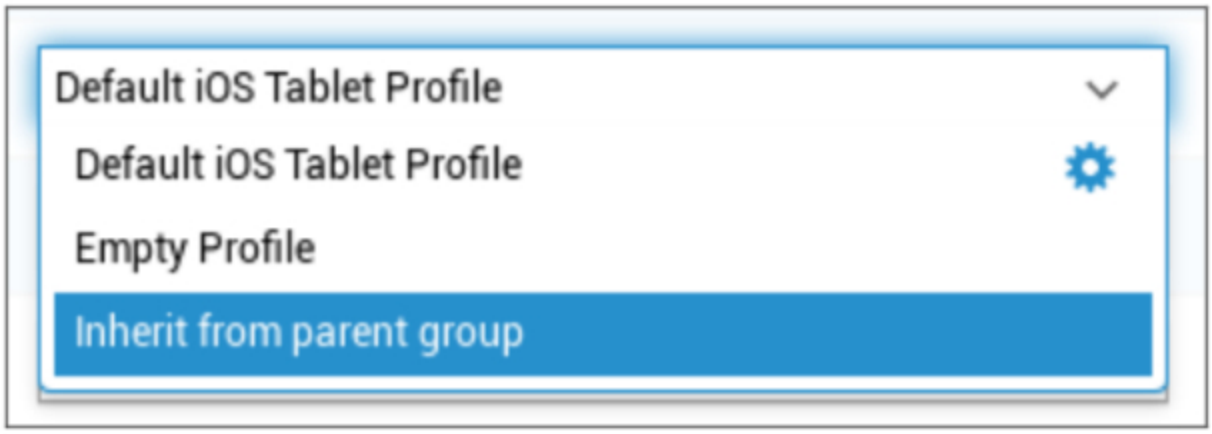
حذف الملف الشخصي

هنا يمكنك حذف ملف تعريف بشكل دائم. يُرجى ملاحظة أنه أثناء عملية الحذف وعملية "التعيين الآن" التالية للملف الشخصي، سيختفي التكوين على الأجهزة المعنية في المجموعة المتأثرة ولا يمكن استعادته!


Delete Group Profile
Profile to Delete
Default iOS Tablet Profile
Cancel
Delete

توريث الملفات الشخصية

أثناء اختيار ملفات التعريف، يتوفر خيار "التوريث من المجموعة الأم".



عندما يتم تنشيط ملف التعريف، سيتم استخدام ملف التعريف الخاص بالمجموعة الأم للجهاز المحدد على التوالي (ونوع الجهاز المعني). يرجى ملاحظة أن التغييرات في هذا الملف الشخصي قد تؤثر على العديد من المجموعات.

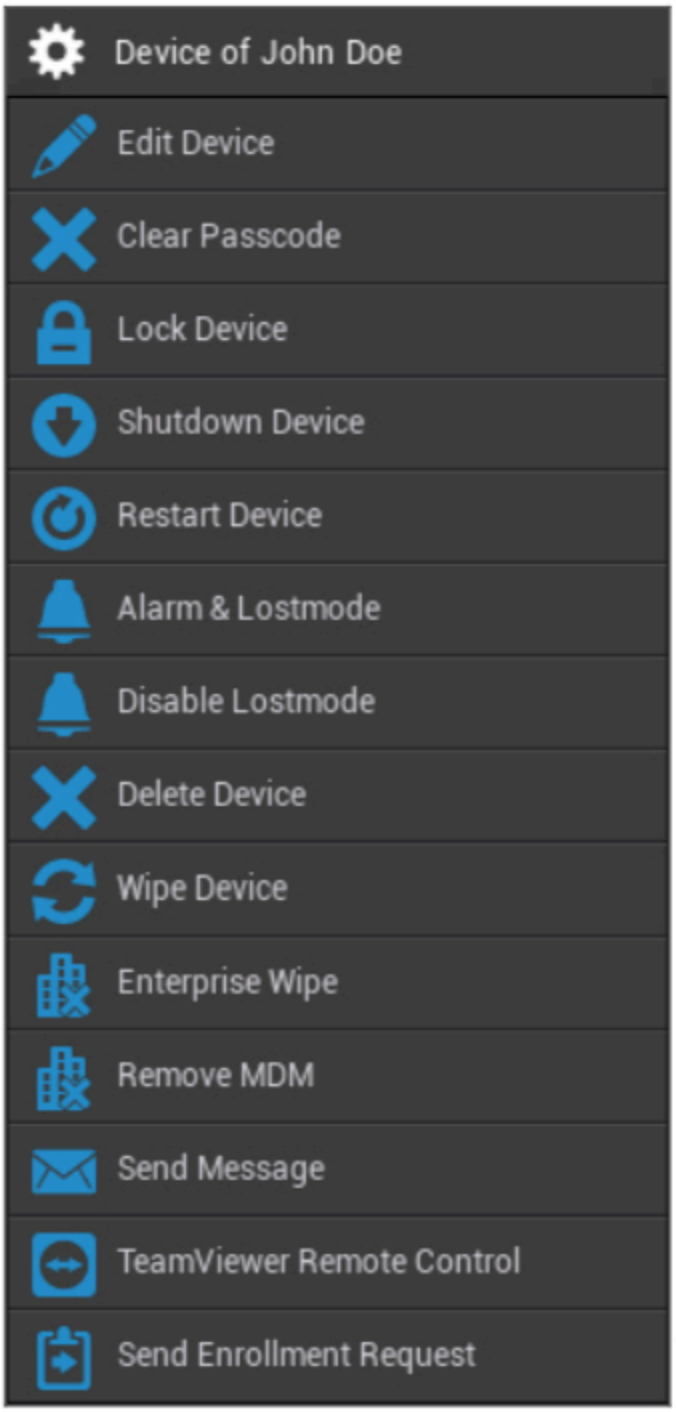
يتم تعيين هذا التكوين كقيمة افتراضية، عند إنشاء مجموعة فرعية جديدة.

يتوفر أيضًا التكوين "ملف تعريف فارغ"، والذي يتوافق مع ملف تعريف فارغ، مما يعني أنه في النهاية لن يتم إجراء أي تكوينات جديدة على جهاز المستخدم النهائي.

إدارة الأجهزة في إدارة الأجهزة المحمولة

عند تحديد جهاز، يمكنك تنفيذ مجموعة متنوعة من المهام عبر "الترس". تختلف هذه المهام باختلاف منصات أنظمة التشغيل (iOS، أندرويد إنتربرايز، أندرويد، ويندوز موبايل، ويندوز 10).

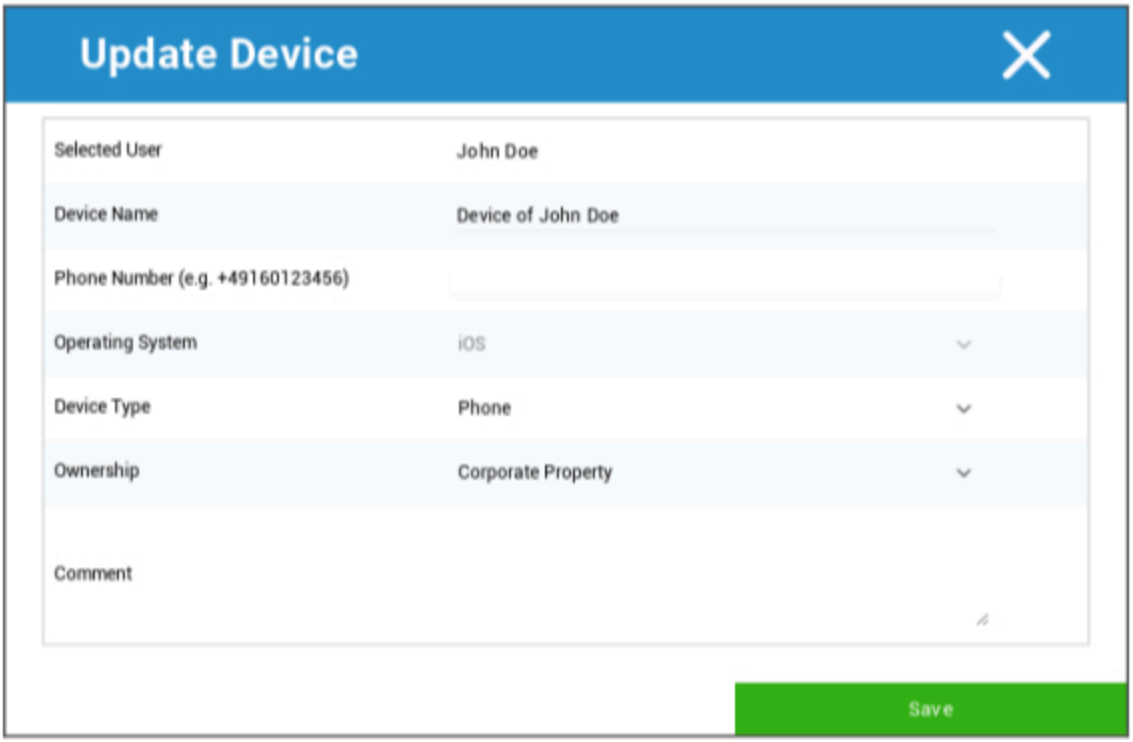
نظام التشغيل IOS



تحرير الجهاز	تحرير الجهاز
مسح رمز المرور	تم مسح رمز مرور الجهاز
قفل الجهاز	قفل الجهاز (قفل الشاشة)
جهاز إيقاف التشغيل	جهاز إيقاف التشغيل

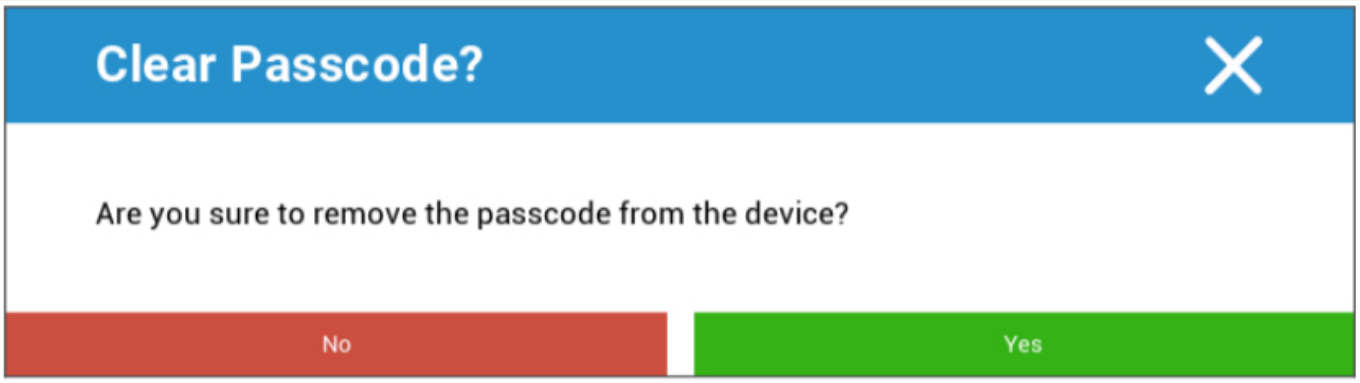
إعادة تشغيل الجهاز	إعادة تشغيل الجهاز
الإنذار ووضعية الضياع	بدء الإنذار ووضعية الضياع
تعطيل الوضع المفقود	تعطيل الوضع المفقود
حذف الجهاز	إزالة الجهاز من AppTec
جهاز المسح	استعادة الجهاز إلى إعدادات المصنع
مسح المؤسسات	يتم حذف المعلومات والتطبيقات والملفات الشخصية التي توفرها AppTec360 (يتم فصل الجهاز عن إدارة الأجهزة المتعددة الوسائط)
إزالة MDM	
إرسال رسالة	إرسال الإشعارات الفورية إلى الجهاز سيتم عرض الرسالة في تطبيق AppTec360 (علامة تبويب الرسائل)
برنامج TeamViewer للتحكم عن بُعد	بدء جلسة التحكم عن بُعد باستخدام برنامج TeamViewer
إرسال طلب التسجيل	إرسال طلب تسجيل (متكرر)

تحرير الجهاز



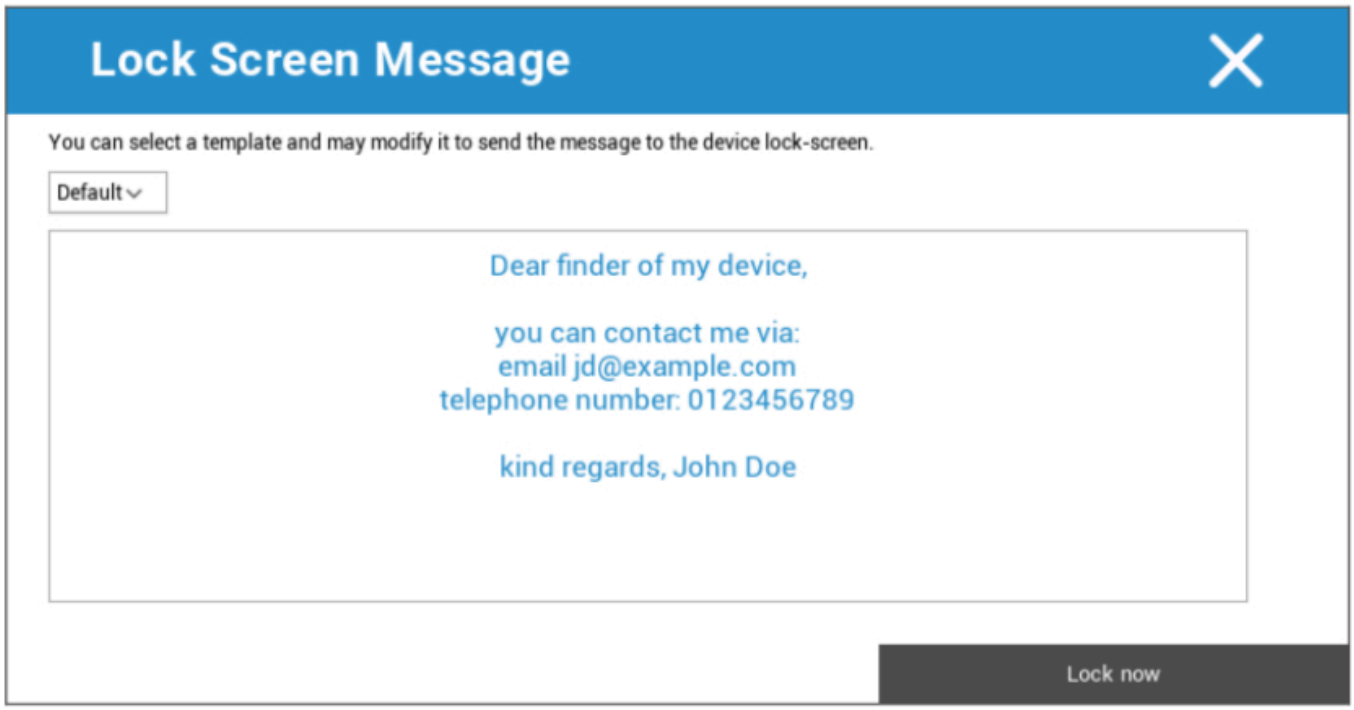
هنا يمكنك تحديث مجموعة متنوعة من المعلومات على الجهاز.

مسح رمز المرور



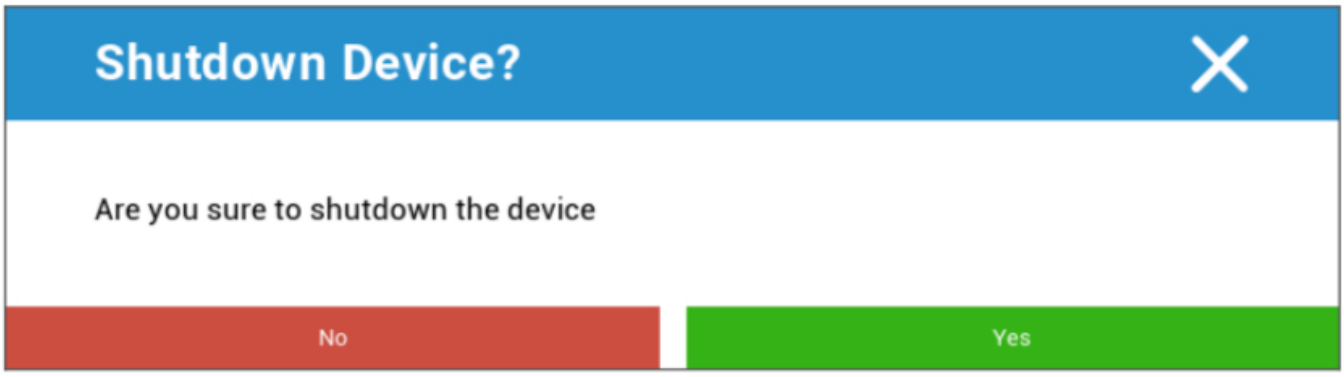
ضمن "مسح رمز المرور" يمكنك إزالة رمز المرور من الجهاز عن بُعد. بعد ذلك، سيُطلب من المستخدم بعد ذلك إصدار كلمة مرور جديدة (حسب إرشادات رمز المرور).

قفل الجهاز



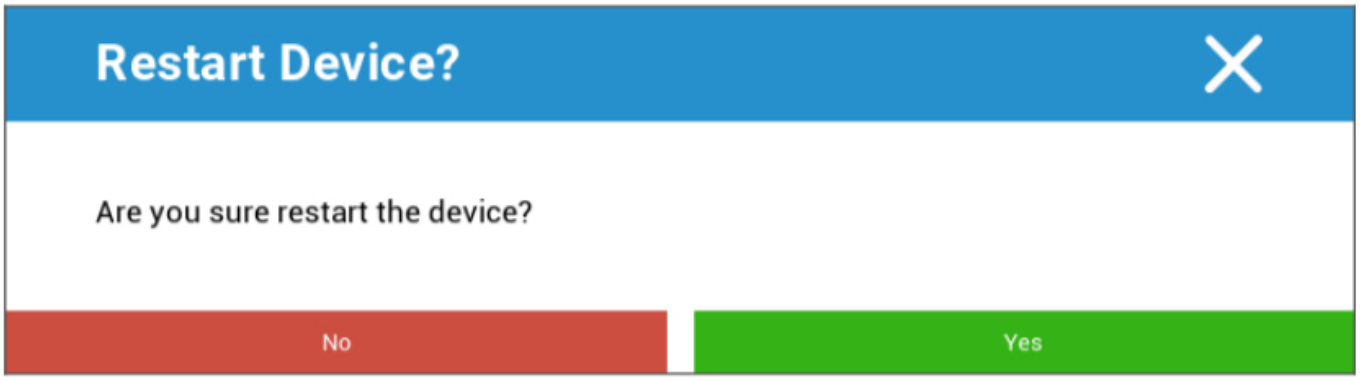
هنا يتم إرسال أمر القفل إلى جهاز المستخدم النهائي (شاشة القفل).

جهاز إيقاف التشغيل



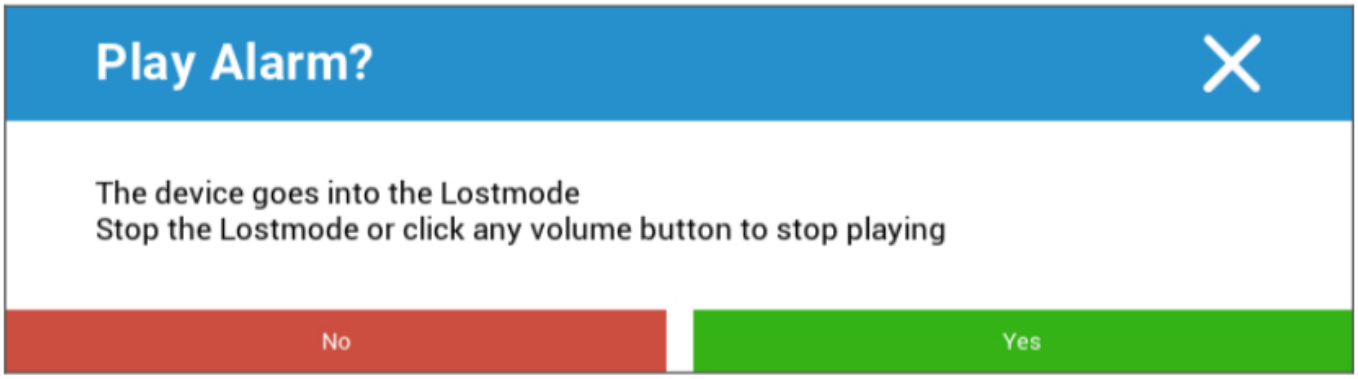
هنا يتم إرسال أمر إيقاف التشغيل إلى جهاز المستخدم النهائي.

إعادة تشغيل الجهاز

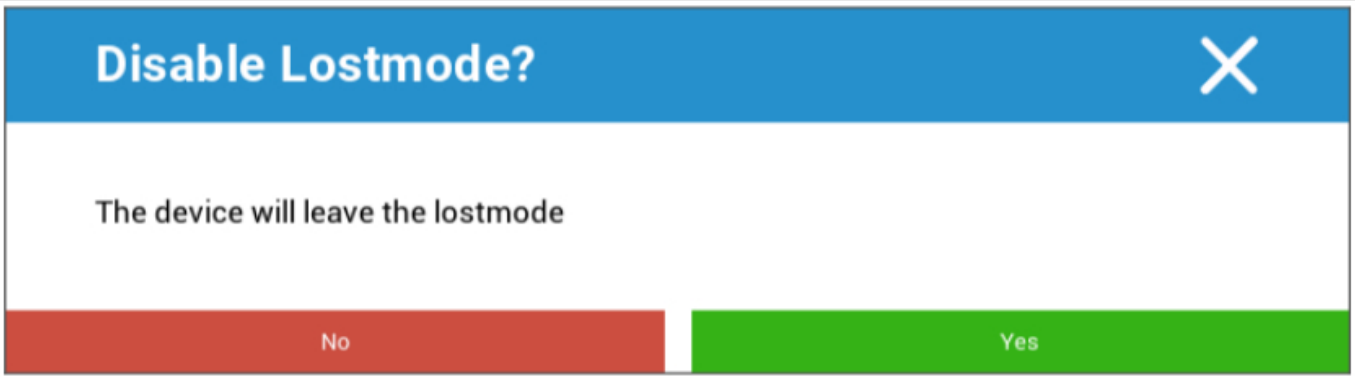


هنا يتم إرسال أمر إعادة التشغيل إلى جهاز المستخدم النهائي.

الإنذار ووضع الفقدان | تعطيل وضع الفقدان | تعطيل وضع الفقدان



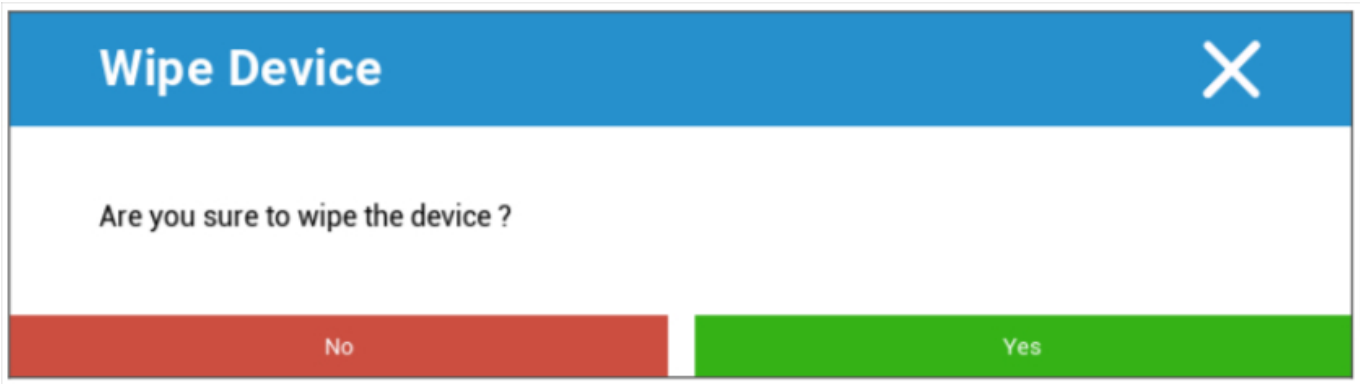
هنا يمكن ضبط الجهاز على وضع Lostmode، الذي يضبط الجهاز على تشغيل صوت إنذار باستمرار. يمكن إيقاف وضع Lostmode بالضغط على أي زر صوت في الجهاز أو عن بُعد بالنقر على "تعطيل وضع Lostmode":



حذف الجهاز

هنا يمكن تنفيذ أمر الحذف. يمكنك مرة أخرى أن تقرر ما إذا كان يجب إزالة الجهاز من AppTec360 فقط ("حذف من النظام") أو إذا كان يجب إزالة الجهاز من AppTec360 واستعادته أيضًا إلى إعدادات المصنع ("مسح وحذف").

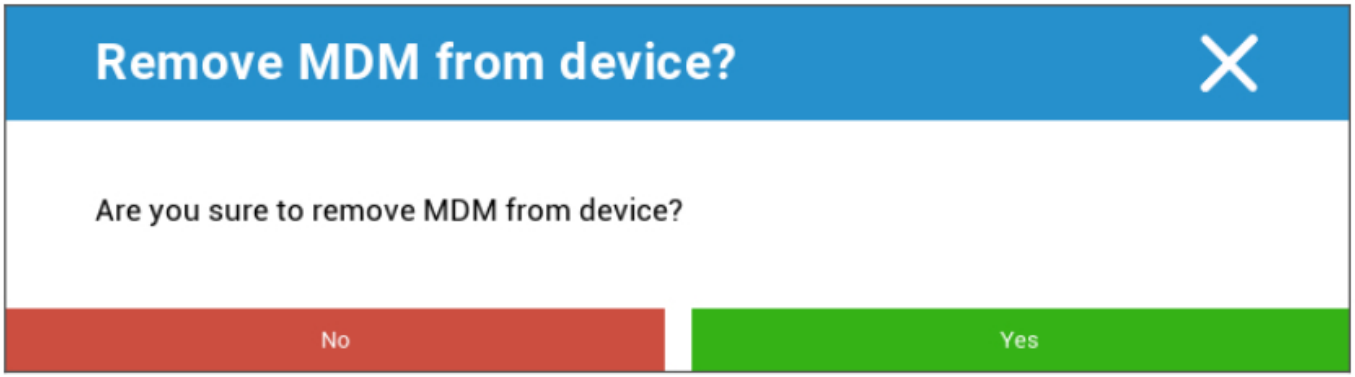
جهاز المسح



ضمن "مسح الجهاز" يمكنك إجراء مسح كامل للجهاز. ستتم استعادة الجهاز إلى إعدادات المصنع.

المسح المؤسسي | إزالة MDM

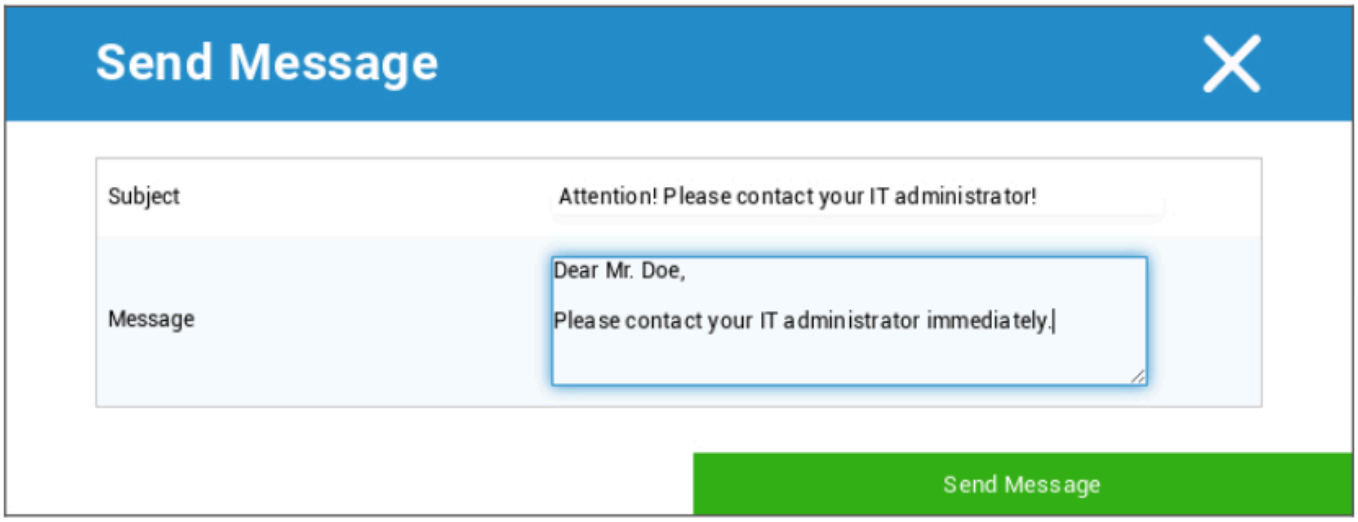
يتم حذف المعلومات والتطبيقات والملفات الشخصية التي توفرها AppTec360 فقط. وبهذه الطريقة، لن تكون بيانات الشركة متاحة على جهاز المستخدم النهائي. لا تتأثر المنطقة الخاصة وتستمر في البقاء على جهاز المستخدم النهائي.



باستخدام "إزالة MDM"، يمكنك إزالة ملف تعريف MDM من جهاز المستخدم النهائي وجميع العناصر الأخرى التي توفرها AppTec.

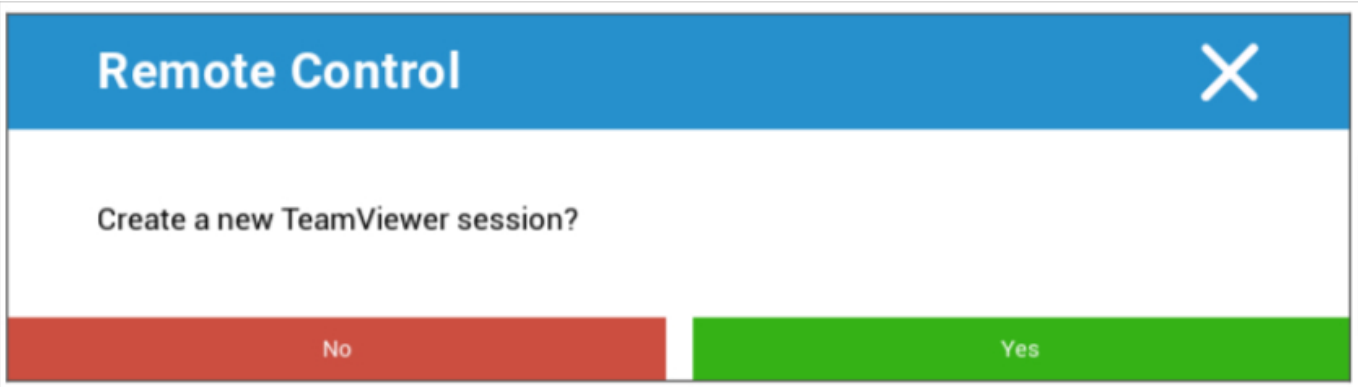
ينفذ هذا الأمر نفس إجراء "مسح المؤسسة".

إرسال رسالة



هنا يمكنك إرسال إشعار دفع إلى الجهاز المعني.

برنامج TeamViewer للتحكم عن بُعد



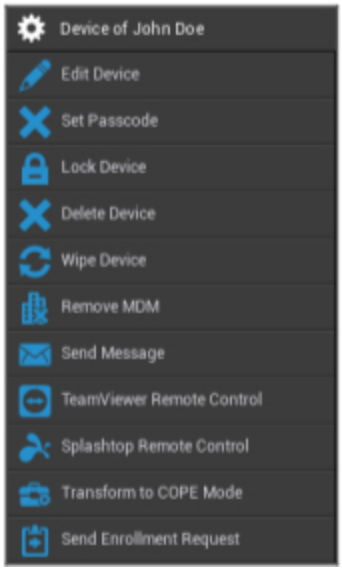
هنا يمكن بدء جلسة تحكم عن بُعد لبرنامج Teamviewer.

إرسال طلب التسجيل

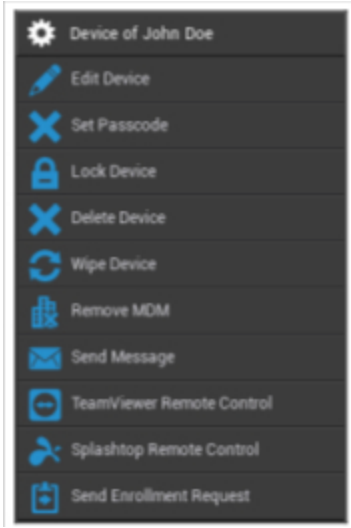
باستخدام "إرسال طلب تسجيل"، يمكنك إرسال طلب تسجيل (مرة أخرى)، إلى المستخدم المعني.

أندرويد

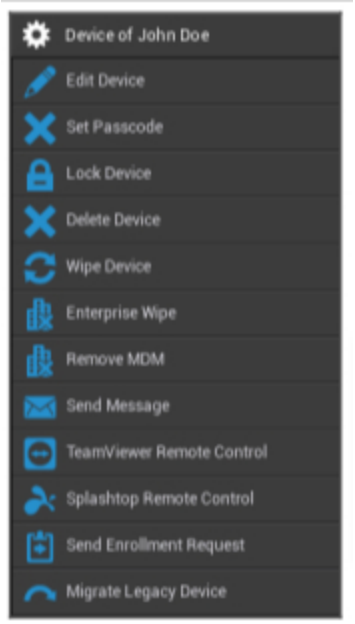
جهاز مُدار بالكامل من AE (مُدار بالكامل)



ملف تعريف عمل AE (الحاوية)



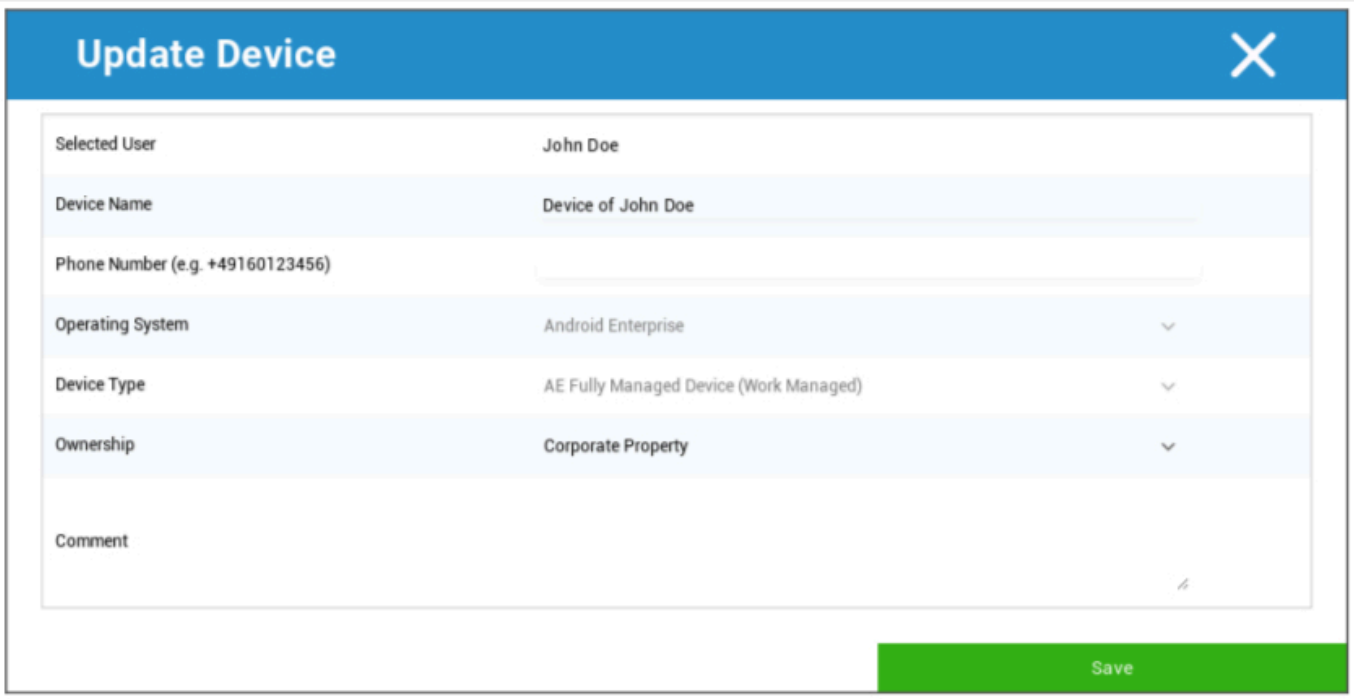
هاتف أندرويد | جهاز لوحي



تحرير الجهاز	تحرير معلومات الجهاز
تعيين رمز المرور	تعيين رمز مرور الجهاز
قفل الجهاز	قفل الجهاز (قفل الشاشة)
حذف الجهاز	حذف الجهاز من AppTec
جهاز المسح	استعادة الجهاز إلى إعدادات المصنع
مسح المؤسسات	يتم حذف المعلومات والتطبيقات والملفات الشخصية التي توفرها AppTec360 (سيتم فصل الجهاز عن نظام إدارة الأجهزة المتعددة الوسائط)
إزالة MDM	
إرسال رسالة	إرسال الإشعارات الفورية إلى الجهاز سيتم عرض الرسالة في تطبيق AppTec360 (علامة تبويب الرسائل)
برنامج TeamViewer للتحكم عن بُعد	بدء جلسة تحكم عن بُعد لهذا الجهاز باستخدام برنامج TeamViewer
جهاز تحكم عن بعد سبلاش توب	بدء جلسة تحكم عن بعد لهذا الجهاز باستخدام Splashtop
التحويل إلى وضع COPE (فقط على جهاز AE المُدار بالكامل (مُدار بشكل كامل)	إنشاء ملف تعريف عمل على جهاز AE المُدار بالكامل (المُدار بشكل كامل)
إرسال طلب التسجيل	إرسال طلب تسجيل (متكرر)
ترحيل الجهاز القديم (فقط على الهاتف/الجهاز اللوحي الذي يعمل بنظام أندرويد عند التسجيل باستخدام توفير وضع مالك الجهاز)	ترحيل ملف تعريف هاتف أندرويد/جهاز لوحي إلى ملف تعريف جهاز مُدار بالكامل (مُدار من قبل العمل)

تحرير الجهاز

هنا يمكنك تحديث مجموعة متنوعة من معلومات الجهاز.



المستخدم المختار	مستخدم الجهاز
اسم الجهاز	اسم الجهاز
رقم الهاتف	رقم هاتف الجهاز
نظام التشغيل	أندرويد إنتربرايز أندرويد
نوع الجهاز	أندرويد إنتربرايز: • جهاز مُدار بالكامل من AE (مُدار بالكامل) • وضع ملف تعريف عمل AE (الحاوية فقط) • جهاز مُدار بالكامل من AE مع ملف تعريف العمل (COPE) أندرويد: • الهاتف • جهاز لوحي
الملكية	الشركات = ممتلكات الشركات

	موظف = خاصية الموظف
تعليق	أوصاف إضافية للجهاز

مسح رمز المرور

هنا يمكنك إزالة رمز مرور الجهاز على الجهاز المحدد. افتراضيًا على نظام Android، سيتم تعيين رمز المرور على "123456"، ويمكن للمستخدم تغييره بعد ذلك ويجب عليه ذلك.

قفل الجهاز

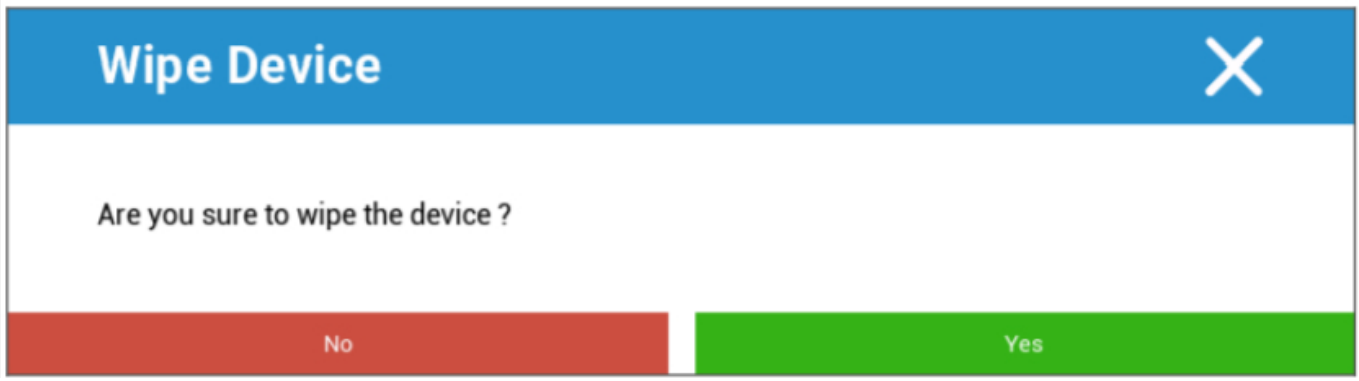
هنا سيتم إرسال أمر قفل الجهاز إلى الجهاز (قفل الشاشة).

حذف الجهاز

هنا يمكن تنفيذ أمر الحذف. يمكنك أن تقرر مرة أخرى، ما إذا كان يجب إزالة الجهاز من AppTec360 فقط ("حذف من النظام") أو إذا كان يجب إزالة الجهاز من AppTec360 واستعادته إلى إعدادات المصنع بالإضافة إلى ذلك ("مسح وحذف").

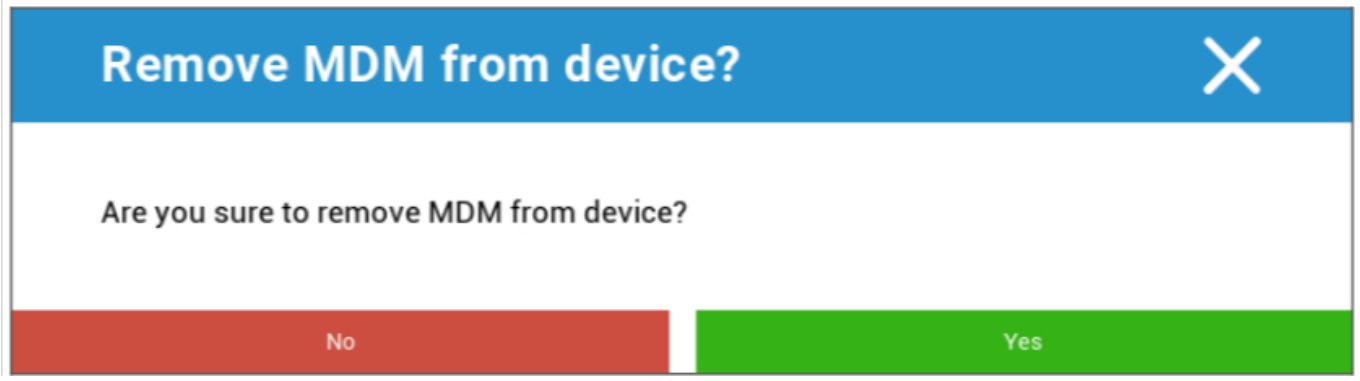
جهاز المسح

ضمن "مسح الجهاز" يمكنك إجراء مسح كامل للجهاز. سيتم بعد ذلك استعادة الجهاز إلى إعدادات المصنع.



بالإضافة إلى ذلك، إذا كان الجهاز يحتوي على بطاقة SD، يمكنك مسح بطاقة SD. يمكنك تحقيق ذلك، من خلال ضبط "مسح بطاقة SD أيضًا؟ " على "تشغيل".

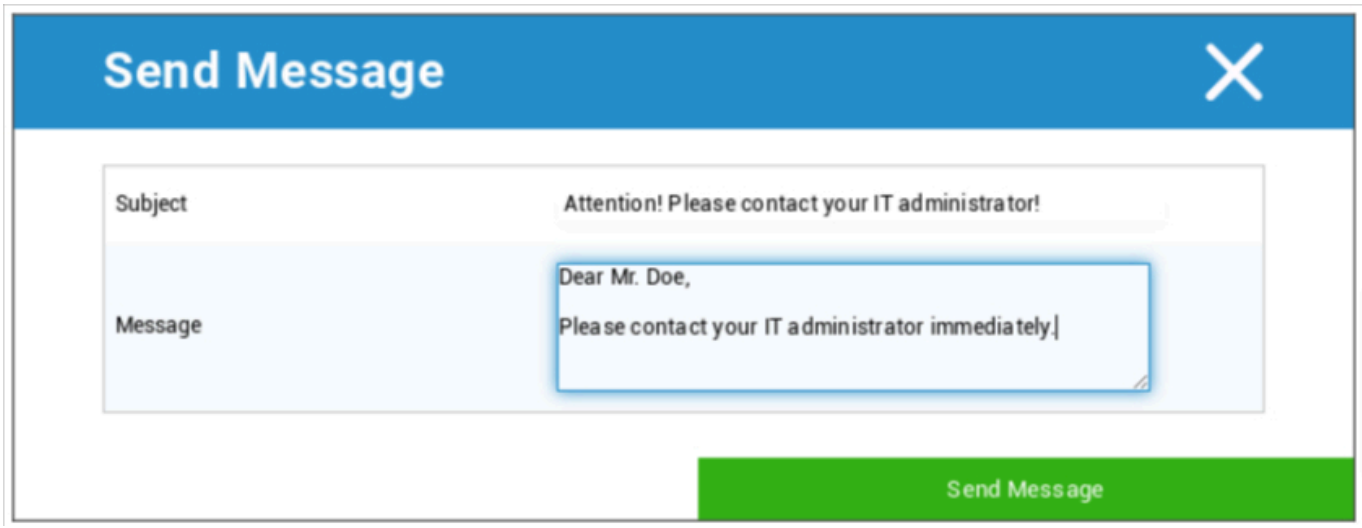
إزالة MDM



هذه هي الطريقة الموصى بها، لإنشاء فصل من MDM.

يتم حذف المعلومات والتطبيقات والملفات الشخصية التي توفرها AppTec360 فقط، مما يعني أن جميع بيانات الشركة لن تكون متاحة على جهاز المستخدم النهائي. ومع ذلك، لا يتأثر المجال الخاص ويستمر في البقاء على جهاز المستخدم النهائي.

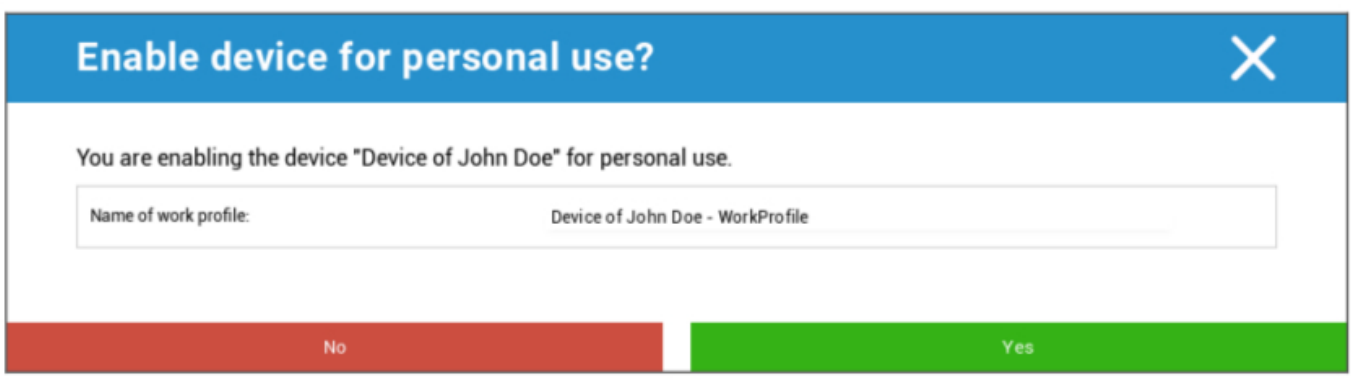
إرسال رسالة



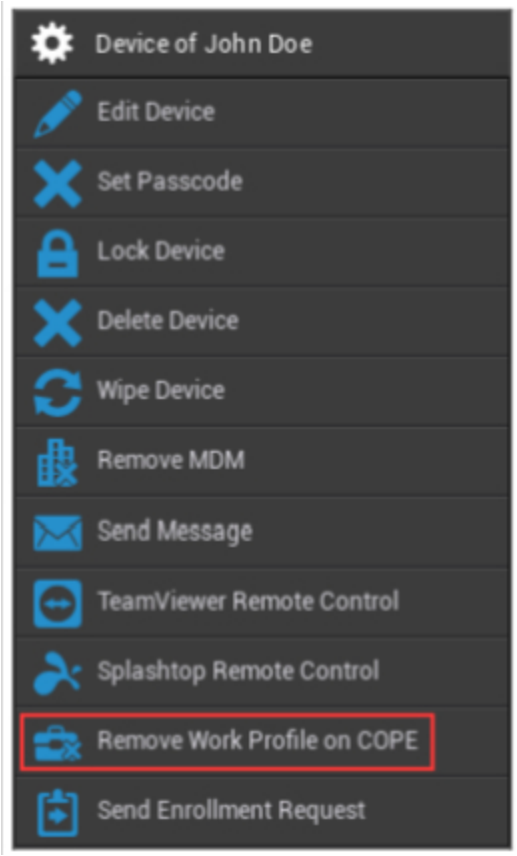
يمكنك هنا إرسال إشعار فوري إلى جهاز المستخدم النهائي المعني.

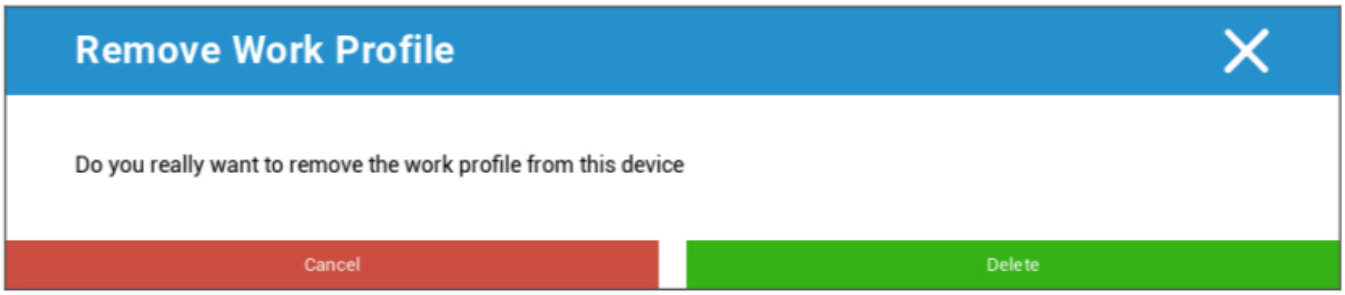
التحويل إلى وضع COPE

إنشاء ملف تعريف عمل على جهاز AE المُدار بالكامل (المُدار بشكل كامل)



بعد تحويل الجهاز إلى وضع COPE، يمكنك إزالة ملف تعريف العمل من خلال النقر على خيار الترس **إزالة ملف تعريف العمل في COPE:**




Remove Work Profile
Do you really want to remove the work profile from this device
Cancel
Delete

إرسال طلب التسجيل

باستخدام "إرسال طلب تسجيل" يمكنك إرسال طلب تسجيل (مرة أخرى)، إلى المستخدم المعني.

يُرجى ملاحظة أن أحدث طلب تسجيل - طلب صالح فقط.

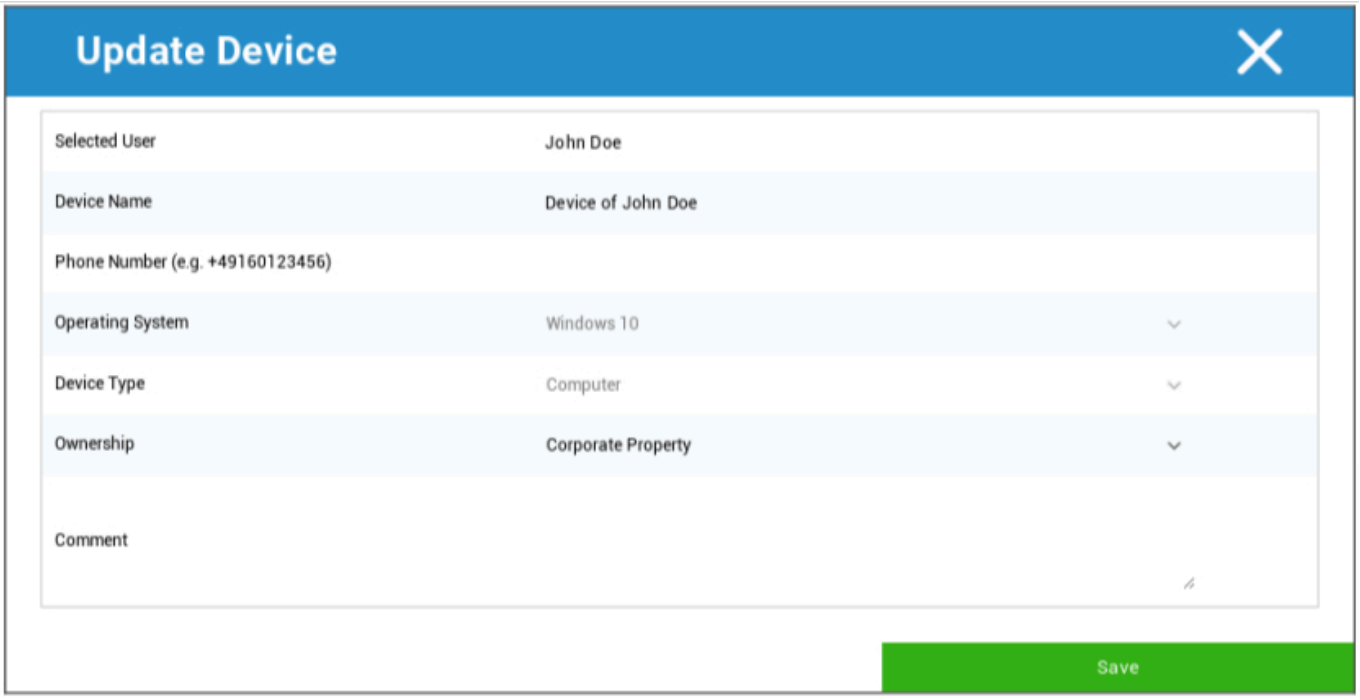
ترحيل الجهاز القديم

ترحيل ملف تعريف هاتف أندرويد/جهاز لوحي إلى ملف تعريف جهاز مُدار بالكامل (مُدار من قبل العمل)

النوافذ

اسم الجهاز	اسم الجهاز المحدد
تحرير الجهاز	تحرير الجهاز
حذف الجهاز	إزالة الجهاز من AppTec
مسح المؤسسات	يتم حذف المعلومات والتطبيقات والملفات الشخصية التي تقدمها AppTec360
إزالة MDM	
برنامج TeamViewer للتحكم عن بُعد	التحكم في الجهاز عن بُعد باستخدام برنامج TeamViewer
إرسال طلب التسجيل	إرسال طلب التسجيل (مرة أخرى)

تحرير الجهاز

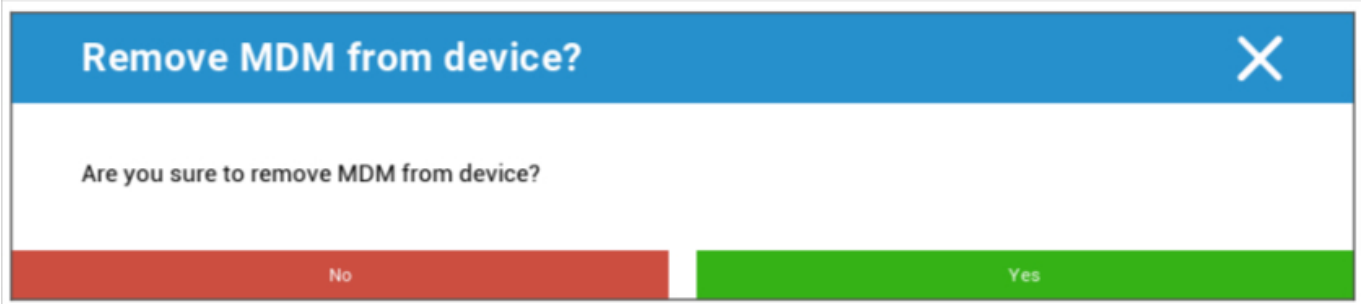


هنا يمكنك تحديث مجموعة متنوعة من المعلومات على الجهاز.

حذف الجهاز

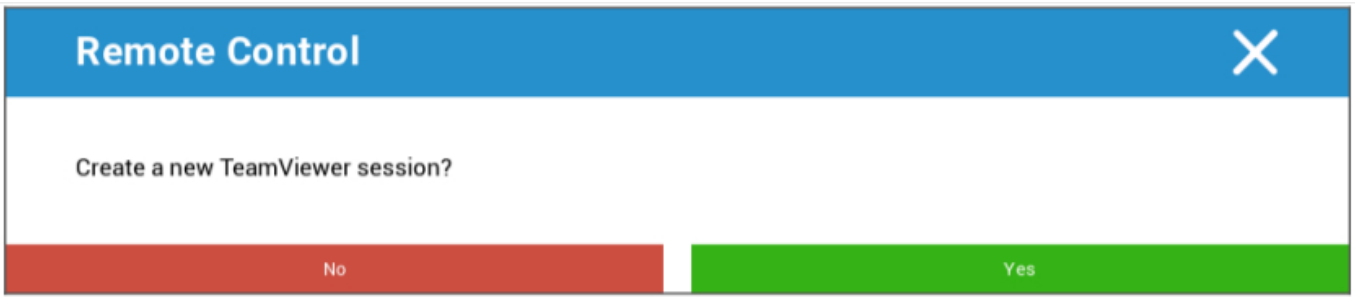
هنا يمكن تنفيذ أمر الحذف الذي يزيل الجهاز من AppTec360 فقط.

المسح المؤسسي | إزالة MDM



يتم حذف المعلومات والتطبيقات والملفات الشخصية التي توفرها AppTec360 فقط. وبهذه الطريقة، لن تكون بيانات الشركة متاحة على جهاز المستخدم النهائي. لا تتأثر المنطقة الخاصة وتستمر في البقاء على جهاز المستخدم النهائي.

برنامج TeamViewer للتحكم عن بُعد



هنا يمكنك بدء جلسة TeamViewer للتحكم عن بُعد لهذا الجهاز.

إرسال طلب التسجيل

باستخدام "إرسال طلب تسجيل"، يمكنك إرسال طلب تسجيل (مرة أخرى)، إلى المستخدم المعني.

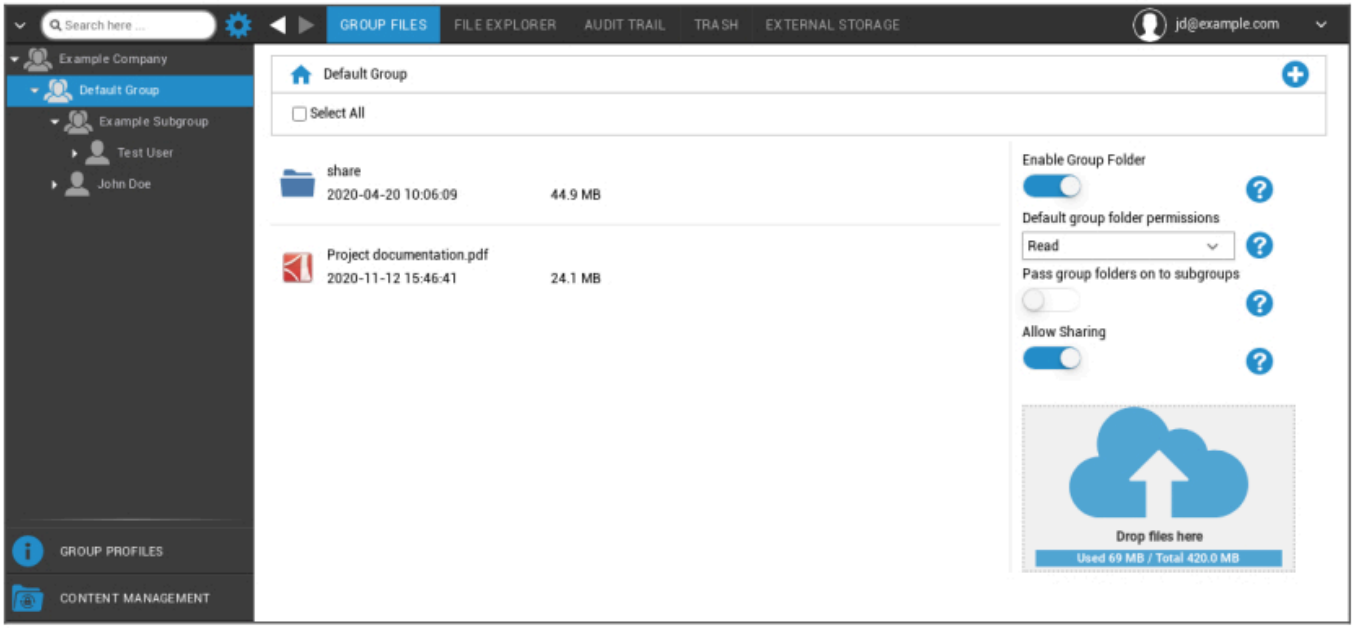
إدارة المحتوى

عندما تكون في مجموعة، يمكنك إدارة ContentBox الخاص بـ AppTec باستخدام "إدارة المحتوى".

باستخدام Content Box، يمكنك توزيع المستندات وبيانات الشركة الأخرى بأمان على أجهزة المستخدم النهائي.

ملفات المجموعة

تمثل "تجميع الملفات" جزءًا أساسيًا ContentBox. هنا يمكنك إنشاء الإعدادات وتحميل المستندات وإنشاء مجلدات جديدة وما إلى ذلك.



باستخدام الرمز الموجود في الزاوية العلوية اليمنى، يمكنك إنشاء مجلدات جديدة مخصصة للمجموعة المعنية باستخدام "إضافة مجلد".

باستخدام الرمز الموجود في الزاوية العلوية اليمنى، يمكنك إنشاء مجلد جديد عبر "إضافة مجلد"، والذي يجب تعيينه إلى المجموعة المعنية.

يمكنك تسمية المجلد بأي اسم تريده.

عبر "تحميل الملفات"، يمكنك تحميل البيانات. هنا سيتم فتح المستكشف القياسي الخاص بك. يمكنك بالطبع تنفيذ هذين الإجراءين في كل مجلد (فرعي).

باستخدام الرمز الموجود في الزاوية العلوية اليسرى، يمكنك العودة إلى القائمة الرئيسية.

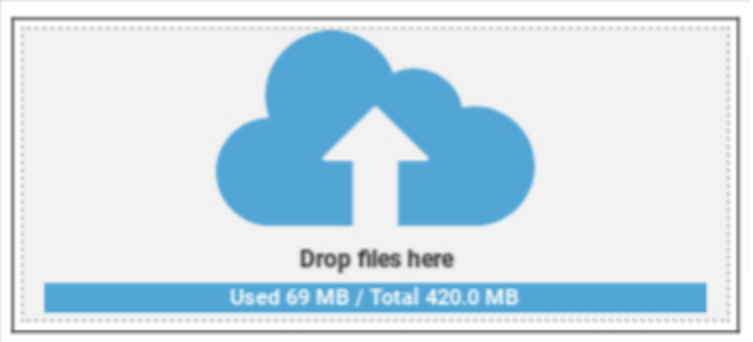
يمكنك تحديد العديد من المجلدات والملفات وتنزيلها باستخدام "تنزيل" أو يمكنك حذفها بالنقر على "حذف".

يمكنك أيضًا تحديد جميع الملفات والمجلدات وتنفيذ الأمرين "تنزيل" و "حذف".

عند تحريك الماوس فوق مجلد أو ملف، سترى النظرة العامة التالية:

- باستخدام "إعادة التسمية"، يمكنك إعادة تسمية المجلد/الملف
- باستخدام "تنزيل"، يمكنك تنزيل المجلد/الملف
- باستخدام "حذف"، يمكنك حذف المجلد/الملف

تمكين مجلد المجموعة	إذا تم تفعيله، فإن جميع أعضاء المجموعة لديهم حق الوصول إلى المجلد المعني
أذونات مجلد المجموعة الافتراضية	أذونات المستخدمين في المجموعة المحددة: قراءة = إذن قراءة فقط تحديث = إذن التحديث إنشاء = إنشاء إذن إنشاء حذف = حذف إذن الحذف
تمرير مجلدات المجموعة إلى المجموعات الفرعية	في حالة تفعيلها، يمكن للمجموعات الفرعية المعنية الوصول إلى ملفات البيانات الأصلية
أذونات المجموعات الفرعية	أذونات المستخدمين في المجموعة الفرعية المحددة: قراءة = إذن قراءة فقط تحديث = إذن التحديث إنشاء = إنشاء إذن إنشاء حذف = حذف إذن الحذف
السماح بالمشاركة	في حالة تفعيلها، يمكن للمستخدم مشاركة الملفات عبر رابط



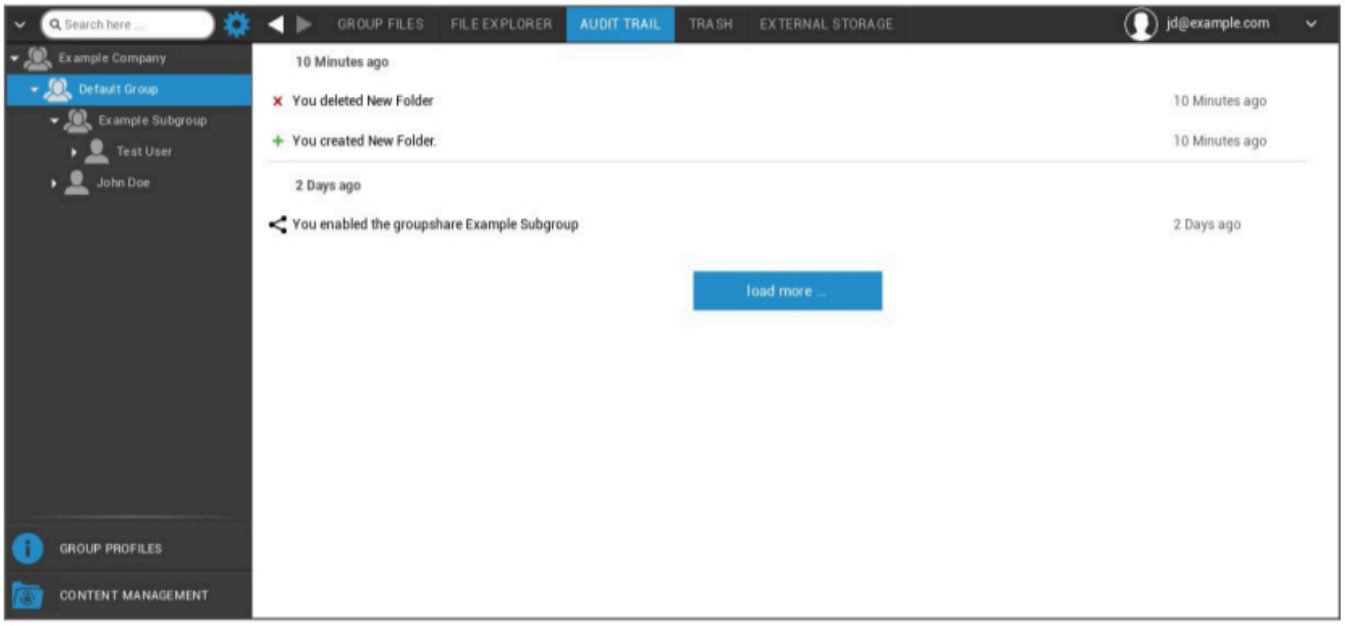
من أجل تحميل الملفات، يمكنك استخدام هذا الحقل، من خلال سحب ملف عن طريق السحب والإفلات إلى هذه النافذة. يمكنك أيضًا النقر على هذا الحقل، من أجل تحديد ملف وتحميله بمساعدة Internet Explorer.

مستكشف الملفات

من خلال "مستكشف الملفات"، يمكنك إدارة جميع المجلدات والملفات - بغض النظر عن المجموعة التي تم إيداعها فيها.

ستجد أيضًا الإعدادات والأزرار التي تعرفت عليها في "ملفات المجموعة".

مسار التدقيق



في "سجل التدقيق"، يمكنك أن ترى من السجل، أي مستخدم أنشأ أو حذف أو شارك ماذا. بهذه الطريقة، يمكنك في أي وقت تحديد ما تم القيام به مع بيانات الشركة.

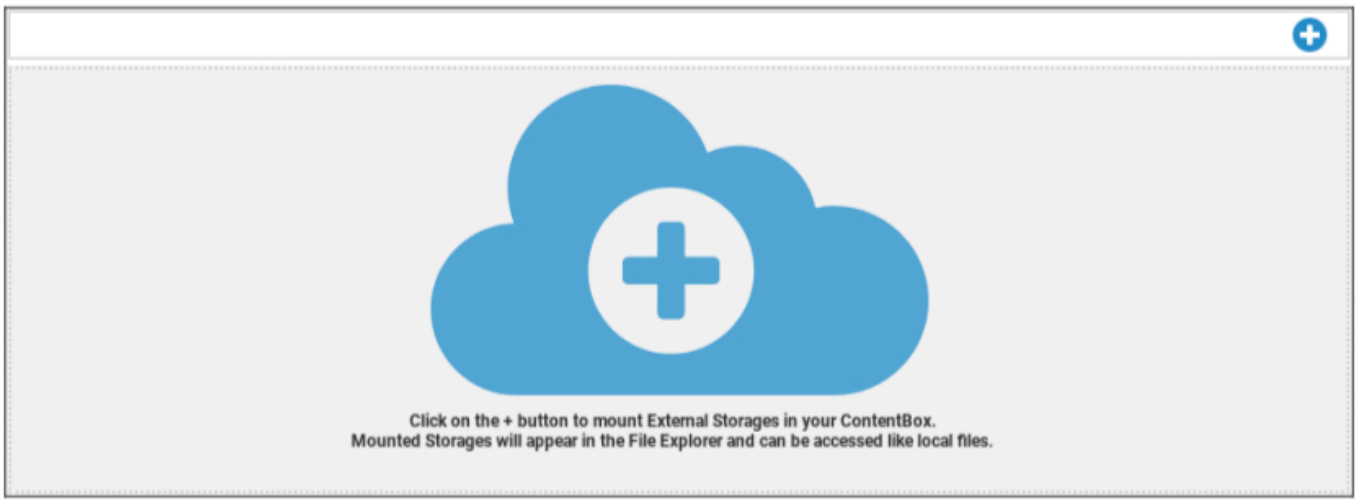
القمامة

في حالة حذفك لشيء ما (عن طريق الخطأ)، يمكنك رؤية المجلدات والملفات الموجودة ضمن "المهملات" واستعادتها، وفقًا لرغباتك.

- باستخدام "إلغاء الحذف"، يمكنك استعادة البيانات/المجلد.
- باستخدام "حذف"، يمكنك حذف البيانات/المجلد نهائيًا - يجب تأكيد أمر الحذف مرة أخرى.

يُرجى ملاحظة أن سعة التخزين التي يتم استخدامها في سلة المهملات تقلل من "المساحة الإجمالية" المتاحة - وهذا من متطلبات السحابة الخاصة.

التخزين الخارجي



تحت عنوان "التخزين الخارجي"، يمكنك توصيل وحدة تخزين خارجية.

باستخدام الرمز، يمكن إضافة مساحة تخزين (إضافية).

النوع	Amazon S3, FTP, SFTP, SFTP, ownCloud, WebDAV, Windows Share, SharePoint

أمازون S3	
اسم العرض	اسم العرض
مفتاح الوصول	مفتاح الوصول
المفتاح السري	مفتاح الأمان
دلو	الهوية المحددة للمجلد الفرعي الذي تم تعيينه لك
اسم المضيف (اختياري)	اسم المضيف (اختياري)
المنفذ (اختياري)	المنفذ (اختياري)
المنطقة	المنطقة (اختياري)
تمكين SSL	تمكين SSL
تمكين نمط المسار التمكين	مسح عنوان المسار الذي تم تعيينه لك

بروتوكول نقل الملفات	
اسم العرض	اسم العرض
المضيف	عنوان المضيف-العنوان
اسم المستخدم	اسم المستخدم
كلمة المرور	كلمة المرور
الجذر	القائمة الرئيسية
تأمين ftps://:	

SFTP	
اسم العرض	اسم العرض
المضيف	عنوان المضيف-العنوان
اسم المستخدم	اسم المستخدم
كلمة المرور	كلمة المرور
الجذر	القائمة الرئيسية

السحابة الخاصة	
اسم العرض	اسم العرض
عنوان URL	عنوان URL لـ ownCloud
اسم المستخدم	اسم المستخدم
كلمة المرور	كلمة المرور
المجلد الفرعي البعيد	مجلد قياسي
تأمين https://:	

WebDAV	
اسم العرض	اسم العرض
عنوان URL	عنوان URL WebDAV
اسم المستخدم	اسم المستخدم
كلمة المرور	كلمة المرور
الجذر	القائمة الرئيسية
تأمين https://	
مشاركة الويندوز	سيتوفر دعم Windows Share قريباً
شير بوينت	سيتوفر دعم Microsoft SharePoint قريباً

سجل التدقيق

هنا يمكنك العثور على سجل يسجل معلومات حول الإجراءات التي يتم تنفيذها في وحدة تحكم MDM.

باستخدام رمز الفلتر، يمكنك تطبيق الفلاتر على القائمة المعروضة.

باستخدام القائمة المنسدلة **العناصر لكل صفحة**: يمكنك تحديد كمية العناصر التي سيتم عرضها في صفحة واحدة من القائمة.

الإجراء المتخذ/تم تغيير الإعدادات	الإجراء الذي تم اتخاذه / الإعداد الذي تم تغييره
القيمة	قيمة الإجراء المتخذ/الإعداد المتغير
المستخدم	اسم المستخدم الذي اتخذ الإجراء / قام بتغيير الإعدادات
التاريخ	الطابع الزمني للوقت الذي تم فيه اتخاذ هذا الإجراء/تم تغيير هذا الإعداد
المسار/النوع	المسار إلى حيث تم اتخاذ هذا الإجراء/تم تغيير هذا الإعداد

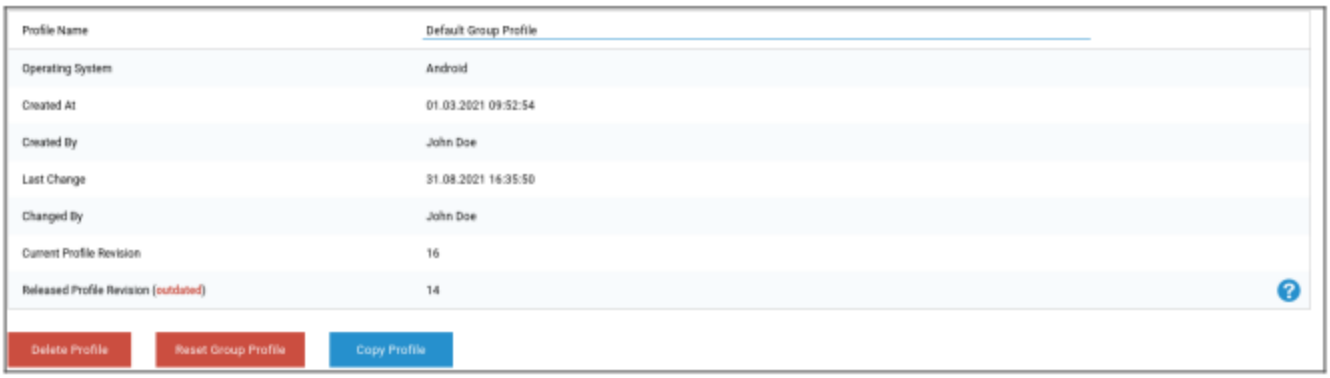
تهيئة نظام التشغيل iOS

جنرال لواء

اعتمادًا على ما إذا كنت قد حددت مجموعة أو جهازًا حاليًا، يختلف العرض ونقاطه الفرعية - يرجى الانتباه جيدًا لذلك!

نظرة عامة على ملف تعريف المجموعة (على مستوى المجموعة فقط)

عند فتح الملف الشخصي للمجموعة، ستحصل على نظرة عامة سريعة على الملف الشخصي



اسم الملف الشخصي	اسم الملف الشخصي (يمكن تغييره هنا)
نظام التشغيل	نظام التشغيل الذي تم إنشاء ملف التعريف له
تم إنشاؤها في	وقت الإنشاء
تم إنشاؤها بواسطة	منشئ الملف الشخصي
آخر تغيير	وقت آخر تغيير في الملف الشخصي
تم التغيير بواسطة	الحساب الذي أجرى التغييرات الأخيرة
مراجعة الملف الشخصي الحالي	مراجعة حالة الملف الشخصي المحفوظة
مراجعة الملف الشخصي الصادر	مراجعة الملف الشخصي المعين ("تعيين الآن"). إذا كانت التسمية تظهر "(قديم)" خلف النص، فهذا يعني أنك قمت بحفظ ملف التعريف ولكنك لم تعيّنه بعد، لذا ستظل الأجهزة تحصل على الإصدار الأقدم.

معلومات عامة

إذا كنت على الجهاز مباشرة، فستتلقى نظرة عامة موجزة عن الجهاز الذي اخترته.

اسم الجهاز	اسم الجهاز
رقم الهاتف	رقم هاتف الجهاز
الطراز	رقم الموديل
نظام التشغيل	نظام التشغيل
الرقم التسلسلي	الرقم التسلسلي للجهاز
ملكية الجهاز	جهاز الشركة أو الجهاز الخاص الشركة = جهاز الشركة موظف = جهاز خاص
نوع الجهاز	نوع الجهاز (جهاز لوحي أو هاتف)
كسر الحماية	إذا كان هناك جيلبريك على الجهاز
تحت الإشراف	يشير إلى ما إذا كان هذا الجهاز خاضع للإشراف أم لا
متوافق	إذا تم انتهاك أي إرشادات
آخر ظهور	حالة آخر مرة اتصل فيها الجهاز مع خادم AppTec360

الإعدادات

تحتوي هذه الإعدادات على اسم الجهاز وخلفية محددة مسبقاً.

تسمية الجهاز باسم النظام	سيكون الاسم الذي سيتم إصداره في وحدة تحكم AppTec360 (في هيكل التسلسل الهرمي الأيسر)، هو نفسه الموجود على جهاز المستخدم النهائي المعني (يمكن الاطلاع عليه في إعدادات الجهاز)
استخدام خلفية مخصصة (الأجهزة الخاضعة للإشراف فقط)	هنا يمكنك التحديد المسبق للخلفية التي يجب عرضها على جهاز المستخدم النهائي (على سبيل المثال لنوع من العلامات التجارية للشركة للجهاز) متاح فقط في الوضع الخاضع للإشراف!
تحديثات نظام التشغيل التلقائية	يفرض تحديثات نظام التشغيل إذا كانت متوفرة. فقط لأجهزة DEP في الوضع الخاضع للإشراف.
الخطوط المخصصة	هنا يمكنك إضافة خطوط مخصصة.
الاسم	اختياري. الاسم المرئي للمستخدم للخط. يتم استبدال هذا الحقل بالاسم الفعلي للخط بعد التثبيت.
الخط	قم بتحميل ملف الخط (.otf أو .ttf).

مراجعة التكوين

ستحصل هنا على نظرة عامة على ملف تعريف المجموعة المخصص للجهاز.

إذا قمت بالنقر على الملف الشخصي للمجموعة، فستتمكن من الوصول إلى الملف الشخصي مباشرةً ويمكنك إجراء الإعدادات.

باستخدام الرمز، يمكنك إعادة التطبيقات المعينة إلى إعدادات ملف تعريف المجموعة.

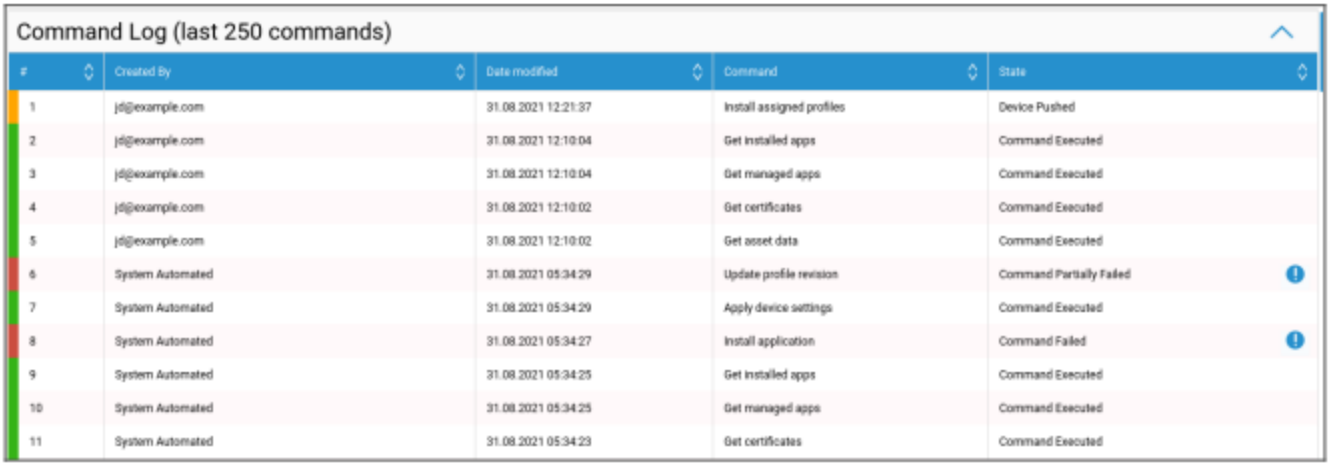
باستخدام الرمز، يمكنك إعادة ضبط ملف تعريف الجهاز بحيث لا يحتوي على أي إعدادات على الإطلاق.

تشير عبارة "تتوفر مراجعة أحدث" إلى أن ملف تعريف المجموعة قد تم تغييره وحفظه ولكن لم يتم تعيينه. يجب تعيين ملف تعريف المجموعة باستخدام "تعيين الآن" على مستوى المجموعة لتطبيق التغييرات على الأجهزة.

سجل الجهاز (على مستوى الجهاز فقط)

سجل الأوامر

هنا يمكنك معرفة الأوامر التي تم إصدارها للجهاز وما هي حالتها.



يتم إنشاء الأوامر التي تم إنشاؤها بواسطة "النظام الآلي" تلقائياً بواسطة النظام.

حالات الأوامر المحتملة

تم دفع الجهاز	تم إرسال طلب دفع إلى خدمة الدفع (مثل APNS) لإخبار الجهاز بالاتصال مرة أخرى بخادم EMM.
تم إنشاء الأمر	تم إنشاء الأمر في النظام.
تم إرسال الأمر	تم إرسال الأمر إلى الجهاز بعد اتصاله بالخادم.
تم تنفيذ الأمر	تم تنفيذ الأمر بنجاح.
فشل الأمر	فشل الأمر. *
فشل الأمر جزئياً	اعتمادًا على نظام تشغيل الجهاز قد يتم تجميع بعض الأوامر معًا. في هذا فشلت بعض أجزاء مجموعة الأوامر هذه. *
تم تنفيذ الأمر، وفشل الأمر في النهاية	تم تنفيذ الأمر ولكن ربما لم يتم تنفيذه.
إعادة دفع الأمر	تم إعادة دفع الأمر من قبل مستخدم.
مهملة	تم تجاهل الأمر. على سبيل المثال لأنه تم استبداله بأمر آخر أو تم إعادة تسجيل الجهاز وإزالة الأوامر القديمة

إذا كانت هناك علامة تعجب خلف الرسالة، فيمكنك الحصول على مزيد من المعلومات من خلال التمرير فوق الرمز بمؤشرك.

إدارة الأصول (على مستوى الجهاز فقط)

إدارة الأصول (على مستوى الجهاز فقط)

معلومات الجهاز

الطراز	رقم طراز الجهاز
نظام التشغيل	نظام التشغيل
إصدار نظام التشغيل	إصدار نظام التشغيل
الرقم التسلسلي	الرقم التسلسلي
UDID	معرّف الجهاز UDID
اسم الجهاز	اسم الجهاز
تحت الإشراف	يعرض إذا كان الجهاز خاضعاً للإشراف
حالة البطارية	حالة البطارية

الواي فاي

عنوان IP	عنوان IP للجهاز
واي فاي ماك	عنوان الواي فاي MAC

خلوي

الحالة	الحالة (بطاقة SIM موجودة)
رقم الهاتف	رقم الهاتف
حالة التجوال	حالة التجوال الحالية
التجوال (الصوت/ البيانات)	حالة التجوال للصوت/البيانات
عنوان IP	عنوان IP
IMEI	رقم IMEI-Number
المشغل/الناقل	مزود الخدمة الخلوية
شبكة ناقل الشريحة SIM	شبكة شركة SIM الناقلة لبطاقة SIM
إصدار الناقل	إصدار الناقل
البرنامج الثابت للمودم	البرامج الثابتة للمودم
MCC/ MNC الحالية	انظر "SIM MCC/MNC"
SIM MCC/MNC	رمز البلد المتنقل هو تعريف قطري محدد من قبل الاتحاد الدولي للاتصالات وفقًا للمعيار E.212، والذي يُستخدم، بالاقتران مع رمز شبكة الهاتف المحمول (MNC)، لتحديد الشبكة الخلوية (= رمز البلد) عندما تنتقل إلى شبكة خلوية أخرى، فإن "MCC/ MNC الحالي" و "MCC/ MNC الحالي" و "MCC/ MNC لبطاقة SIM" مختلفان بالتالي.

بلوتوث

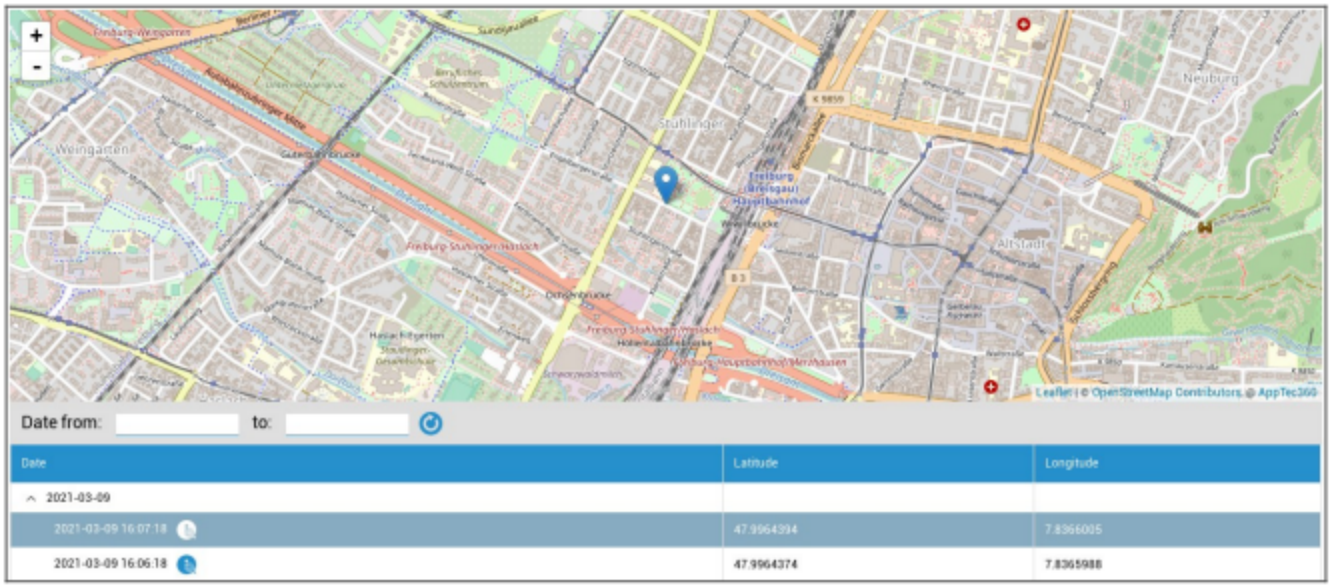
بلوتوث ماك	عنوان MAC الخاص بالبلوتوث

إدارة الأمن

مكافحة السرقة (على مستوى الجهاز فقط)

معلومات GPS (على مستوى الجهاز فقط)

هنا يمكنك تقييم الموقع الحالي/الأخير للجهاز. يمكن حماية تحديد الموقع إما بكلمة مرور واحدة أو حتى بكلمتي مرور - انظر: الإعدادات العامة - الخصوصية - الوصول إلى GPS



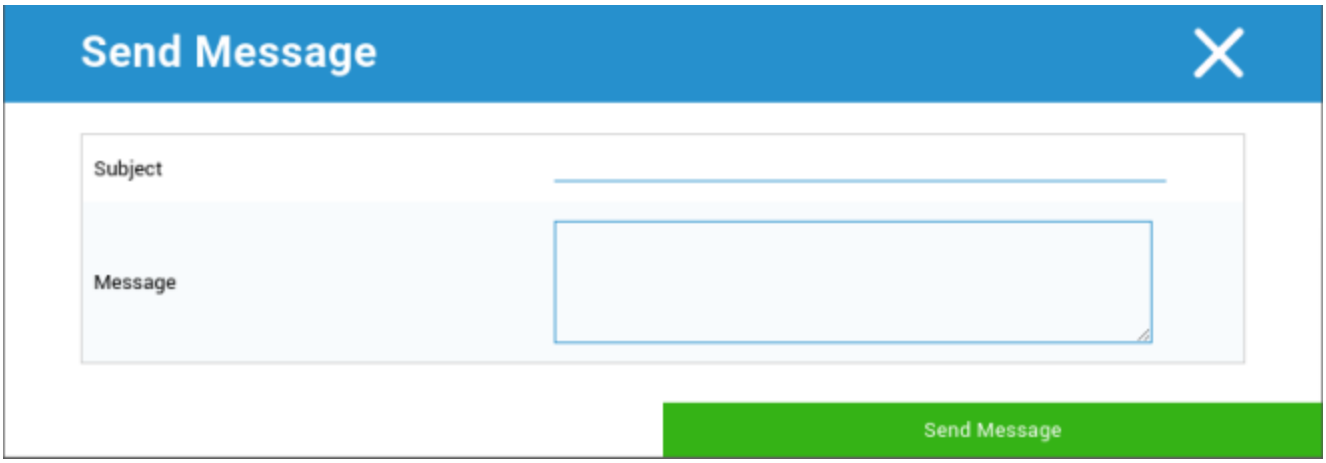
المسح والقفل (على مستوى الجهاز فقط)

ضمن "المسح والقفل"، يمكنك تنفيذ الإجراءات الثلاثة التالية:

مسح كامل	تتم استعادة الجهاز مرة أخرى إلى إعدادات المصنع (يتم حذف بيانات الشركة وكذلك البيانات الشخصية)
مسح المؤسسات	تتم إزالة بيانات الشركة فقط من جهاز المستخدم النهائي (جميع التطبيقات والبيانات وما إلى ذلك التي تم توفيرها بواسطة AppTec)
قفل الشاشة	يتم تنشيط قفل الشاشة، ويكفي إلغاء قفل الجهاز باستخدام كلمة مرور الجهاز/رقم التعريف الشخصي
تأمين الطب الشرعي (الأجهزة الخاضعة للإشراف فقط)	في حالة تفعيل هذه الوظيفة بالرمز  ، سيتم قفل الجهاز، من خلال عرض رسالة لا يمكن إغلاقها. كما لا يمكن للموظف إلغاء قفل الجهاز. يمكن للمسؤول فقط إلغاء قفل الجهاز في وحدة التحكم باستخدام رمز إلغاء القفل  .
السماح بتأمين التنشيط (الأجهزة الخاضعة للإشراف فقط)	في حالة تفعيل هذه الوظيفة، سيتم قفل الجهاز، بمجرد تفعيل "Find my iPhone" في إعدادات iCloud

الرسالة (على مستوى الجهاز فقط)

من خلال النافذة التالية، يمكنك ملء الموضوع والرسالة وإرسالها إلى جهاز المستخدم النهائي:



تهيئة الأمان

رمز المرور

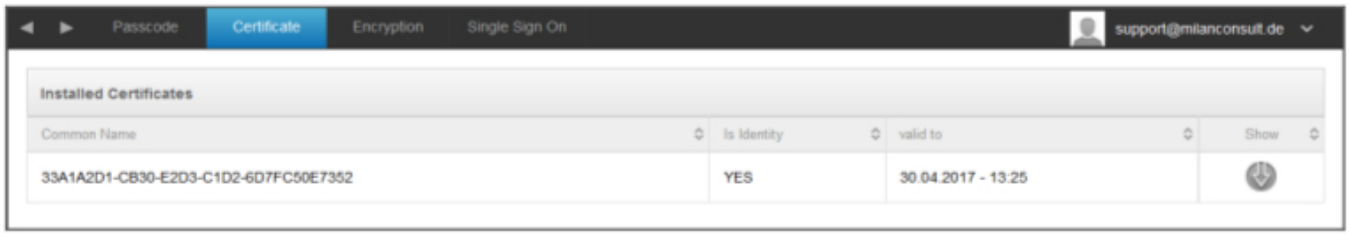
هنا تقوم بإنشاء إعدادات كلمة مرور الجهاز

يسمح بتعطيل الرمز المسموح به	عندما يتم تنشيط هذا الإعداد، لا توجد مطالبة بإدخال كلمة مرور بمجرد إنشاء كلمة المرور، لا يمكن إلغاء تنشيطها
السماح بقيمة بسيطة	السماح للمستخدم باستخدام نفس سلاسل الأرقام المتشابهة والمتصاعدة والمختزلة (على سبيل المثال 1234، 1111)
تتطلب قيمة أبجدية رقمية	يجب أن تحتوي كلمات المرور على حرف واحد على الأقل
الحد الأدنى لطول رمز المرور	الحد الأدنى لطول كلمة المرور
الحد الأدنى لعدد الأحرف المعقدة	الحد الأدنى لعدد الرموز الأبجدية الرقمية في كلمة المرور
الحد الأقصى لعمر رمز المرور	عدد الأيام التي يجب تغيير كلمة المرور بعدها
القفل التلقائي الأقصى	الحد الأقصى للوقت الذي يتم بعده قفل الجهاز
فترة السماح القصوى لقفل الجهاز	الوقت، وبعد ذلك يدخل الجهاز في وضع الاستعداد المغلق
الحد الأقصى لعدد المحاولات الفاشلة	يحدد، كم مرة يمكن إدخال كلمة مرور بشكل غير صحيح، قبل أن يتم إجراء مسح كامل للجهاز
الحد الأقصى لعمر رمز المرور (1-730 يوماً)	الحد الأقصى لعمر كلمة المرور
سجل رمز المرور (1-50 رمز مرور)	يُسمح باستخدام كلمة مرور قديمة بعد هذا الرقم

يؤدي النقر على سلة المهملات إلى فتح مربع حوار إعادة تعيين كلمة المرور، والذي يمكن من خلاله مسح كلمة مرور الجهاز المنسية.

الشهادة (على مستوى الجهاز فقط)

عرض الشهادات المتوفرة على الجهاز


Passcode
Certificate
Encryption
Single Sign On
support@mlianconsult.de
Installed Certificates
Common Name
Is Identity
valid to
Show
33A1A2D1-CB30-E2D3-C1D2-6D7FC50E7352
YES
30.04.2017 - 13:25

التشفير

طلب تشفير التخزين	تنشيط وظيفة تشفير الجهاز المثبتة

تسجيل دخول واحد

تحت نقطة "تسجيل الدخول الأحادي"، يمكنك تكوين مصادقة Kerberos.

هنا، تقوم بتأسيس بيانات اعتماد الوصول وعناوين URL/التطبيقات المعنية المسموح لها باستخدام رموز Kerberos المميزة.

متوفر في الوضع الخاضع للإشراف	
اسم الحساب	اسم الحساب
الاسم الرئيسي	الهوية الفريدة التي يمكن توزيع تذاكر Kerberos عليها
عالم	عالم Kerberos الخاص بك، الذي سيتم استخدامه (على سبيل المثال: نطاقك)

باستخدام الرمز، يمكنك إنشاء عناوين URL إضافية.

نمط عنوان URL المستخدم لتقييد هذا الحساب	عناوين URL التي سيتم تحديدها لاحقاً، والتي يمكن توزيع تذاكر Kerberos عليها

باستخدام الرمز، يمكنك إنشاء تطبيقات إضافية.

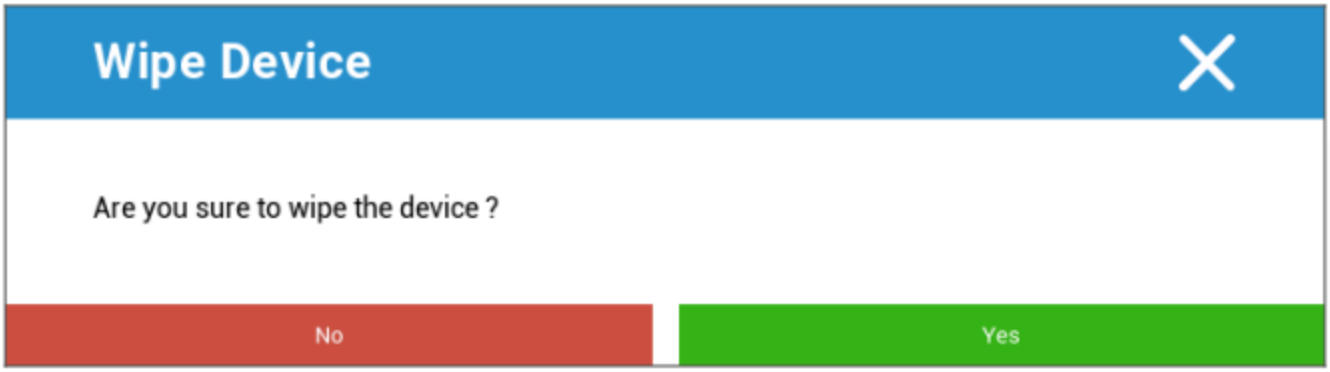
تطبيقات لتقييد هذا الحساب	التطبيقات التي سيتم تحديدها، والتي يمكن توزيع تذاكر Kerberos عليها

نهاية العمر الافتراضي (على مستوى الجهاز فقط)

المسح (على مستوى الجهاز فقط)

ضمن "مسح"، يمكنك استعادة الجهاز إلى إعدادات المصنع. هنا سيتم حذف بيانات الشركة وكذلك البيانات الخاصة على جهاز المستخدم النهائي.

بالنقر على "رمز ناقص" يجب أن تتلقى الرسالة التالية



باستخدام "نعم" يمكنك إجراء المسح.

تحت عنوان "تقرير المسح" يمكن عرض العناصر التالية

ممسوح بواسطة	تاريخ من قام بالمسح
التاريخ	التاريخ
الحالة	الحالة (على سبيل المثال، إذا تم إجراء المسح بنجاح)

إعدادات التقييد

وظائف الجهاز

هنا يمكنك حظر وظائف جهاز المستخدم النهائي الفردية

السماح بتثبيت التطبيقات	السماح بتثبيت التطبيقات
السماح للكاميرا	السماح باستخدام الكاميرا
السماح بخدمة FaceTime	السماح بخدمة FaceTime
السماح بالتقاط الشاشة	السماح بالتقاط الشاشة
السماح بالمزامنة التلقائية أثناء التجوال	السماح بالمزامنة التلقائية أثناء التجوال
السماح لسيري	السماح لسيري
السماح بالاتصال الصوتي	السماح بالاتصال الصوتي
السماح بالشراء داخل التطبيق	السماح بالشراء داخل التطبيق
طلب كلمة مرور لمتجر iTunes لجميع عمليات الشراء	طلب كلمة مرور لمتجر iTunes لجميع عمليات الشراء
السماح بالألعاب متعددة اللاعبين	السماح بالألعاب متعددة اللاعبين
السماح بإضافة أصدقاء مركز اللعب Game Center	السماح بإضافة أصدقاء مركز اللعب Game Center
السماح بالفتح من مُدار إلى غير مُدار	السماح بفتح المحتوى في التطبيقات المُدارة في التطبيقات غير المُدارة
السماح بالفتح من غير مُدار إلى مُدار	السماح بفتح المحتوى في التطبيقات غير المُدارة في التطبيقات المُدارة
السماح بعرض اليوم في شاشة القفل	عندما يكون هذا الإعداد نشطًا، سيتم عرض عرض "اليوم" في مركز الإشعارات على شاشة القفل
السماح لمركز التحكم في شاشة القفل	السماح لمركز التحكم على شاشة القفل
السماح باستخدام معرّف اللمس	السماح باستخدام معرّف اللمس
السماح بتحديثات PKI عبر الأثير	السماح بتحديثات PKI عبر الأثير
السماح بدفتر المرور أثناء القفل	السماح بدفتر المرور أثناء قفل الجهاز
الحد من تتبع الإعلانات	تعمل هذه الوظيفة على إلغاء تنشيط تتبع الإعلانات (على سبيل المثال لا يمكن للمعلنين استخدام تتبع الإعلانات من أجل توزيع إعلانات مخصصة)
السماح بالمناولة	السماح بالمناولة

السماح بنتائج الإنترنت في دائرة الضوء	السماح بنتائج الإنترنت في دائرة الضوء (مثل Bing أو Wikipedia)
طلب رمز المرور عند أول إقران AirPlay	طلب رمز المرور عند أول إقران AirPlay
قوة حماية المعصم لساعة القوة	إذا تم تفعيلها، فإن ساعة Apple Watch مجبرة على استخدام "حماية المعصم" (التعرف على المعصم)
السماح لمكتبة صور iCloud	السماح بمكتبة صور iCloud. إذا لم يُسمح بذلك، فسيتم مسح جميع الصور التي لم يتم تنزيلها بالكامل من iCloud، على وحدة التخزين المحلية
متوفر في الوضع الخاضع للإشراف	
السماح بتعديل الحساب	السماح بتعديل "البريد، وجهات الاتصال، والتقويم"
السماح ب AirDrop	السماح ب AirDrop
السماح بالتعديل الخلوي للتطبيق الخلوي	يحظر هذا الإعداد الإعداد الإعداد الذي يسمح للتطبيقات باستخدام بيانات الهاتف المحمول يمكن تعيين هذا الإعداد، على سبيل المثال، يدوياً على جهاز المستخدم النهائي ومن ثم يمكن تفعيل هذا القيد
السماح لسيري بالاستعلام عن المحتوى الذي ينشئه المستخدم من الويب	يتم حظر البحث على الويب على مواقع إلكترونية معينة، مثل ويكيبيديا، لأن كل شخص يمكنه إجراء تغييرات كما يحلو له
تمكين فلتر الألفاظ النابية في Siri	الألفاظ النابية الموجهة إلى سيري تخضع للرقابة
السماح لمتجر iBook Store	السماح لمتجر iBook Store
السماح بمتجر iBook Store Erotica	السماح بمتجر iBook Store Erotica
السماح بتعديل إعدادات "العثور على أصدقائي	السماح بتعديل إعدادات "العثور على أصدقائي
السماح لمركز الألعاب	السماح لمركز الألعاب
السماح بإقران المضيف	اقتران كمبيوتر التحكم بالكمبيوتر
السماح بتثبيت ملفات تعريف التكوين	السماح بتثبيت ملفات تعريف التكوين
السماح بإزالة التطبيق	إزالة تطبيقات التحكم
السماح برسالة iMessage	السماح برسالة iMessage
السماح بمسح جميع المحتويات والإعدادات	السماح بمسح جميع المحتويات والإعدادات
السماح بتكوين القيود	السماح بتكوين القيود

السماح بالبودكاست	السماح بالبودكاست
السماح بالبحث عن التعريف	السماح بالبحث عن التعريف
السماح بلوحة المفاتيح التنبؤية	السماح بلوحة المفاتيح التنبؤية
السماح بالتصحيح التلقائي	السماح بالتصحيح التلقائي
السماح بتثبيت تطبيق واجهة المستخدم	في حالة إلغاء التفعيل، لا يمكن تثبيت أي تطبيقات من AppStore العام (لن يتم عرض الأيقونة بعد الآن). ومع ذلك، لا يزال من الممكن تثبيت التطبيقات عبر iTunes وأداة التهيئة
السماح باختصارات لوحة المفاتيح	السماح باختصارات لوحة المفاتيح، إذا كان الجهاز متصلاً بلوحة مفاتيح فعلية
السماح بإقران ساعة Apple Watch	يمنع الاقتران بين الجهاز وساعة Apple Watch، وسيتم إنهاء الاتصالات الحالية
السماح بتعديل رمز المرور	في حالة عدم السماح بذلك، لا يمكن إضافة كلمة مرور الجهاز أو تغييرها أو إزالتها
السماح بتعديل اسم الجهاز	إرشادات تحديد ما إذا كان يمكن تغيير اسم الجهاز
السماح بتعديل الخلفية	إرشادات تحديد ما إذا كان يمكن تغيير الخلفية
السماح بالتنزيلات التلقائية للتطبيقات	في حالة إلغاء التفعيل، لن يتم تثبيت التطبيق الذي تم شراؤه تلقائيًا على الأجهزة الأخرى. لا ينطبق على تحديثات التطبيقات الحالية
السماح بالأخبار	السماح بالأخبار على جهاز iOS
السماح بالثقة في تطبيق المؤسسة	إذا تم تعيينه على خطأ، يمنع الثقة في تطبيقات المؤسسات

آي كلاود

حظر وظائف معينة أثناء الاقتران على iCloud

السماح بالنسخ الاحتياطي	السماح بالنسخ الاحتياطي
السماح بمزامنة المستندات	السماح بمزامنة المستندات
السماح ببث الصور	السماح ببث الصور
السماح بتدفق الصور المشتركة	السماح بتدفق الصور المشتركة
السماح بمزامنة سلسلة المفاتيح السحابية	السماح بمزامنة سلسلة المفاتيح السحابية
السماح للتطبيقات المُدارة بتخزين البيانات	السماح للتطبيقات المُدارة بتخزين البيانات
السماح بمزامنة الملاحظات والميزات البارزة لكتب المؤسسة	السماح بمزامنة الملاحظات والتمييزات لكتب المؤسسة
السماح بالنسخ الاحتياطي لكتب المؤسسة	السماح بالنسخ الاحتياطي لكتب المؤسسة

الأمان والخصوصية

حظر هذه الوظائف المرتبطة بالبيانات التشخيصية

السماح بإرسال بيانات التشخيص إلى Apple	السماح بإرسال بيانات التشخيص إلى Apple
السماح للمستخدم بقبول شهادات TLS غير الموثوق بها	السماح للمستخدم، لقبول شهادات TLS غير الموثوق بها
فرض النسخ الاحتياطية المشفرة	فرض النسخ الاحتياطية المشفرة

BYOD

أمان iOS المدمج (حاوية)

لطالما كان نظام iOS قادرًا على التمييز بين المُدار (الأعمال) وغير المُدار (الخاص). يتم التعامل مع كل ما يأتي من نظام MDM على أنه مُدار. على سبيل المثال إذا قمت بتثبيت تطبيق عبر نظام MDM أو تهيئة حساب Exchange، فسيتم التعامل مع ذلك على أنه مُدار من قبل نظام iOS.

سيتم التعامل مع أي شيء آخر يتم تهيئته/تثبيته يدويًا على الجهاز على أنه غير مُدار. على سبيل المثال إذا قام المستخدم بتثبيت واتساب من تلقاء نفسه أو إذا كان المستخدم يضيف حساب Exchange. لكن هذا الفصل لم يؤثر أبدًا على جهات الاتصال. ولكن منذ نظام التشغيل iOS 11.3 (والإصدارات الأحدث) تمت إضافة هذا أيضًا لجهات الاتصال.

نظرًا لأن هذه وظيفة أساسية في نظام التشغيل، فلن تحتاج إلى تثبيت شيء ما أو إعداد حاوية خاصة.

قم بتنشيط الوظيفة المدمجة للفصل بين التطبيقات/المعلومات/الملفات الخاصة وتطبيقات/ملفات العمل. سيؤدي هذا الإعداد أيضًا إلى تعطيل بعض الوظائف الأخرى، التي قد تؤدي إلى إيقاف تشغيل أجزاء من هذا الفصل عن طريق الخطأ.

التفعيل

تنشيط حلول الحاويات التي تدعمها AppTec360

تمكين حاوية Google Divide Container	تمكين حاوية Google Divide Container
تمكين حاوية SecurePIM الآمنة	تمكين حاوية SecurePIM الآمنة

في حال قمت بتفعيل حاوية SecurePIM، ستجد أيضاً النقطة التالية تحت عنوان "التفعيل". بالإضافة إلى ذلك، سيتم فتح أربع علامات تبويب أخرى على الفور، وهي موضحة أدناه.

عنوان البريد الإلكتروني للدعم	عنوان البريد الإلكتروني للدعم حيث يمكن للمستخدم اللجوء إليه في حالة وجود مشاكل

كلمة مرور SecurePIM الآمنة

ضمن "كلمة مرور SecurePIM الآمنة"، يمكنك وضع المبادئ التوجيهية لقوة أمان كلمة المرور.

مهلة الجلسة	هنا يمكنك تحديد عدد الدقائق التي يجب إدخال كلمة مرور جديدة بعد كم دقيقة يجب إدخال كلمة مرور جديدة مرة أخرى، بمجرد تشغيل SecurePIM في الخلفية
طول كلمة المرور	طول كلمة المرور للدخول إلى حاوية SecurePIM الآمنة
الأحرف الكبيرة	الحد الأدنى من الأحرف الكبيرة
الأحرف الصغيرة	الحد الأدنى من الأحرف الصغيرة
الشخصيات الخاصة	الحد الأدنى من الأحرف الخاصة
الأرقام	الحد الأدنى من الأرقام
تطبيق المسح	عدد المرات التي يمكن فيها إدخال كلمة مرور بشكل غير صحيح، قبل أن يتم حذف محتوى SecurePIM (ومع ذلك، يظل التطبيق موجودًا على جهاز المستخدم النهائي)

أمان SecurePIM الآمن

ضمن "SecurePIM Security"، يمكنك إنشاء مجموعة متنوعة من إعدادات الأمان.

الكشف عن أجهزة Jailbroken	إذا تم تفعيل هذا الإعداد، فسيتم حظر الوصول إلى حاوية SecurePIM، بمجرد اكتشاف أن الجهاز مكسور الحماية
الحقول النصية الآمنة	سيتم تشفير محتوى حقول التقديم، ولن تصل أي معلومات إلى نظام التشغيل (iOS) ملاحظة: طالما كان هذا الإعداد نشطًا، فلن يكون التصحيح التلقائي متاحًا
تصدير بيانات الاتصال إلى الجهاز	في حالة تفعيل هذا الإعداد، يُسمح للمستخدم بتصدير جهات اتصال Exchange إلى جهازه المحلي ملاحظة: يتم تصدير الاسم ورقم الهاتف فقط
عرض موقع الحدث	في حالة تنشيط هذا الإعداد، سيتم عرض موقع الأحداث القادمة في شريط الإشعارات
إظهار عنوان الحدث	إذا تم تفعيل هذا الإعداد، فسيتم عرض موقع عنوان الحدث القادم في شريط الإشعارات

متصفح SecurePIM الآمن

هنا يمكنك تهيئة متصفح SecurePIM.

باستخدام الرمز، يمكنك تحديد عنوان URL جديد.

باستخدام الرمز، يمكنك إزالة عنوان URL محدد مرة أخرى.

"عناوين URL المدرجة في القائمة البيضاء" هي عناوين URL التي يمكن تحميلها.

"عناوين URL المدرجة في القائمة السوداء" هي عناوين URL التي لا يمكن تحميلها وبالتالي يتم حظرها.

يرجى ملاحظة أن إدخالات القائمة البيضاء لها أولوية أعلى من إدخالات القائمة السوداء. تحت "عنوان الإشارة المرجعية" يمكنك إصدار عنوان. باستخدام "عنوان URL للإشارة المرجعية"، يمكنك ربط عنوان URL بعنوان الإشارة المرجعية - وبهذه الطريقة يمكنك توزيع إشارات مرجعية فردية على المستخدمين المعنيين.

المبادلات

ضمن "Exchange" يمكنك تكوين حساب Exchange تحت عنوان "Exchange".

عنوان البريد الإلكتروني لـ ActiveSync	عنوان البريد الإلكتروني للتبادل (لاحظ "العناصر النائبة")
تسجيل الدخول إلى برنامج ActiveSync Exchange	تبادل أسماء المستخدمين (لاحظ "العناصر النائبة")
خادم أكتيف سينك إكستشينك إكستشينج	عنوان خادم التبادل (FQDN)
نطاق تبادل ActiveSync ActiveSync Exchange	عنوان نطاق التبادل
شهادة المستخدم	شهادة المستخدم
المصادقة المستندة إلى الشهادة	يصادق المستخدم على نفسه بشهادة
السماح بتشفير S/MIME	السماح للمستخدم بتشفير بريده الإلكتروني
السماح بتوقيع S/MIME	السماح للمستخدم بالتوقيع على بريده
التحقق من CRL	إذا كانت الشهادة الخاصة نشطة، ستتم مقارنة الشهادة الخاصة بقائمة إبطال الشهادات (CRL)

إدارة الاتصال

الواي فاي

معرّف مجموعة الخدمات (SSID)	SSID للشبكة التي سيتم الاتصال بها
الانضمام التلقائي	تفعيل الانضمام التلقائي عند الانضمام إلى شبكة
الشبكة الخفية	تنشيط، في حالة عدم قيام نقطة الوصول إلى نقطة الوصول ببث SSID

إعداد الوكيل

تكوين وكيل لكل نقطة وصول لكل نقطة وصول

لا يوجد	عدم إنشاء أي وكيل
يدوي	إنشاء وكيل يدوي
عنوان URL الخادم الوكيل	عنوان الوصول إلى إعدادات الوكيل
الميناء	إنشاء المنفذ الخاص بالوكيل
المصادقة	اسم المستخدم الخاص بالمصادقة على البروكسي
كلمة المرور	كلمة المرور الخاصة بالمصادقة على الوكيل
أوتوماتيكي	إنشاء وكيل تلقائياً
عنوان URL الخادم الوكيل	عنوان URL للوصول إلى إعدادات الوكيل

نوع الأمان

إنشاء نوع الأمان لبروتوكول الوصول الآمن

WEP	
كلمة المرور	كلمة المرور الخاصة بـ AP

WPA/WPA2	
كلمة المرور	كلمة المرور الخاصة بـ AP

WEP للمؤسسات - WPA / WPA2 للمؤسسات - أي مؤسسة WEP - أي مؤسسة		
البروتوكولات		
TLS	تنشيط/إلغاء التنشيط	
TTLS	تنشيط/إلغاء التنشيط	
برنامج LEAP	تنشيط/إلغاء التنشيط	
PEAP	تنشيط/إلغاء التنشيط	
EAP-FAST	تنشيط/إلغاء التنشيط	
EAP-SIM	تنشيط/إلغاء التنشيط	
استخدام PAC		استخدام نظام التحكم في الوصول المحمي (PAC)
توفير PAC	تكوين توفير PAC	
توفير PAC بشكل مجهول	التوفير المجهول لـ PAC	
المصادقات الداخلية	بروتوكول المصادقة الذي يجب استخدامه: PAP، CHAP، CHAP، MSCHAP، MSCHAPv2	
اسم المستخدم	اسم مستخدم المصادقة	
عدم استخدام كلمة المرور لكل اتصال	عدم استخدام كلمة المرور لكل اتصال	
شهادة الهوية	تحميل/تحديد شهادة المصادقة	
الهوية الخارجية	الهوية التي يمكن رؤيتها خارجيًا	
الثقة		
الشهادة الموثوقة 1	تحميل أول شهادة موثوق بها	
الشهادة الموثوقة 2	تحميل شهادة ثانية موثوق بها	
الشهادة الموثوقة 3	تحميل شهادة ثالثة موثوق بها	
أسماء شهادات الخادم الموثوق به	أسماء شهادات الخادم المتوقعة (في قائمة مفصولة بفاصلة)	

لا يوجد	عدم إنشاء أي أمان

VPN

اسم الاتصال	اسم ملف تعريف VPN-ملف تعريف VPN

نوع VPN

VPN

سيتم توجيه كل حركة مرور شبكة الجهاز عبر اتصال VPN.

نوع الاتصال		إنشاء نوع اتصال VPN
IPsec (سيسكو)		بروتوكول IPsec من سيسكو
PPTP		بروتوكول PPTP
L2TP		بروتوكول L2TP
Cisco AnyConnect		بروتوكول AnyConnect
جونيبر SSL		بروتوكول SSL جونيبر SSL
F5 SSL		بروتوكول F5 SSL
سونيك وول mConnect		سونيك وول موبايل كونكت
أروبا فيا		بروتوكول أروبا VIA
SSL مخصص		الاتصال عبر SSL مخصص SSL
OpenVPN		بروتوكول OpenVPN

لكل تطبيق VPN

عند فتح تطبيق معين، سيتم إنشاء اتصال VPN

بدء الاتصال بشبكة VPN لكل تطبيق تلقائياً	بدء الاتصال بشبكة VPN لكل تطبيق تلقائياً
نوع الاتصال	إنشاء نوع اتصال VPN
Cisco AnyConnect	بروتوكول AnyConnect
جونيبر SSL	بروتوكول SSL جونيبر SSL
F5 SSL	بروتوكول F5 SSL
سونيك وول mConnect	سونيك وول موبايل كونكت
أروبا فيا	بروتوكول أروبا VIA
SSL مخصص	الاتصال عبر SSL مخصص SSL
OpenVPN	بروتوكول OpenVPN

إعداد الوكيل

تكوين وكيل للاتصال بشبكة VPN

لا يوجد	عدم إنشاء أي وكيل
يدوي	إنشاء وكيل يدوياً
عنوان URL الخادم الوكيل	عنوان الوصول إلى إعدادات الوكيل
الميناء	إنشاء المنفذ الخاص بالوكيل
المصادقة	اسم المستخدم للمصادقة في الوكيل
كلمة المرور	كلمة المرور للمصادقة في الوكيل
أوتوماتيكي	إنشاء وكيل تلقائياً
عنوان URL الخادم الوكيل	عنوان URL للوصول إلى إعدادات الوكيل

إظهار العناصر النائبة	يعرض جميع متغيرات المستخدم المتاحة، التي يمكن أن يستخدمها AppTec360

شبكة APN

اسم نقطة الوصول	اسم نقطة الوصول
اسم مستخدم نقطة الوصول	اسم مستخدم نقطة الوصول
كلمة مرور نقطة الوصول	كلمة مرور نقطة الوصول
خادم وكيل	عنوان الخادم الوكيل
الميناء	منفذ الوكيل المعني

خلوي

تمكين تجوال البيانات	تمكين تجوال البيانات
تمكين التجوال الصوتي	تمكين التجوال الصوتي
تمكين نقطة الاتصال	تمكين نقطة الاتصال

وكيل HTTP

نوع الوكيل	
يدوي	إنشاء وكيل يدوياً
عنوان URL الخادم الوكيل	عنوان الوصول إلى إعدادات الوكيل
الميناء	إنشاء منفذ الوكيل
المصادقة	اسم المستخدم للمصادقة في الوكيل
كلمة المرور	كلمة المرور للمصادقة في الوكيل
أوتوماتيكي	إنشاء وكيل تلقائياً
عنوان URL لـ PAC الوكيل	عنوان URL لـ PAC الوكيل
السماح بالاتصال المباشر في حالة تعذر الوصول إلى PAC	السماح بالاتصال المباشر (بدون VPN)، إذا تعذر الوصول إلى PAC
السماح بتجاوز البروكسي للوصول إلى الشبكات الأسيرة	السماح بتجاوز البروكسي للوصول إلى الشبكات الداخلية الأسيرة

AirPrint

عنوان IP	عنوان IP للطابعة
مسار الموارد	مسار محدد إلى جهاز AirPrint

AirPlay

اسم الجهاز	اسم الجهاز
كلمة المرور	كلمة مرور الاقتران
القائمة البيضاء	تحديد قائمة بالأجهزة التي يمكن للجهاز الاقتران بها حصريًا

إدارة PIM

المزامنة النشطة للتبادل

اسم الحساب	اسم حساب البريد الإلكتروني
مضيف Exchange ActiveSync Exchange ActiveSync	عنوان/رقم QDN للخادم
السماح بالتحرك	السماح بنقل رسائل البريد الإلكتروني
الاستخدام في البريد فقط	قد تحدث التفاعلات على تطبيق البريد الأصلي فقط
استخدام SSL	استخدام تشفير SSL
المجال	مجال الخادم
المستخدم	اسم المستخدم
عنوان البريد الإلكتروني	عنوان البريد الإلكتروني (على مستوى الجهاز فقط)
كلمة المرور (على مستوى الجهاز فقط)	كلمة مرور المستخدم
شهادة الهوية	حدد الشهادة المعنية للمصادقة على الخادم
الأيام الماضية من البريد للمزامنة	عدد الأيام، حتى تتم مزامنة رسائل البريد الإلكتروني مرة أخرى. بلا حدود = غير محدود
تمكين S/MIME	تمكين تشفير S/MIME
توقيع الشهادة	تحميل شهادة التوقيع المعنية
شهادة التشفير	تحميل شهادة التشفير المعنية

البريد الإلكتروني

إعداد حسابات POP3/ IMAP على جهاز المستخدم النهائي

وصف الحساب	اسم حساب البريد الإلكتروني		
نوع الحساب	IMAP	بادئة المسار	بادئة المسار للمجلدات الخاصة
	الملوثات العضوية الثابتة		
اسم عرض المستخدم	اسم عرض المستخدم		
عنوان البريد الإلكتروني	عنوان البريد الإلكتروني للمستخدم		
السماح بالتحرك	السماح بنقل رسائل البريد الإلكتروني		
تمكين S/MIME	تمكين تشفير S/MIME		
توقيع الشهادة	تحميل شهادة التوقيع المعنية		
شهادة التشفير	تحميل شهادة التشفير المعنية		

البريد الوارد

إعدادات الخادم الوارد

عنوان خادم البريد	عنوان خادم البريد
منفذ خادم البريد	منفذ خادم البريد
اسم المستخدم	اسم المستخدم المعني
نوع المصادقة	نوع المصادقة
لا يوجد	لا يوجد نوع مصادقة
كلمة المرور (على مستوى الجهاز فقط)	مطالبة كلمة المرور
الاستجابة لتحديات إدارة الألفية الجديدة	
NTLM	مصادقة NTLM-المصادقة
HTTP MD5 Digest	
استخدام SSL	استخدم SSL، إذا لزم الأمر

البريد الصادر

إعدادات الخادم الصادر

عنوان خادم البريد	عنوان خادم البريد
منفذ خادم البريد	منفذ خادم البريد
اسم المستخدم	اسم المستخدم المعني
نوع المصادقة	
لا يوجد	لا توجد طريقة مصادقة
كلمة المرور (على مستوى الجهاز فقط)	مطالبة كلمة المرور
الاستجابة لتحديات إدارة الألفية الجديدة	
NTLM	مصادقة NTLM-المصادقة
HTTP MD5 Digest	
استخدام SSL	استخدم SSL، إذا لزم الأمر
كلمة المرور الصادرة نفس كلمة المرور الواردة	كلمة المرور الصادرة نفس كلمة المرور الواردة
الاستخدام في البريد فقط	تنشيط، إذا كانت جميع رسائل البريد الإلكتروني الصادرة سيتم إرسالها عبر تطبيق البريد الإلكتروني

كالداف

تكوين إعداد حساب CalDav وتوزيع حساب CalDav

وصف الحساب	اسم العرض للحساب
اسم المضيف	اسم المضيف و/أو عنوان IP
الميناء	منفذ حساب CalDav
عنوان URL الرئيسي	عنوان URL الرئيسي للحساب
اسم المستخدم	اسم المستخدم الخاص ب CalDav
كلمة المرور (على مستوى الجهاز فقط)	كلمة مرور CalDav المحتملة
استخدام SSL	استخدم SSL، إذا لزم الأمر

التقويمات المشتركة

إعداد التقويمات المشتركة وتوزيعها

الوصف	اسم العرض للحساب
عنوان URL	عنوان URL لقاعدة بيانات التقويم
اسم المستخدم	اسم مستخدم اشتراك التقويم
كلمة المرور (على مستوى الجهاز فقط)	كلمة مرور اشتراك التقويم
استخدام SSL	استخدم SSL، إذا لزم الأمر

LDAP

في هذا المجال، قم بإعداد اتصال LDAP، من أجل السماح بتبادل ديناميكي للشهادات، بين جهاز المستخدم النهائي والدليل النشط.

يرجى ملاحظة أن المستخدم المحدد يتطلب إذن القراءة المعني.

وصف الحساب	وصف الحساب
اسم مستخدم الحساب	مستخدم للدخول إلى LDAP
كلمة مرور الحساب	كلمة المرور للدخول إلى LDAP
اسم مضيف الحساب	اسم مضيف خادم LDAP/عنوان IP
استخدام SSL	استخدم SSL، إذا لزم الأمر

في الجزء الثاني، يمكنك تحديد عوامل تصفية فردية للبحث في سجل LDAP.

الوصف	النطاق	قاعدة البحث
وصف المرشح	مستوى البحث في سجل LDAP	تحديد المرشح الفردي

إدارة الويب

مقاطع الويب

في هذا الموقع تحديد الإشارات المرجعية، مع روابط لصفحات الويب وبوابات الإنترانت وما إلى ذلك، والتي ستكون مرئية كتطبيق على جهاز المستخدم النهائي.

التسمية	اسم الاتصال على جهاز المستخدم النهائي
عنوان URL	رابط الموقع الإلكتروني المعني
قابل للإزالة	في حالة تفعيله، يمكن للمستخدم إزالة مشبك الويب
أيقونة	عبر هذا الحوار، قم بتحميل شعار للاتصال: الأبعاد 180×180، بصيغة png
أيقونة مركبة مسبقاً	في حالة تفعيلها، لن يتم عرض أي تأثيرات إضافية (ظل، انعكاس) على الأيقونة
شاشة كاملة	عند فتح مقاطع الويب، يتم فتح المتصفح في وضع ملء الشاشة

تصفية محتوى الويب

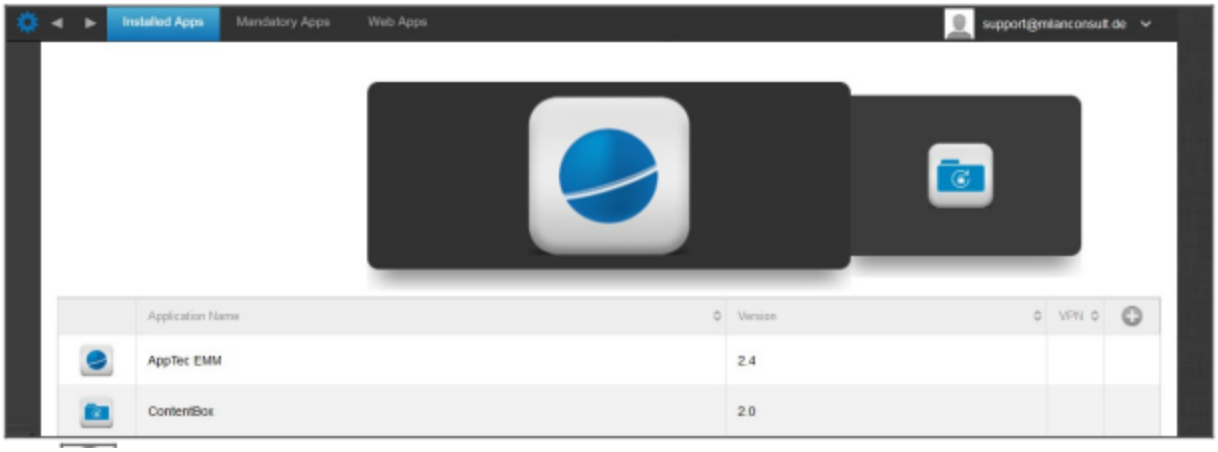
يتيح عامل تصفية محتوى الويب إمكانية تقييد الوصول إلى صفحات إنترنت محددة.

المواقع الإلكترونية المسموح بها	
الحد من محتوى البالغين	يتم تطبيق فلتر الويب تلقائياً على محتوى البالغين
عناوين URL المسموح بها	باستخدام الرمز + إضافة الصفحات المسموح بها
عناوين URL المدرجة في القائمة السوداء	باستخدام رمز + إضافة الصفحات المحظورة
مواقع إلكترونية محددة فقط	يمكن عرض محتوى محدد فقط، والذي يمكنك إضافته باستخدام الرمز +.

إدارة التطبيقات

مدير تطبيقات المؤسسات

التطبيقات المثبتة (على مستوى الجهاز فقط)



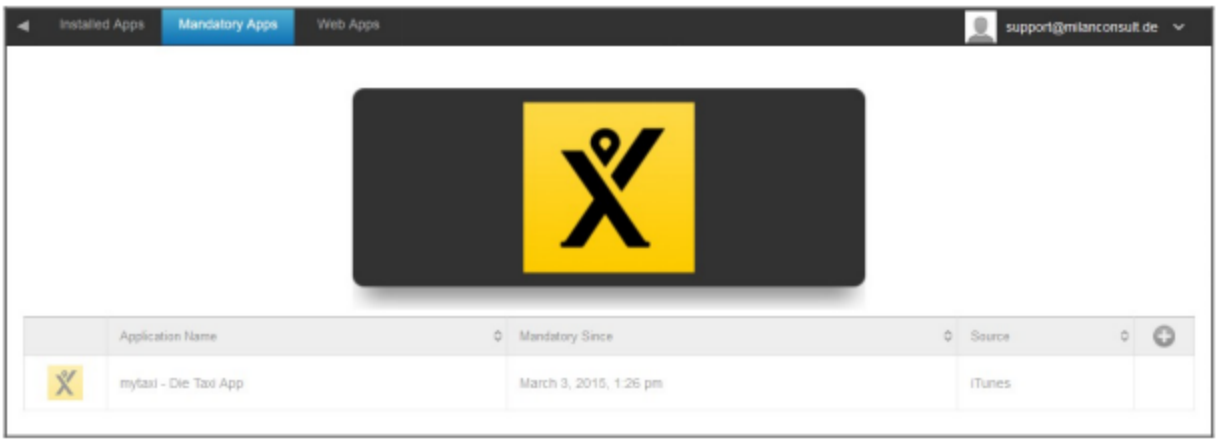
هنا يمكنك رؤية التطبيقات المثبتة حالياً على الجهاز.

التطبيقات الإلزامية

ضمن التطبيقات الإلزامية، يمكنك تفويض التطبيقات الضرورية.

سيتم تذكير المستخدم باستمرار بتثبيت هذا التطبيق المذكور.

من خلال، يمكن تعريف التطبيق المفوض.



يمكن أن يكون هذا تطبيق متجر تطبيقات Apple App Store، ولكن يمكن أن يكون تطبيقاً داخلياً أيضاً.

إذا كان ذلك يتضمن جهازاً خاضعاً للإشراف، فسيتم تثبيت التطبيق تلقائياً.

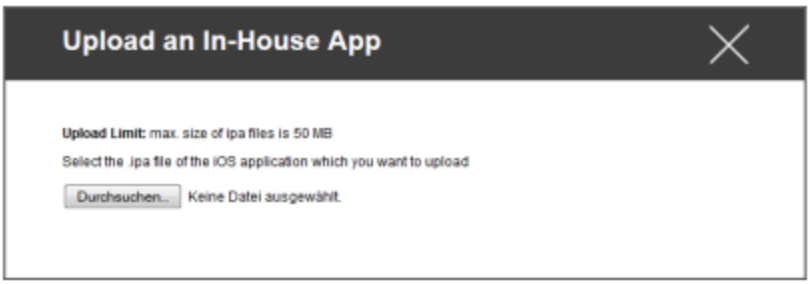
يمكنك دفع تطبيق "Apple AppStore" من AppStore العام إلى الجهاز، بالإضافة إلى تطبيق داخلي مطور داخلياً.

أو يمكنك الاختيار من فئة "تطبيقات iOS الداخلية" واختيار تطبيق داخلي قمت بتحميله ضمن الإعدادات العامة.

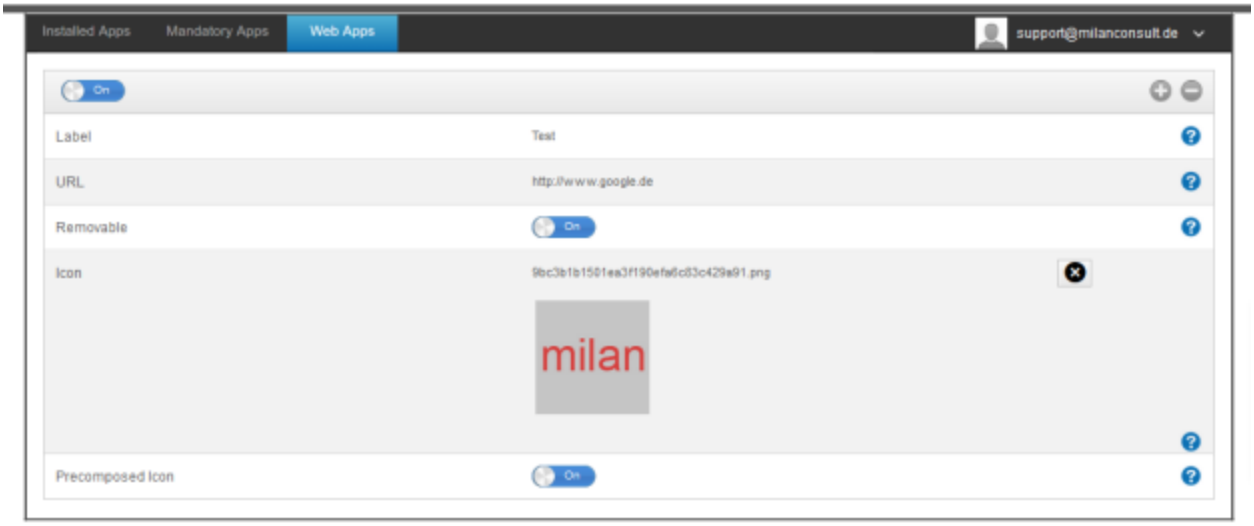
خيارات التثبيت-خيارات التثبيت

مواكبة آخر المستجدات (مدعومة فقط لـ VPP لكل جهاز)	مرة واحدة في الأسبوع، سيتم تحديد ما إذا كان هناك تحديث للتطبيق. إذا كانت الإجابة بنعم، سيتم تثبيت هذا التحديث بالنسبة للتطبيقات الداخلية، سيتم استخدام هدف التحديث الذي قمت بتكوينه في الإعدادات العامة لعملية التحديث.
التجاوز عند عدم الإدارة	إذا كان التطبيق مثبتاً بالفعل، فسيتولى جهاز إدارة الأجهزة المحمولة MDM إدارة التطبيق
إزالة التطبيق عند إزالة ملف تعريف MDM	في حالة إزالة إدارة الجهاز، سيتم إلغاء تثبيت التطبيق
منع النسخ الاحتياطي لبيانات التطبيق	لن يتم إنشاء نسخة احتياطية للبيانات الخاصة بالتطبيق
إعداد التطبيق	ضمن "إعدادات التطبيق"، يمكنك تعيين قيم معينة للتطبيق في المقدمة (طالما أن التطبيق يدعم ذلك، إذا لزم الأمر اسأل مطور التطبيق).

يمكنك أيضًا تحديد ملف ipa وتحميله مباشرة، عبر "تحميل تطبيق داخلي".



تطبيقات الويب



تحت نقطة "تطبيقات الويب"، يمكنك، كما هو الحال مع "مقاطع الويب"، دفع صفحات الإنترنت أو بوابات الإنترانت كتطبيق على جهاز المستخدم النهائي، في منطقة إدارة الويب. بشكل افتراضي، سيتم عرض "تطبيقات الويب" في وضع ملء الشاشة، والذي يمكن تهيئته ضمن "مقاطع الويب".

التسمية	اسم الاتصال على جهاز المستخدم النهائي
عنوان URL	رابط الموقع الإلكتروني المعني
قابل للإزالة	إذا تم تنشيطه، يمكن للمستخدم إزالة مشبك الويب
أيقونة	عبر هذا الحوار، قم بتحميل شعار للاتصال: الأبعاد 180×180، بصيغة png
أيقونة مركبة مسبقاً	في حالة تفعيلها، لن يتم عرض أي تأثيرات إضافية (ظل، انعكاس) على الأيقونة

التقييد والإعدادات

التطبيقات المدرجة في القائمة السوداء/القائمة البيضاء

هنا يمكنك تعيين التطبيقات المحظورة (أو المسموح بها) بناءً على إعداداتك في "الإعدادات العامة". سيؤدي النقر على سيظهر لك البحث عن التطبيقات المعروفة. هناك يمكنك البحث عن التطبيقات التي تريد إضافتها.

لاحظ أن الجهاز الخاضع للإشراف ضروري لهذه الوظيفة

قيود SysApp

حظر تطبيقات أو وظائف معينة في جهازك

السماح باستخدام YouTube	السماح باستخدام YouTube
السماح باستخدام متجر iTunes	السماح باستخدام متجر iTunes
السماح باستخدام Safari	السماح باستخدام Safari
تمكين الملء التلقائي	السماح بالملء التلقائي
فرض التحذير من الاحتيال	يفرض التحذير من الاحتيال
تمكين JavScript	تمكين استخدام JavaScript
حظر النوافذ المنبثقة	يحجب جميع أنواع الجرو
السماح بملفات تعريف الارتباط	اختر متى يقبل Safari ملفات تعريف الارتباط

تطبيق-VPN

من خلال الرمز، يمكنك تحديد التطبيقات التي ستقوم تلقائياً بتشغيل اتصال VPN المحدد عند بدء التشغيل.

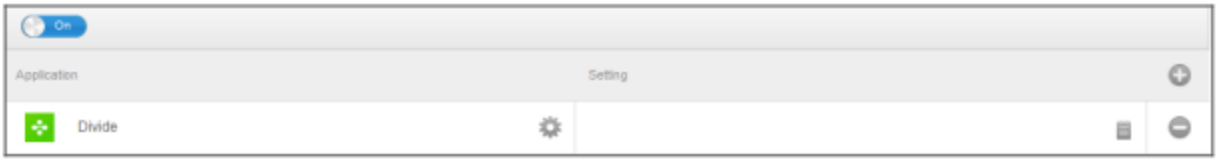
إعدادات التطبيق

ضمن "إعدادات التطبيق"، يمكنك تعيين قيم معينة للتطبيق في المقدمة (طالما أن التطبيق يدعم ذلك، إذا لزم الأمر اسأل مطور التطبيق).

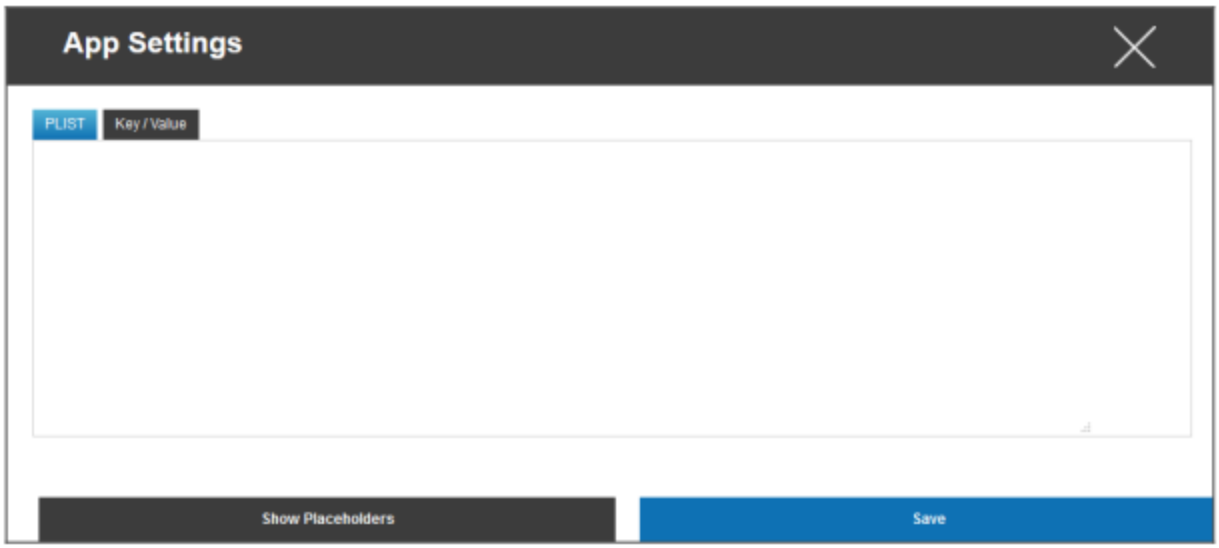
عبر الرمز، يمكنك إضافة تطبيق (إضافي). ستجد، مرة أخرى، تمثيل AppTec360 المألوف لتطبيق-استيراد التطبيقات.

ابحث هنا عن التطبيق الذي ترغب في تهيئته وحدده. سيتم تطبيق الإعدادات على التطبيقات المُدارة فقط.

في حالة نجاح عملية الاستيراد، سترى الشاشة التالية:

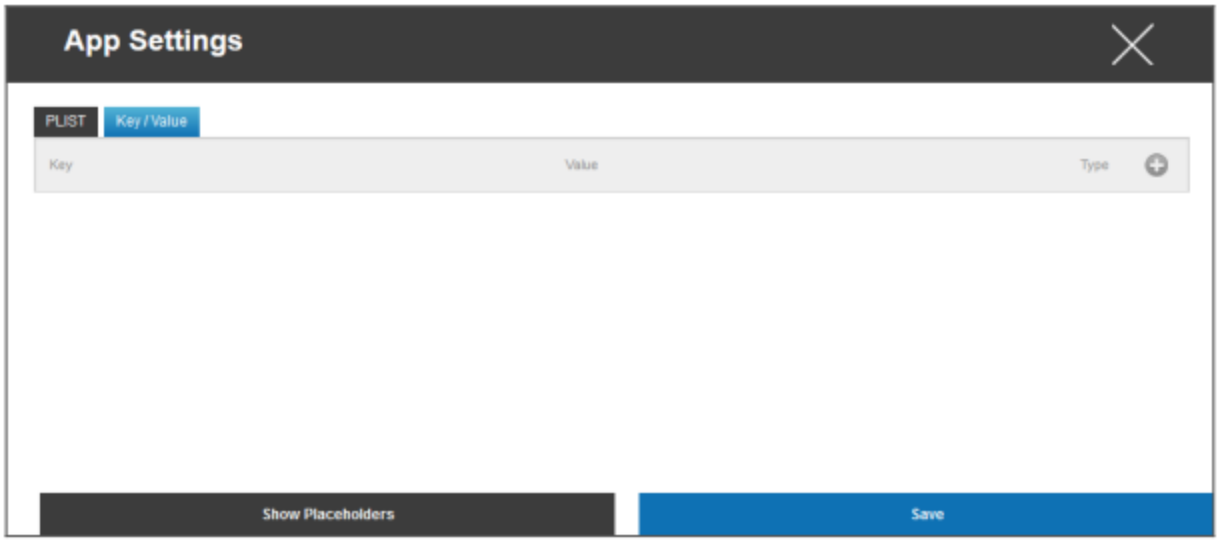


الآن، بنقرة على، يمكنك إجراء مجموعة متنوعة من التكوينات. ستتلقى بعد ذلك النظرة العامة التالية:

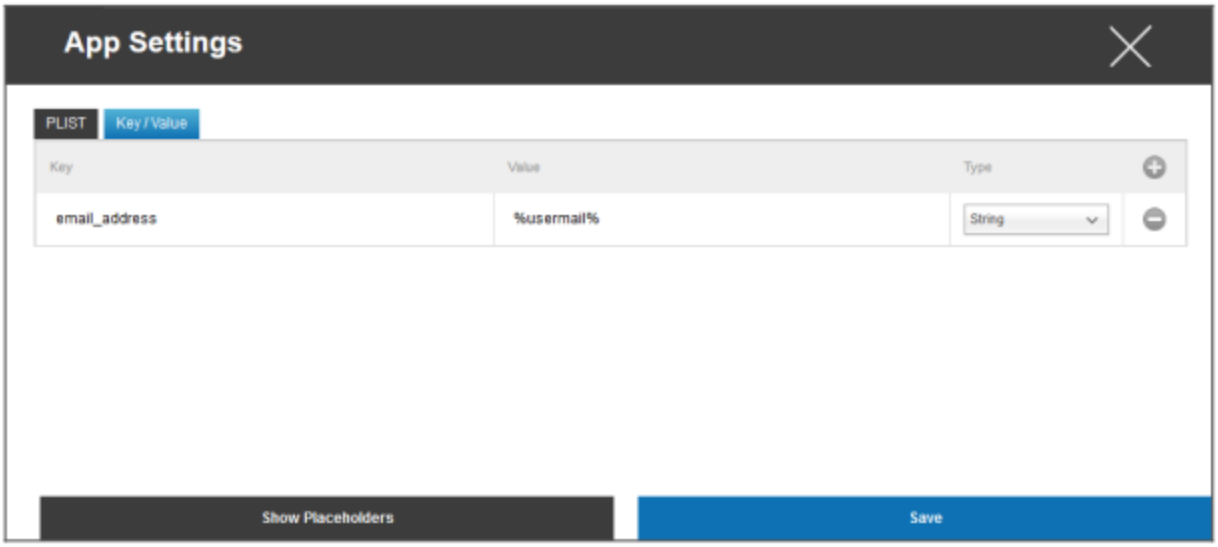


إذا كان لديك بالفعل قائمة PLIST (النص المصدر للتكوين)، يمكنك إضافتها هنا وحفظها كلها باستخدام "حفظ".

تحت "المفتاح/القيمة"، يمكنك إرفاق تكوينات محددة بالتطبيق



هنا، يمكنك إنشاء مفتاح جديد وقيمته بالرمز.



وبالطبع، جميع العناصر النائبة في AppTec تحت تصرفك

شرح "النوع":

الخيط	النص
منطقية	صواب/خطأ
العدد	العدد

باستخدام الرمز، يمكنك إزالة التطبيق مرة أخرى.

متجر تطبيقات المؤسسات

تطبيقات iTunes

تحت هذه النقطة، يمكنك توزيع تطبيقات اختيارية للمستخدم الخاص بك.

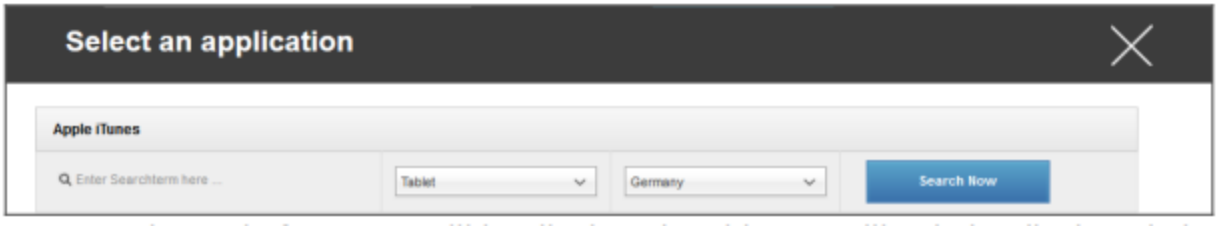
إذا كان هناك تطبيق هنا، فسيتم تثبيته تلقائياً على جهاز المستخدم النهائي لمتجر AppTec360.

هذه ببساطة روابط إلى متجر تطبيقات Apple الرسمي. ولهذا السبب، يجب تجهيز كل جهاز مستخدم نهائي بمعرف Apple.

في هذه المرحلة، نوصي بأن يكون لكل مستخدم معرف Apple الخاص به.

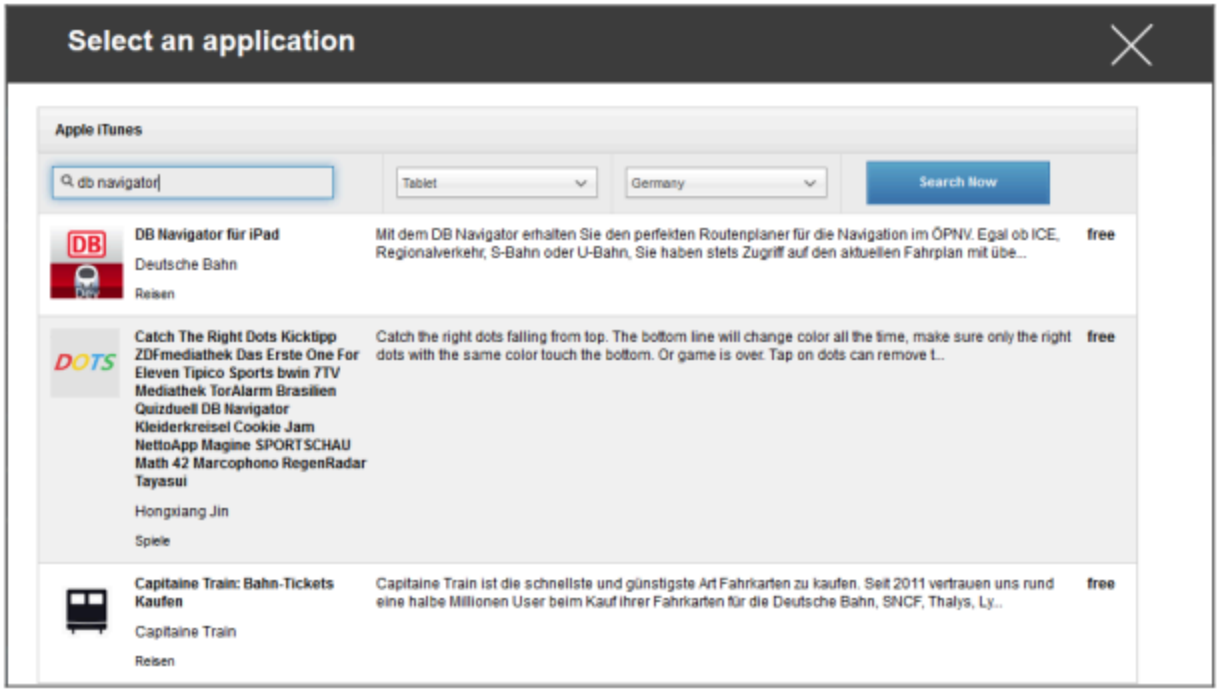
باستخدام الرمز، يمكنك إضافة تطبيقات إضافية.

بعد ذلك، يجب أن تفتح نافذة تحتوي على النظرة العامة التالية.



يُرجى ملاحظة أنه سيتم عرض التطبيقات المجانية فقط، وسيتم عرض التطبيقات المدفوعة فقط عبر VPN.

ضمن "أدخل مصطلح البحث هنا ..."، يمكنك البحث عن تطبيق موجود في متجر تطبيقات Apple.



وبمجرد النقر على الأيقونة أو على اسم التطبيق، سيُطلب منك مرة أخرى إجراء تكوينات إضافية.

مواكبة آخر المستجدات	مرة واحدة في الأسبوع، سيتم تحديد ما إذا كان هناك تحديث للتطبيق. إذا كانت الإجابة بنعم، سيتم تثبيت هذا التحديث
إزالة التطبيق عند إزالة ملف تعريف MDM	في حالة إزالة إدارة الجهاز، سيتم إلغاء تثبيت التطبيق
منع النسخ الاحتياطي لبيانات التطبيق	لن يتم إنشاء نسخة احتياطية للبيانات الخاصة بالتطبيق
تطبيق-VPN	اختر اتصال VPN، والذي سيتم تشغيله عند فتح التطبيق

بعد النقر على "تثبيت"، ستتم إضافة التطبيق إلى متجر تطبيقات المؤسسات ويمكن بعد ذلك تثبيته على جهاز المستخدم النهائي، عبر AppTec360 AppStore.

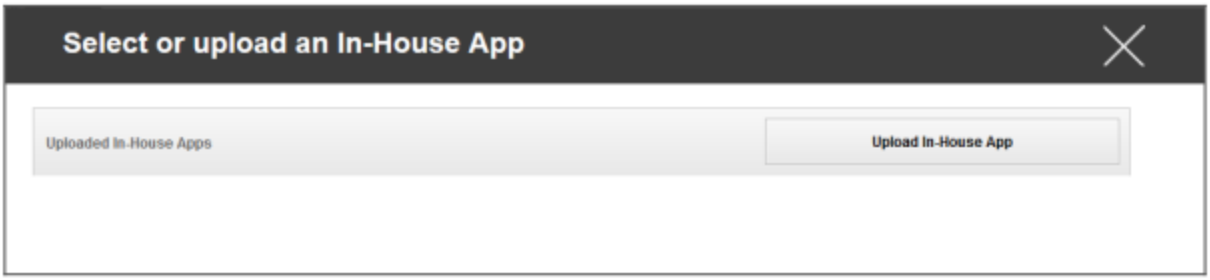
إذا تم استيراد متجر التطبيقات بنجاح، فستتلقى النظرة العامة التالية:

داخل الشركة

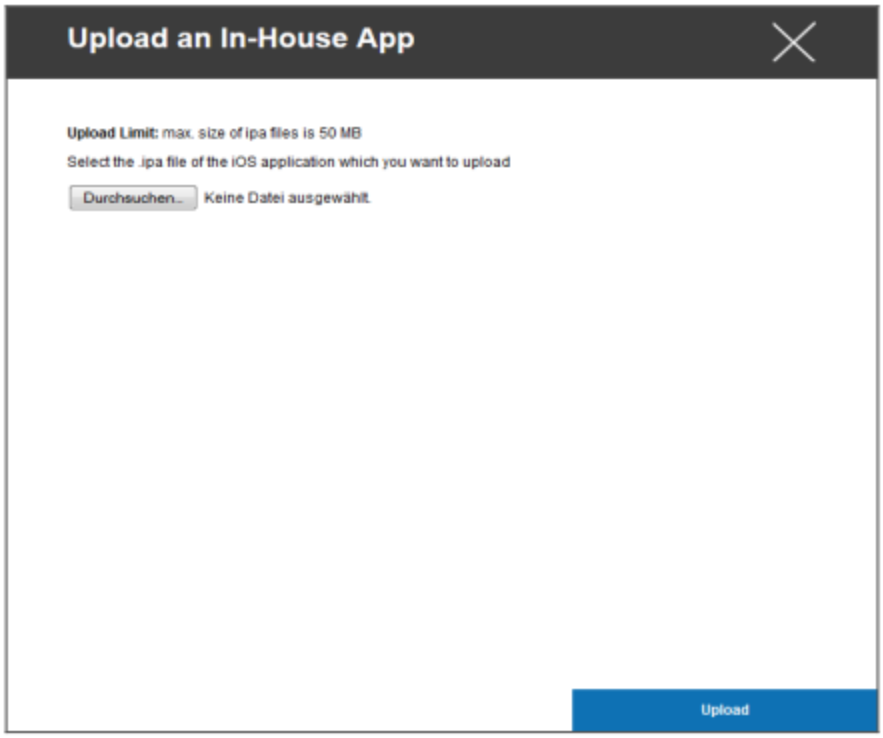
تحت نقطة "داخلياً"، يمكنك تحميل التطبيقات المطورة داخلياً وتوزيعها.

باستخدام الرمز، يمكنك توزيع تطبيقات إضافية داخل الشركة.

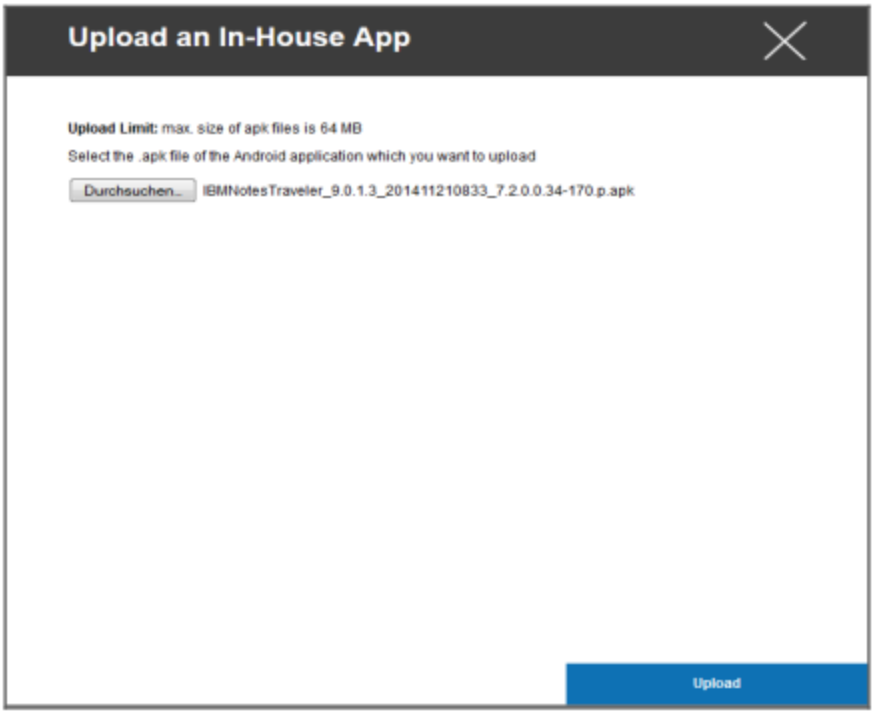
إذا لم تقم بتوزيع تطبيق In-House App من قبل، فستتلقى بعد ذلك النظرة العامة التالية:



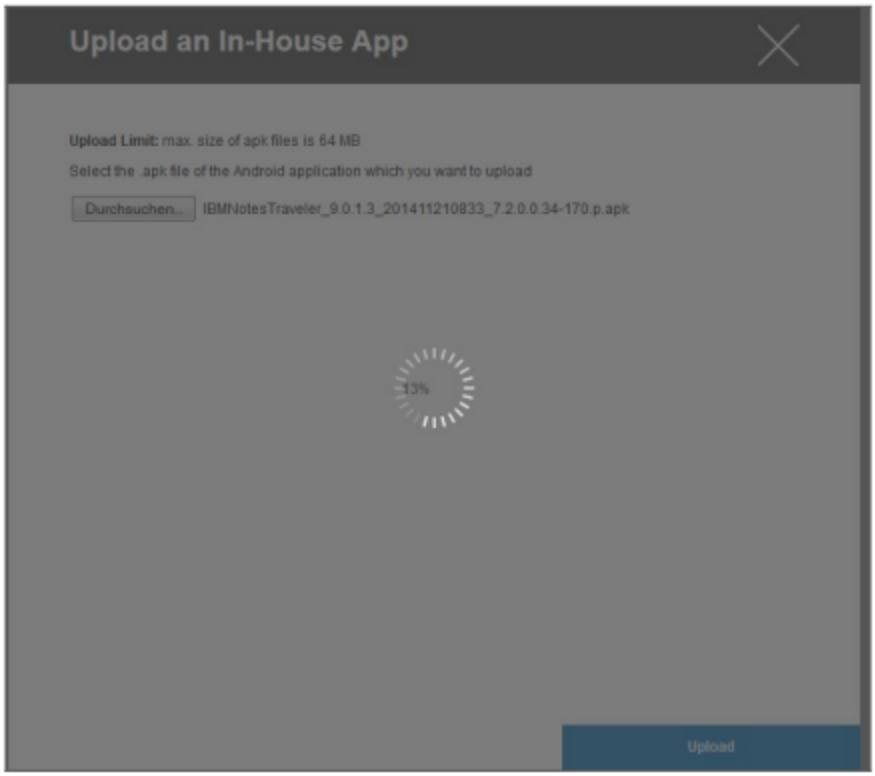
لهذا، انقر فوق "تحميل تطبيق داخلي"، وستتلقى بعد ذلك النظرة العامة التالية:



الآن، حدد باستخدام "بحث..." ملف .ipa ثم انقر على "تحميل"



سيتم الآن تحميل تطبيقك. في منتصف الدائرة، يمكنك رؤية النسبة المئوية لمقدار ما تم تحميله بالفعل من تطبيقك.



في حال تم تحميل التطبيق الداخلي بنجاح، سترى التطبيق الذي تم تحميله حديثاً في كتالوج التطبيقات.

يتوفر للمستخدم الآن خيار الاطلاع على هذا التطبيق وتثبيته في متجر AppTec360 على جهاز المستخدم النهائي، تحت فئة "في المنزل".

نظرًا لأن هذا لا يتضمن تطبيق Apple AppStore عام، فإن المستخدم لا يحتاج إلى معرف Apple مخزن على جهاز المستخدم النهائي.

وضع الكشك

يتوفر وضع كشك iOS في الوضع الخاضع للإشراف فقط

يسمح لك وضع الكشك بتحديد تطبيق أو عنوان URL مسبقًا، بحيث يمكن تشغيل/زيارة هذا التطبيق/عنوان URL حصريًا.

بالإضافة إلى ذلك، يمكنك إلغاء تنشيط العديد من أزرار الأجهزة في وضع الكشك.

نوع التطبيق

الحزمة

إذا كنت تريد تشغيل التطبيق في وضع الكشك، حدد "حزمة" ضمن "نوع التطبيق"

تطبيق الكشك	انقر هنا، لتحديد تطبيق يجب تشغيله في وضع الكشك ستجد النظرة العامة الحالية لإدارة التطبيقات يمكنك الاختيار بين "تطبيقات Apple iTunes Apps" و"تطبيقات iOS الداخلية"

عنوان URL

إذا كنت تريد تشغيل عنوان URL في وضع الكشك، حدد "عنوان URL" ضمن "نوع التطبيق"

عنوان URL	الآن، حدد عنوان URL المطلوب
سياسة نفس المنشأ	إذا كانت هذه الوظيفة نشطة، يمكن للمستخدم بعد ذلك تصفح الصفحات الفرعية لعنوان URL المحدد مسبقًا فقط على سبيل المثال، إذا قمت بتعريف عنوان URL التالي: www.mypage.com، ثم يمكن للمستخدم التصفح على www.mypage.com/subpage
عناوين URL المدرجة في القائمة البيضاء	هنا يمكنك الاحتفاظ بقائمة بيضاء، كل عناوين URL هذه مسموح بها 1 عنوان URL كحد أقصى لكل سطر يجب أن يبدأ عنوان URL ب http:/ أو https://
عناوين URL المدرجة في القائمة السوداء	هنا يمكنك الاحتفاظ بقائمة سوداء، كل عناوين URL هذه غير مسموح بها 1 عنوان URL كحد أقصى لكل سطر يجب أن يبدأ عنوان URL ب http:/ أو https://
مسح المتصفح بعد عدم النشاط	بعد عدم النشاط سيتم تفريغ ذاكرة التخزين المؤقت للمتصفح
تم تمكين كلمة مرور الخروج	إذا قمت بتفعيل هذه الوظيفة، يكون لدى المستخدم خيار إنهاء وضع الكشك بكلمة مرور تم تحديدها مسبقًا من قبلك
كلمة مرور الخروج	هذه هي كلمة المرور التي تم تحديدها مسبقاً من قبلك

إعدادات وضع الكشك

وضع الكشك المجدول	استنادًا إلى الوقت من اليوم، يمكنك ضبط وضع الكشك، بحيث يبدأ الوضع وينتهي تلقائيًا في الوقت الذي تم تحديده مسبقًا
وقت البدء	وقت البدء
الوقت بالدقائق	الوقت بالدقائق، وبعد ذلك ينبغي إنهاء وضع الكشك مرة أخرى
تعطيل اللمس	في حالة تنشيطها، يتم إلغاء تنشيط شاشة اللمس
تعطيل دوران الجهاز	في حالة تنشيطه، يتم إلغاء تنشيط التكييف التلقائي للشاشة
تعطيل مفتاح تبديل الرنين	إذا تم تنشيطه، سيتم بعد ذلك إلغاء تنشيط مفتاح الرنين. منذ ذلك الحين، يعتمد السلوك على الوظيفة التي تم تعيينها مسبقًا
تعطيل أزرار الصوت	إذا تم تنشيطها، سيتم إلغاء تنشيط أزرار مستوى الصوت
تعطيل زر الاستيقاظ أثناء النوم	في حالة تنشيطه، سيتم إلغاء تنشيط مفتاح التشغيل/إيقاف التشغيل
تعطيل القفل التلقائي	في حالة تنشيطه، لن يتم تحويل الجهاز إلى وضع الاستعداد
تمكين التعليق الصوتي	إذا تم تنشيطه، سيتم تفعيل المساعد الصوتي فوق الصوتي
تمكين التكبير/التصغير	في حالة تنشيطه، سيتم تفعيل التكبير/التصغير
تمكين عكس الألوان	في حالة تنشيطه، سيتم تنشيط وضع العرض المقلوب
تمكين اللمس المساعد	إذا تم تنشيطه، سيتم تنشيط AssistiveTouch
تمكين اختيار التحدث	في حالة تنشيطه، سيتم تنشيط تحديد الكلام
تمكين الصوت الأحادي	إذا تم تنشيطه، سيتم تنشيط الصوت الأحادي في حالة تنشيطه
تحويل صوتي	إذا تم تنشيطه، يمكن للمستخدم تمكين VoiceOver
تكبير/تصغير	في حالة تفعيلها، يمكن للمستخدم تمكين التكبير/التصغير
عكس الألوان	في حالة تفعيلها، يمكن للمستخدم تمكين الألوان المقلوبة
اللمس المساعد	إذا تم تنشيطه، يمكن للمستخدم تمكين اللمس المساعد في حالة تفعيله

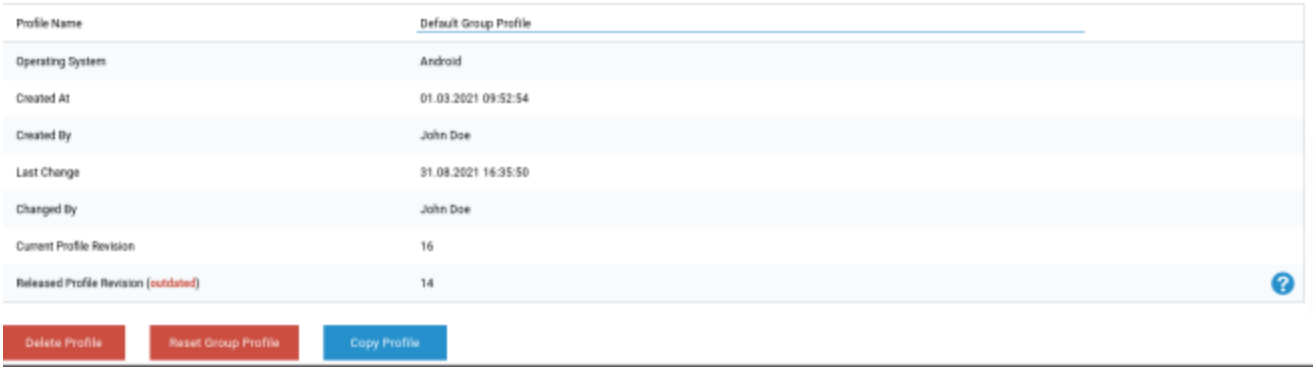
أندرويد إنتربرايز – تهيئة الأجهزة المدارة بالكامل

اعتمادًا على ما إذا كنت قد حددت حاليًا ملف تعريف مجموعة أو جهاز، تختلف النظرة العامة ونقاطها الفرعية - يرجى مراعاة ذلك بعناية!

جنرال لواء

نظرة عامة على ملف تعريف المجموعة (على مستوى المجموعة فقط)

عند فتح الملف الشخصي للمجموعة، ستحصل على نظرة عامة سريعة على الملف الشخصي.



اسم الملف الشخصي	اسم الملف الشخصي (يمكن تغييره هنا)
نظام التشغيل	نظام التشغيل الذي تم إنشاء ملف التعريف له
تم إنشاؤها في	وقت الإنشاء
تم إنشاؤها بواسطة	منشئ الملف الشخصي
آخر تغيير	وقت آخر تغيير في الملف الشخصي
تم التغيير بواسطة	الحساب الذي أجرى التغييرات الأخيرة
مراجعة الملف الشخصي الحالي	مراجعة حالة الملف الشخصي المحفوظة
مراجعة الملف الشخصي الصادر	مراجعة الملف الشخصي المعين ("تعيين الآن"). إذا كانت التسمية تظهر "(قديم)" خلف النص، فهذا يعني أنك قمت بحفظ ملف التعريف ولكنك لم تعيّنه بعد، لذا ستظل الأجهزة تحصل على الإصدار الأقدم.

نظرة عامة على الجهاز (على مستوى الجهاز فقط)

في حالة وجودك على أحد الأجهزة، ستتلقى ملخصاً عاماً للجهاز المحدد، ويتضمن ما يلي

اسم الجهاز	اسم الجهاز
الموقع	إحداثيات الموقع
رقم الهاتف	رقم الهاتف
التطبيقات الإلزامية المعينة	عدد التطبيقات الإلزامية المعينة
إصدار نظام التشغيل	إصدار نظام التشغيل الخاص بالجهاز
نظام التشغيل	نظام التشغيل (أندرويد إنتربرايز)
الرقم التسلسلي	الرقم التسلسلي للجهاز
ملكية الجهاز	جهاز الشركة أو الجهاز الخاص
نوع الجهاز	جهاز AE Work المُدار من قبل AE
متجذر	الحالة، التي تشير إلى ما إذا كان الجهاز قد تم تجذيره
متوافق	متوافق مع المبادئ التوجيهية
عنوان IP	عنوان IP الخاص بالجهاز
آخر ظهور	النقطة الزمنية، عندما كان الجهاز متصلاً بـ AppTec لآخر مرة
الدفعة الأخيرة	النقطة الزمنية، عندما تم إرسال آخر دفعة إلى الجهاز
وضع مالك جهاز AE	نعم
تعيين المستخدم	المستخدم أو المجموعة التي تم تعيين هذا الجهاز لها

مراجعة التكوين (على مستوى الجهاز فقط)

هنا تتلقى نظرة عامة على ملف تعريف المجموعة المعين للجهاز.

إذا نقرت على ملف تعريف المجموعة، ستحصل على وصول مباشر إلى ملف التعريف هذا ويمكنك إجراء الإعدادات.

باستخدام هذا الرمز، يمكنك إعادة التطبيقات الموزعة إلى إعدادات ملف تعريف المجموعة.

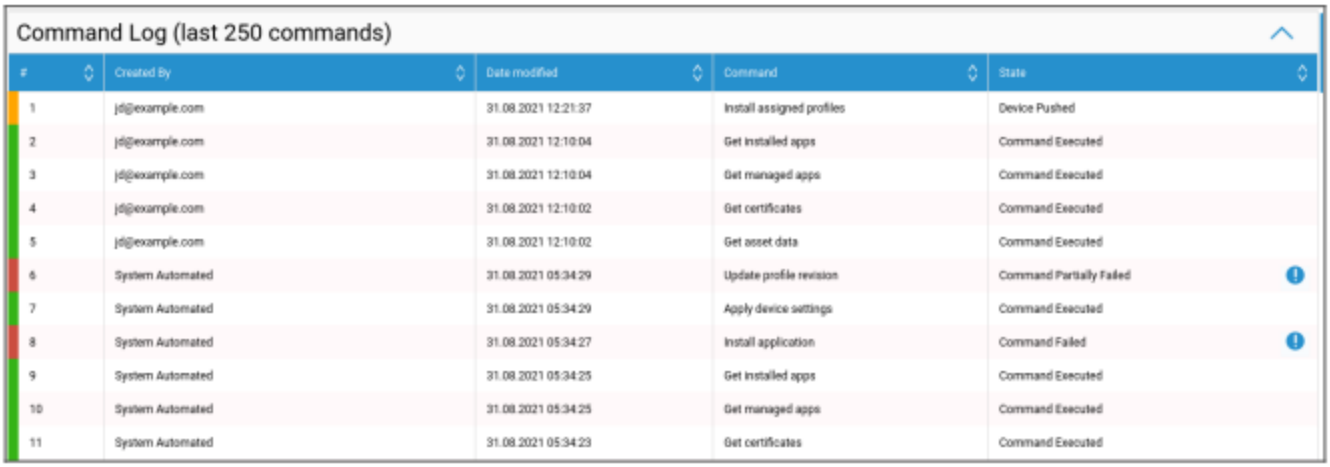
باستخدام هذا الرمز، يمكنك إعادة جميع التطبيقات المستخدمة إلى إعدادات ملف تعريف المجموعة.

تشير عبارة "تتوفر مراجعة أحدث" إلى أن ملف تعريف المجموعة قد تم تغييره وحفظه ولكن لم يتم تعيينه. يجب تعيين ملف تعريف المجموعة باستخدام "تعيين الآن" على مستوى المجموعة لتطبيق التغييرات على الأجهزة.

سجل الجهاز (على مستوى الجهاز فقط)

سجل الأوامر

هنا يمكنك معرفة الأوامر التي تم إصدارها للجهاز وما هي حالتها.



يتم إنشاء الأوامر التي تم إنشاؤها بواسطة "النظام الآلي" تلقائياً بواسطة النظام.

حالات الأوامر المحتملة

تم دفع الجهاز	تم إرسال طلب دفع إلى خدمة الدفع (مثل APNS) لإخبار الجهاز بالاتصال مرة أخرى بخادم EMM.
تم إنشاء الأمر	تم إنشاء الأمر في النظام.
تم إرسال الأمر	تم إرسال الأمر إلى الجهاز بعد اتصاله بالخادم.
تم تنفيذ الأمر	تم تنفيذ الأمر بنجاح.
فشل الأمر	فشل الأمر. *
فشل الأمر جزئياً	اعتمادًا على نظام تشغيل الجهاز قد يتم تجميع بعض الأوامر معًا. في هذا فشلت بعض أجزاء مجموعة الأوامر هذه. *
تم تنفيذ الأمر، وفشل الأمر في النهاية	تم تنفيذ الأمر ولكن ربما لم يتم تنفيذه.
إعادة دفع الأمر	تم إعادة دفع الأمر من قبل مستخدم.
مهملة	تم تجاهل الأمر. على سبيل المثال لأنه تم استبداله بأمر آخر أو تم إعادة تسجيل الجهاز وإزالة الأوامر القديمة

إذا كانت هناك علامة تعجب خلف الرسالة، فيمكنك الحصول على مزيد من المعلومات من خلال التمرير فوق الرمز بمؤشرك.

إعدادات الجهاز

تهيئة العميل

هنا يمكنك إجراء التكوينات التالية على جهاز Android الخاص بك:

وقت عدم الامتثال	مهلة استجابة المستخدم التي يتم بعدها تطبيق إجراء الإنفاذ.
إجراء الإنفاذ بعد انتهاء مهلة الامتثال	إجراء الإنفاذ عندما لا يقوم المستخدم بتنفيذ الإجراءات التي تؤدي إلى حالة جهاز متوافق
تواتر جمع البيانات	التواتر الذي سيتم به جمع معلومات الجهاز/النظام العالمي لتحديد المواقع
تردد نبضات قلب الجهاز	الفاصل الزمني الذي يجب أن يتصل فيه الجهاز بخادم AppTec360 دقيقة واحدة 1 دقيقة كحد أقصى. 24 ساعة
تمكين تحديثات الموقع	إذا تم تنشيطه، يرسل الجهاز تحديثات الموقع إلى خادم AppTec360
وقت تحديث الموقع	يحدد الفترات الزمنية التي يرسل فيها الجهاز تحديثات الموقع الجغرافي إلى AppTec360
استخدام دقة الموقع الجغرافي من Google لتحديث الموقع الجغرافي	إذا تم تنشيطه، فسيتم استخدام موقع الشبكة لتحديثات الموقع (إذا تم إلغاء تنشيطه ضمن "القيود"، فلن يؤثر هذا الإعداد على أي شيء)
استخدام موقع GPS لتحديث الموقع	في حالة تفعيله، سيتم استخدام GPS لتحديثات الموقع الجغرافي
السماح بالمواقع الوهمية (الوهمية)	السماح بتزوير معلومات الموقع الجغرافي عبر تطبيقات الطرف الثالث
إجراء فقدان الاتصال المفقود	في حالة التمكين، يمكنك تحديد إجراء في حالة عدم حصول الجهاز على اتصال بخادم MDM في الفاصل الزمني لنبض القلب. على سبيل المثال، إذا كان وقت نبض القلب للجهاز 5 دقائق، فإنه يتصل بالخادم في الساعة 10:35 صباحاً. بعد ذلك يغادر الجهاز نطاق Wi-Fi. سيفشل نبض القلب التالي في الساعة 10:40 صباحاً، وسيتم تنفيذ الإجراء المحدد.
الإجراء	الإجراء الذي يجب اتخاذه، بمجرد أن يصبح الجهاز غير متوافق. • جهاز القفل = جهاز القفل = جهاز القفل • مسح الجهاز = ستتم استعادة الجهاز إلى إعدادات المصنع • مسح الجهاز وبطاقة SD = ستتم استعادة الجهاز إلى إعدادات المصنع وسيتم حذف تخزين بطاقة SD

العتبة	يمكنك تحديد عتبة من نبضات القلب الفاشلة الضرورية لتشغيل الإجراء المحدد.

وضع إنفاذ السياسة	افتراضي:	ستتم مطالبة المستخدمين بشكل دوري بتنفيذ الإجراءات المعلقة
	تطبيق السياسات الكسولة	لن تتم مطالبة المستخدمين أبداً بتنفيذ الإجراءات المعلقة. سيتم عرض جميع الإجراءات المعلقة في عميل AppTec360
	إنفاذ السياسة الصارمة:	سيُطلب من المستخدمين دون توقف تنفيذ الإجراءات المعلقة
قفل إصدار AppTec360	في حالة التمكين، يمكن تحديد رمز إصدار لعميل AppTec360 MDM Client. سيتم تحديث عميل AppTec360 إلى الإصدار المحدد فقط. سيتم تجاهل الإصدارات الأحدث. لا يمكن إجراء ترقية إلى إصدار أقل.	
رمز الإصدار	كود الإصدار الخاص بعميل AppTec360 MDM المراد تأمينه عليه.	
تعطيل تنبيهات AppTec360	في حالة تعطيله لن يعرض عميل AppTec360 إشعاراً في شريط الإشعارات. وبالتالي يمكن للمستخدمين إغلاق عميل AppTec360 عبر مدير المهام. إذا تم إغلاق عميل AppTec360، فلن تعمل العديد من الميزات بما في ذلك وضع الكشك وقائمة التطبيقات السوداء/القائمة البيضاء بشكل صحيح. توفر أجهزة سامسونج آلية حماية لعميل AppTec360. يتم تعطيل الإشعار بشكل افتراضي على أجهزة Samsung التي تدعم واجهات برمجة تطبيقات KNOX. يجب عدم تعطيل الإشعار في الأجهزة التي تعمل بنظام Android 8.0 أو أعلى.	

ورق حائط

تعيين خلفية مخصصة	تمكين/تعطيل الخلفية المخصصة
ورق حائط	اضبط وضع الخلفية لاستخدام رمز لوني أو صورة
تحديد اللون	حدد لون الخلفية كقيمة سداسي عشري، على سبيل المثال #000000 للأسود أو #ffffffffff للأبيض
تعيين الصورة كخلفية	قم بتحميل ملف الصورة التي تريد استخدامها كخلفية

إدارة الأصول (على مستوى الجهاز فقط)

معلومات الجهاز

الطراز	تسمية طراز الجهاز
نظام التشغيل	نظام التشغيل
إصدار نظام التشغيل	إصدار نظام التشغيل
الرقم التسلسلي	الرقم التسلسلي
اسم الجهاز	اسم الجهاز
حالة البطارية	حالة البطارية
الذاكرة الحرة/إجمالي الذاكرة الحرة	الذاكرة الحرة/الإجمالية
خزنة سامسونج	واجهة Samsung SAFE، مطلوبة لمجموعة متنوعة من خيارات الإعدادات
بطاقة SD متوفرة	بطاقة SD متوفرة
مضاهاة بطاقة SD	محاكاة بطاقة SD
بطاقة SD قابلة للإزالة	بطاقة SD قابلة للإزالة
ذاكرة SD الحرة/إجمالي الذاكرة الحرة	ذاكرة بطاقة SD الحرة/إجمالي ذاكرة بطاقة SD الحرة

الواي فاي

عنوان IP	عنوان IP للجهاز
واي فاي ماك	عنوان MAC الواي فاي

خلوي

الحالة	الحالة (بطاقة SIM مثبتة)
رقم الهاتف	رقم الهاتف
التجوال (الصوت/البيانات)	التجوال للصوت/البيانات
حالة التجوال	حالة التجوال الحالية
عنوان IP	عنوان IP
المشغل/الناقل	المشغل/الناقل
التكنولوجيا الخلوية	التكنولوجيا الخلوية
IMEI	رقم IMEI
ICCID	هذا هو المعرف الخاص ببطاقة SIM، وغالبًا ما تكون أيضًا بطاقة ذكية أو بطاقة دائرة متكاملة (ICC)
IMSI	توفر الهوية الدولية للمشتركين في الهاتف المحمول (IMSI) في شبكات GSM وUMTS للهواتف المحمولة تعريفاً محدداً لمستخدمي الشبكة يتكون IMSI من 15 رقماً كحد أقصى ويتم تكوينه بالطريقة التالية: • رمز البلد المتنقل (MCC)، 3 أرقام • رمز شبكة الهاتف المحمول (MNC)، 2 أو 3 أرقام • رقم تعريف مشترك الهاتف المحمول (MSIN)، من 1-10 أرقام
MCC/ MNC الحالية	انظر "SIM MCC/MNC"
SIM MCC/MNC	رمز البلد المتنقل هو مُعرِّف قطري محدد، وضعه الاتحاد الدولي للاتصالات وفقاً للمعيار E.212. يعمل هذا بالاقتران مع رمز شبكة الهاتف المحمول (MNC) لتحديد هوية شبكة الهاتف المحمول. يعني رمز البلد/رمز شبكة الهاتف المحمول الخاص ببطاقة SIM. إذا كنت تقوم بالتجوال في شبكة جوال أخرى، فمن المنطقي أن يكون "MCC/ MNC الحالي" و "MCC/ MNC لشريحة SIM"، مختلفين.

بلوتوث

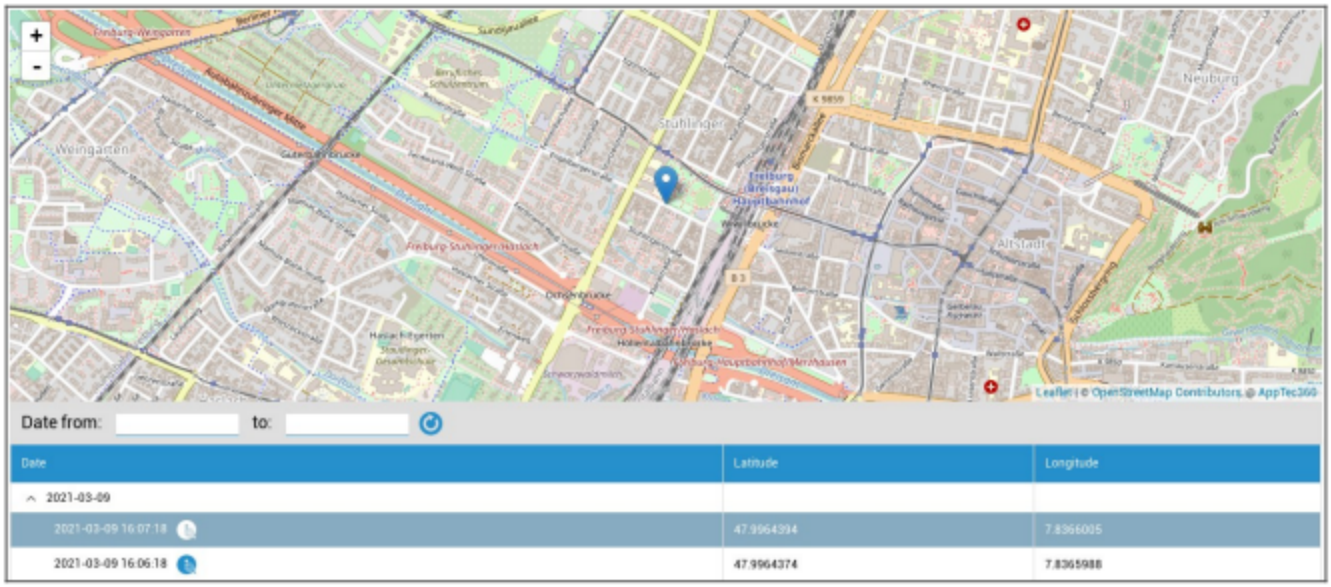
بلوتوث ماك	عنوان MAC للبلوتوث

إدارة الأمن

مكافحة السرقة (على مستوى الجهاز فقط)

معلومات GPS (على مستوى الجهاز فقط)

هنا يمكنك تحديد موقع الجهاز الحالي/الأخير. يمكن حماية تحديد الموقع باستخدام كلمة مرور واحدة أو حتى كلمتي مرور - انظر: الإعدادات العامة - الخصوصية - الوصول إلى نظام تحديد المواقع العالمي (GPS)



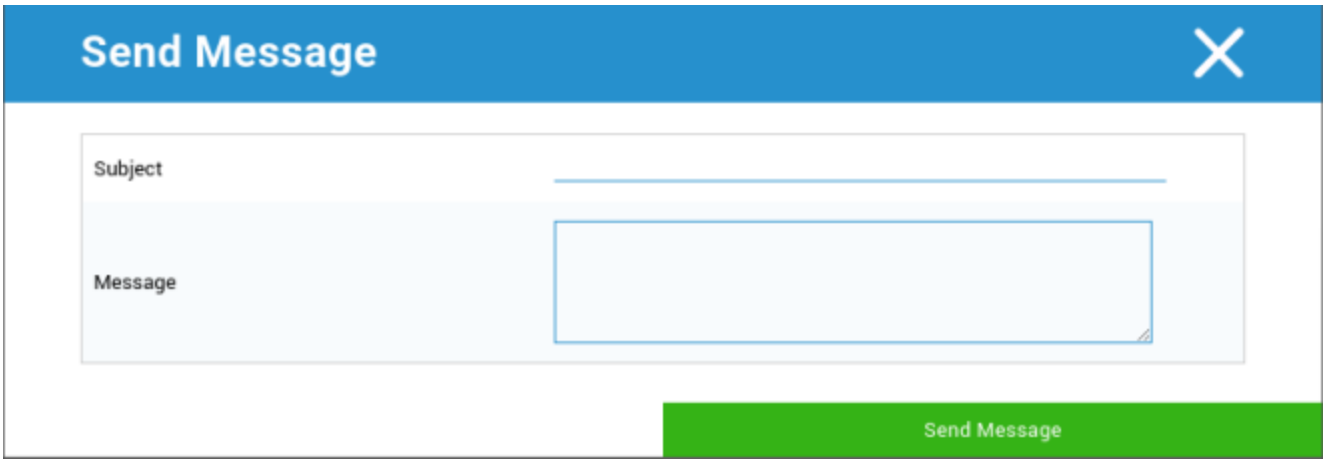
المسح والقفل (على مستوى الجهاز فقط)

ضمن "المسح والقفل"، يمكنك تنفيذ الإجراءات الثلاثة التالية:

مسح كامل	تتم استعادة الجهاز مرة أخرى إلى إعدادات المصنع (يتم حذف بيانات الشركة وكذلك البيانات الشخصية)
مسح المؤسسات	تتم إزالة بيانات الشركة فقط من جهاز المستخدم النهائي (جميع التطبيقات والبيانات وما إلى ذلك التي تم توفيرها بواسطة AppTec360)
قفل الشاشة	يتم تنشيط قفل الشاشة، ويكفي إلغاء قفل الجهاز باستخدام كلمة مرور الجهاز/رقم التعريف الشخصي

الرسالة (على مستوى الجهاز فقط)

هنا يمكنك ملء الموضوع والرسالة وإرسالها إلى جهاز المستخدم النهائي.



تهيئة الأمان

رمز مرور الجهاز

تحت "رمز المرور" يمكنك تفويض كلمة مرور الجهاز، وتتوفر لك خيارات الإعداد التالية

الحد الأدنى لطول كلمة المرور	ينشئ، الحد الأدنى لعدد الرموز التي يجب أن تحتويها كلمة المرور	
جودة كلمة المرور	غير محدد	لا تتضمن هذه السياسة أي متطلبات لكلمة المرور.
	البيومترية ضعيفة	تسمح هذه السياسة بتكنولوجيا التعرف البيومترية منخفضة الأمان. وهذا يعني التقنيات التي يمكن أن تتعرف على هوية الفرد إلى حوالي 3 أرقام من رقم التعريف الشخصي (الكشف الخاطئ أقل من 1 من كل 1000).
	شيء ما	تتطلب هذه السياسة تعيين نوع من كلمة المرور أو النمط الذي يجب تعيينه، ولكنها لا تفرض أي قواعد محددة.
	حروف الهجاء	يجب أن يكون المستخدم قد أدخل كلمة مرور تحتوي على الأقل على أحرف أبجدية (أو رموز أخرى).
	أبجدي رقمي	يجب أن يكون المستخدم قد أدخل كلمة مرور تحتوي على الأقل على كل من الأحرف الرقمية والأبجدية (أو رموز أخرى).
	مجمع	يجب أن يكون المستخدم قد أدخل كلمة مرور تحتوي على الأقل على حرف ورقم عددي ورمز خاص، بشكل افتراضي. باستخدام هذه النوعية من كلمات المرور، يمكن تقييد كلمات المرور بحيث تحتوي على مجموعات مختلفة من الأحرف، مثل حرف كبير على الأقل، إلخ.
الحد الأدنى لطول كلمة المرور	قم بتعيين عدد الأحرف المطلوبة لكلمة المرور. على سبيل المثال، يمكنك أن تطلب أن يكون رقم التعريف الشخصي أو كلمات المرور ستة أحرف على الأقل.	
الحد الأدنى من الأرقام العددية المطلوبة في كلمة المرور	الحد الأدنى من الأرقام العددية المطلوبة في كلمة المرور	
الحد الأدنى من الأحرف الصغيرة المطلوبة في كلمة المرور	الحد الأدنى من الأحرف الصغيرة المطلوبة في كلمة المرور	
الحد الأدنى من الأحرف الكبيرة المطلوبة في كلمة المرور	الحد الأدنى من الأحرف الكبيرة المطلوبة في كلمة المرور	
الحد الأدنى من الأحرف غير	الحد الأدنى من الأحرف غير الأحرف المطلوبة في كلمة المرور	

المطلوبة في كلمة المرور	
الحد الأدنى من الرموز المطلوبة في كلمة المرور	الحد الأدنى من الرموز المطلوبة في كلمة المرور

الحد الأقصى لقفل وقت عدم النشاط	الحد الأقصى لعدم نشاط المستخدم حتى قفل الوقت
مهلة انتهاء صلاحية كلمة المرور	ينشأ، وبعد هذه الفترة الزمنية تنتهي صلاحية كلمة المرور ويجب إصدار كلمة مرور جديدة
تقييد سجل كلمات المرور	عدد كلمات المرور المستخدمة سابقاً غير المسموح بها
الحد الأقصى لمحاولات كلمة المرور الفاشلة	يحدد، كم مرة يمكن إدخال كلمة مرور بشكل غير صحيح، قبل أن يتم إجراء مسح كامل للجهاز
السماح بالمصادقة البيومترية	تمكين المصادقة عبر بصمة الإصبع أو مسح قزحية العين. فقط لنظام Samsung KNOX 2.1 والإصدارات الأحدث

مضاد الفيروسات

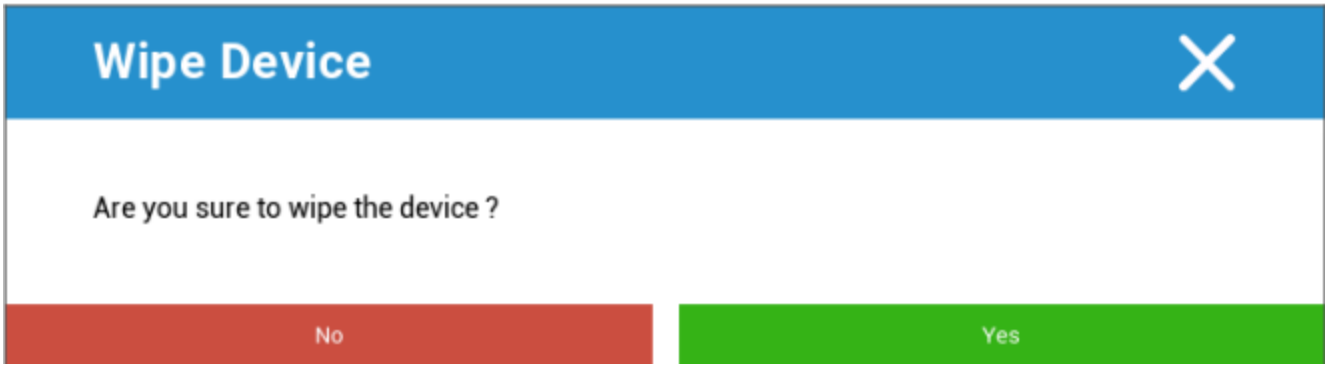
المسح التلقائي	تمكين عمليات الفحص التلقائي الدورية
فترة المسح الضوئي	الفترة الفاصلة للفحص (سريع / كامل)
المسح التلقائي الكامل	تمكين الفحص التلقائي الكامل
التحديثات التلقائية	تمكين التحديثات التلقائية
تحديث فترة التحقق من التحديث	كم مرة يجب تحديث التطبيق وقاعدة البيانات الخاصة به (الفيروسات / التعليمات البرمجية التالفة)
حماية التطبيق	تمكين الفحص التلقائي للتطبيق
حماية بطاقة SD	تمكين الفحص التلقائي لبطاقة SD
تحديث Wi-Fi فقط	عند التمكين، لن يتم تطبيق التحديثات إلا عند اتصال الجهاز بشبكة Wi-Fi بنجاح

نهاية العمر الافتراضي (على مستوى الجهاز فقط)

المسح (على مستوى الجهاز فقط)

ضمن "مسح"، يمكنك استعادة الجهاز إلى إعدادات المصنع. هنا سيتم حذف بيانات الشركة وكذلك البيانات الخاصة على جهاز المستخدم النهائي.

بالنقر على "رمز الطرح" تتلقى الرسالة التالية:



باستخدام "نعم" يمكنك إجراء المسح.

تحت عنوان "تقرير المسح" يمكن عرض العناصر التالية

ممسوح بواسطة	تاريخ من قام بالمسح
التاريخ	التاريخ
الحالة	الحالة (على سبيل المثال، إذا تم إجراء المسح بنجاح)

إعدادات التقييد

القيود

هنا، يمكن تقييد وحظر مجموعة متنوعة من الأشياء.

تمكين الكاميرا	السماح باستخدام الكاميرا	
فرض المزامنة التلقائية	على	يتم تنشيط المزامنة بشكل دائم
	إيقاف التشغيل	يتم إلغاء تنشيط المزامنة بشكل دائم
	اختيار المستخدم	تم تحديده من قبل المستخدم
قوة البلوتوث	على	يتم تنشيط البلوتوث بشكل دائم
	إيقاف التشغيل	تم إلغاء تنشيط البلوتوث بشكل دائم
	اختيار المستخدم	تم تحديده من قبل المستخدم
قوة نظام تحديد المواقع العالمي (GPS)	على	يتم تنشيط GPS بشكل دائم
	إيقاف التشغيل	تم إلغاء تنشيط GPS بشكل دائم
	اختيار المستخدم	تم تحديده من قبل المستخدم
موقع شبكة القوة	على	توطين الإنترنت الدائم
	إيقاف التشغيل	التعطيل الدائم لتوطين الإنترنت بشكل دائم
	اختيار المستخدم	تم تحديده من قبل المستخدم

الأمن		
عدم السماح بموقع المشاركة	يحدد ما إذا كان المستخدم غير مسموح له بتشغيل مشاركة الموقع.	
تعطيل التمهيد الآمن	يحدد ما إذا كان المستخدم غير مسموح له بإعادة تشغيل الجهاز في وضع التمهيد الآمن.	
عدم السماح بإعادة تعيين الشبكة	يحدد ما إذا كان المستخدم غير مسموح له بإعادة تعيين إعدادات الشبكة من الإعدادات.	
عدم السماح بإعادة ضبط المصنع	يحدد ما إذا كان المستخدم غير مسموح له بإعادة ضبط الجهاز.	
تمكين بنك التنمية الآسيوي	يسمح بالاتصال بجهاز كمبيوتر شخصي عبر ADB	
تعطيل حماية المفاتيح	تعطيل برنامج حماية المفاتيح	
معلومات شاشة قفل مالك الجهاز	يضبط معلومات مالك الجهاز لتظهر على شاشة القفل.	
إنفاذ الامتثال	وضع موجه المستخدم	سيُطلب من المستخدم تنفيذ الإجراءات اللازمة.
	حاوية إقفال الحاوية	إخفاء جميع التطبيقات حتى يتم استيفاء جميع المتطلبات

إدارة التطبيقات	
السماح بالربط بين تطبيقات الملفات الشخصية	السماح للتطبيقات في ملف التعريف الأصلي بمعالجة روابط الويب من ملف التعريف المُدار.
عدم السماح بالتحكم في التطبيق	يحدد ما إذا كان المستخدم غير مسموح له بتعديل التطبيقات في الإعدادات أو المشغلات.
عدم السماح بتثبيت التطبيق	يحدد ما إذا كان المستخدم غير مسموح له بتثبيت التطبيقات.
تعطيل إلغاء تثبيت التطبيقات	يحدد ما إذا كان المستخدم غير مسموح له بإلغاء تثبيت التطبيقات.
سياسة إذن وقت التشغيل	يحدد كيفية التعامل مع طلبات الأذونات الجديدة من التطبيقات.
السماح بمصادر غير معروفة	في حالة التمكين، يمكن للمستخدمين تحميل التطبيقات بشكل جانبي عن طريق تثبيت ملف .apk.

الاتصال	
عدم السماح بتكوين شبكة الجوال	يحدد ما إذا كان المستخدم غير مسموح له بتكوين شبكات الهاتف المحمول.
عدم السماح بتكوين الربط	يُحدد ما إذا كان المستخدم غير مسموح له بتكوين نقاط الاتصال والنقاط الساخنة المحمولة.
عدم السماح بتكوين VPN	يحدد ما إذا كان المستخدم غير مسموح له بتكوين شبكة VPN.
عدم السماح بتكوين Wifi	يحدد ما إذا كان المستخدم غير مسموح له بتغيير نقاط وصول WiFi.
عدم السماح بشعاع NFC الصادر	يحدد ما إذا كان المستخدم غير مسموح له باستخدام NFC لإرسال البيانات من التطبيقات.
تكوين قفل الواي فاي القفل	يتحكم هذا الإعداد في ما إذا كان ينبغي تأمين تكوينات WiFi التي تم إنشاؤها بواسطة تطبيق مالك الجهاز (أي أن تكون قابلة للتحرير أو الإزالة فقط من قبل تطبيق مالك الجهاز، وليس حتى من قبل تطبيق الإعدادات).
تمكين تجوال البيانات	تنشيط تجوال البيانات

بلوتوث	
عدم السماح بالبلوتوث	يحدد ما إذا كان البلوتوث غير مسموح به على الجهاز. يتطلب أندرويد 8.0
عدم السماح بمشاركة البلوتوث	يحدد ما إذا كانت مشاركة البلوتوث الصادرة غير مسموح بها على الجهاز. يتطلب أندرويد 8.0
عدم السماح بتكوين البلوتوث	يحدد ما إذا كان المستخدم غير مسموح له بتكوين البلوتوث.

إدارة الحسابات	
عدم السماح بإضافة ملف تعريف مُدار	يحدد ما إذا كان المستخدم غير مسموح له بإضافة ملفات تعريف مُدارة. يتطلب أندرويد 8.0
عدم السماح بإضافة مستخدمين	يحدد ما إذا كان المستخدم غير مسموح له بإضافة مستخدمين جدد.
عدم السماح بإزالة ملف التعريف المُدار	يحدد ما إذا كان يمكن إزالة ملفات التعريف المدارة لهذا المستخدم، بخلاف مالك ملف التعريف الخاص به. يتطلب أندرويد 8.0
عدم السماح بتعديل الحساب	يحدد ما إذا كان المستخدم غير مسموح له بإضافة حسابات وإزالتها، ما لم تتم إضافتها برمجيًا بواسطة المصادقة.

الاتصالات الهاتفية	
عدم السماح بالمكالمات الصادرة	يحدد عدم السماح للمستخدم بإجراء مكالمات هاتفية صادرة.
عدم السماح بالرسائل النصية القصيرة	يحدد أن المستخدم غير مسموح له بإرسال أو استقبال الرسائل النصية القصيرة.

النظام	
عدم السماح بإنشاء النوافذ	يحدد أنه لا ينبغي إنشاء نوافذ غير نوافذ التطبيق.
عدم السماح بتعيين أيقونة المستخدم	يحدد ما إذا كان المستخدم غير مسموح له بتغيير الرمز الخاص به.
عدم السماح بتعيين الخلفية	تقييد المستخدم لعدم السماح بتعيين خلفية.
تعطيل شريط الحالة	يؤدي تعطيل شريط الحالة إلى حظر الإشعارات والإعدادات السريعة وتراكبات الشاشة الأخرى التي تسمح بالهروب من جهاز يستخدم مرة واحدة.
تمكين الوقت التلقائي	يضبط الوقت تلقائياً.
تمكين المنطقة الزمنية التلقائية	يضبط المنطقة الزمنية تلقائياً.
البقاء قيد التشغيل أثناء التوصيل بالكهرباء	سيبقى الجهاز نشطاً أثناء توصيله بمصدر طاقة.

التخزين	
تعطيل تعطيل التحقق من التطبيق	يحدد ما إذا كان المستخدم غير مسموح له بتعطيل التحقق من التطبيق.
عدم السماح بتركيب الوسائط المادية	يحدد ما إذا كان المستخدم غير مسموح له بتركيب وسائط خارجية فعلية.
تمكين خدمة النسخ الاحتياطي	تدير خدمة النسخ الاحتياطي جميع آليات النسخ الاحتياطي والاستعادة على الجهاز. سيؤدي تعيين هذا إلى خطأ إلى منع النسخ الاحتياطي للبيانات أو استعادتها. يتم إيقاف تشغيل خدمة النسخ الاحتياطي بشكل افتراضي. يتطلب أندرويد 8.0
تمكين وحدة تخزين USB للتخزين الشامل	تمكين استخدام وحدة التخزين الشامل USB.

لوحة المفاتيح	
عدم السماح بالملء التلقائي	يحدد ما إذا كان المستخدم غير مسموح له باستخدام خدمات الملء التلقائي. يتطلب أندرويد 8.0
عدم السماح بالنسخ واللصق بين الملفات الشخصية	يحدد ما إذا كان يمكن لصق ما تم نسخه في حافظة ملف التعريف هذا في ملفات التعريف ذات الصلة.

الصوت	
عدم السماح بتعديل الحجم	يحدد ما إذا كان المستخدم غير مسموح له بتعديل مستوى الصوت الرئيسي.
تعطيل إلغاء كتم صوت الميكروفون	يحدد ما إذا كان المستخدم غير مسموح له بضبط مستوى صوت الميكروفون.
جهاز كتم الصوت	جهاز كتم الصوت.

إدارة الشهادات

هنا يمكنك توزيع الشهادات الموثوقة وشهادات الهوية على أجهزتك.

مطلوب Android 8 أو أعلى لتوزيع الشهادات الموثوقة و Android 9 أو أعلى لتوزيع شهادات الهوية.

باستخدام "+" يمكنك إضافة شهادات متعددة.

يجب أن تكون الشهادات الموثوقة بتنسيق PEM.

يجب أن تكون شهادات الهوية بتنسيق PKCS12

إدارة الاتصال

الواي فاي

بالنسبة لهذا الإعداد، قم بإجراء التهيئة المسبقة لأجهزة المستخدم النهائي، للوصول إلى نقاط الوصول الداخلية

معرّف مجموعة الخدمات (SSID)	SSID للشبكة التي سيتم الاتصال بها
الشبكة الخفية	تنشيط، في حالة عدم قيام نقطة الوصول إلى نقطة الوصول ببث SSID

نوع الأمان

إنشاء نوع أمان نقطة الوصول

WEP

كلمة المرور	كلمة المرور الخاصة بـ AP

WPA/WPA2

كلمة المرور	كلمة المرور الخاصة بـ AP

802.1x EAP 802.1x

طريقة EAP-Method

الأشخاص ذوو الإعاقة	الهوية	الهوية
	كلمة المرور	كلمة المرور

PEAP	بروتوكول المصادقة في المرحلة 2	لا شيء	لا يوجد بروتوكول إضافي
		MSCHAPV2	بروتوكول MSCHAPV2
		GTC	بروتوكول GTC
	شهادة المرجع المصدق (CA)	شهادة المرجع المصدق (CA)	
	الهوية	الهوية	
	هوية مجهولة	هوية مجهولة	
	كلمة المرور	كلمة المرور	

TTLS	بروتوكول المصادقة في المرحلة 2	لا شيء	لا يوجد بروتوكول إضافي
		برنامج مساعدة الشعب الفلسطيني	بروتوكول PAP
		MSCHAP	بروتوكول MSCHAP
		MSCHAPV2	بروتوكول MSCHAPV2
		GTC	بروتوكول GTC
	شهادة المرجع المصدق (CA)	شهادة المرجع المصدق (CA)	
	الهوية	الهوية	
	هوية مجهولة	هوية مجهولة	
	كلمة المرور	كلمة المرور	

TLS	شهادة المرجع المصدق (CA)	شهادة المرجع المصدق (CA)
	الهوية	الهوية
	كلمة المرور	كلمة المرور

VPN

اسم الاتصال	اسم اتصال VPN

نوع VPN

VPN

عميل VPN

عميل VPN AppTec360	
تكوين البوابة	حدد تكوين الشبكة الخاصة الافتراضية للبوابة (انظر **الإعدادات العامة > البوابة العامة > إعدادات الشبكة الخاصة الافتراضية**)
دائماً على VPN	تمكين الإغلاق الأصلي
تمكين تأمين AppTec360 AppTec360	تمكين تأمين AppTec360 AppTec360

مدمج (متوفر فقط على أجهزة سامسونج)			
نوع الاتصال	PPTP	الخادم	الخادم
		تمكين تشفير PPTP PPTP	تمكين تشفير PPTP PPTP
	L2TP / IPSec PSK	الخادم	الخادم
		المفتاح المشترك المسبق IPSec	المفتاح المشترك المسبق IPSec
		تمكين L2TP سري L2TP	تمكين L2TP سري L2TP
		L2TP سري L2TP	L2TP سري L2TP
	IPSec XAuth PSK	الخادم	الخادم
		معرّف IPSec	معرّف IPSec
		المفتاح المشترك المسبق IPSec	المفتاح المشترك المسبق IPSec
نطاقات بحث DNS	نطاقات بحث DNS		
إعدادات الخبراء	خوادم DNS	خوادم DNS	
	مسارات إعادة التوجيه	مسارات إعادة التوجيه	

فتح VPN			
الخادم	الخادم		
ملف تعريف OpenVPN	ملف تعريف OpenVPN		
تطبيق OpenVPN	OpenVPN للأندرويد (موصى به)		
	اتصال OpenVPN		
إعدادات الخبراء	خوادم DNS	خوادم DNS	
	مسارات إعادة التوجيه	مسارات إعادة التوجيه	

سامسونج / سترونج سوان			
نوع الاتصال	PPTP	الخادم	الخادم
		اسم المستخدم	اسم المستخدم
		كلمة المرور	كلمة المرور
		تمكين تشفير PPTP PPTP	تمكين تشفير PPTP PPTP
	L2TP / IPSec PSK	الخادم	الخادم
		المفتاح المشترك المسبق IPSec	المفتاح المشترك المسبق IPSec
		اسم المستخدم	اسم المستخدم
		كلمة المرور	كلمة المرور
		تمكين L2TP سري L2TP	L2TP سري L2TP
	IPSec XAuth PSK	الخادم	الخادم
		معرّف IPSec	معرّف IPSec
		المفتاح المشترك المسبق IPSec	المفتاح المشترك المسبق IPSec
		اسم المستخدم	اسم المستخدم
		كلمة المرور	كلمة المرور
إعدادات الخبراء	خوادم DNS	خوادم DNS	
	مسارات إعادة التوجيه	مسارات إعادة التوجيه	

Cisco Any Connect من Cisco Any Connect		
الخادم	الخادم	
وضع الشهادة	معاق	معاق
	أوتوماتيكي	أوتوماتيكي
إعدادات الخبراء	خوادم DNS	خوادم DNS
	مسارات إعادة التوجيه	مسارات إعادة التوجيه

لكل تطبيق VPN

عميل VPN

عميل AppTec360 VPN		
تكوين البوابة	حدد تكوين الشبكة الخاصة الافتراضية للبوابة (انظر **الإعدادات العامة > البوابة العامة > إعدادات الشبكة الخاصة الافتراضية**)	
تطبيقات VPN	تطبيقات VPN	
دائماً على VPN	تمكين الإغلاق الأصلي	دائماً على VPN
تمكين تأمين AppTec360 AppTec360	تمكين تأمين AppTec360 AppTec360	

سامسونج / سترونج سوان			
نوع الاتصال	PPTP	الخادم	الخادم
		تطبيقات VPN	تطبيقات VPN
		اسم المستخدم	اسم المستخدم
		كلمة المرور	كلمة المرور
		تمكين تشفير PPTP PPTP	تمكين تشفير PPTP PPTP
	L2TP / IPSec PSK	الخادم	الخادم
		تطبيقات VPN	تطبيقات VPN
		المفتاح المشترك المسبق IPSec	المفتاح المشترك المسبق IPSec
		اسم المستخدم	اسم المستخدم
		كلمة المرور	كلمة المرور
		تمكين L2TP سري L2TP	L2TP سري L2TP
	IPSec XAuth PSK	الخادم	الخادم
		تطبيقات VPN	تطبيقات VPN
		معرّف IPSec	معرّف IPSec
		المفتاح المشترك المسبق IPSec	المفتاح المشترك المسبق IPSec
		اسم المستخدم	اسم المستخدم
		كلمة المرور	كلمة المرور
إعدادات الخبراء	خوادم DNS	خوادم DNS	
	مسارات إعادة التوجيه	مسارات إعادة التوجيه	

القيود

هنا يمكنك تعيين القيود، فيما يتعلق بإدارة الاتصال.

السماح بتجوال البيانات	السماح ببيانات الجوال أثناء التجوال
فرض تجوال البيانات	إذا تم تفعيله، يتم تفعيل التجوال لبيانات الهاتف المحمول بشكل دائم (غير مستحسن!) يحل هذا الإعداد محل إعداد "السماح بتجوال البيانات"!
الإعدادات التالية متوفرة فقط على SAFE 2.x أو أعلى	
السماح بمكالمات الطوارئ فقط	السماح بمكالمات الطوارئ فقط
السماح بالواي فاي	السماح بالواي فاي
الحد الأدنى لمستوى أمان شبكة WiFi	الحد الأدنى لمستوى أمان شبكة WiFi مفتوح = يُسمح باستخدام جميع أنواع الواي فاي
منع المستخدم من إضافة شبكات WiFi	لا يجوز للمستخدم إضافة شبكة WiFi بنفسه هذا الإعداد ممكن فقط، إذا تم تعريف ملف تعريف WiFi ضمن "إدارة الاتصال"
السماح بالرسائل النصية القصيرة ورسائل الوسائط المتعددة	الكل = كل حركة مرور الرسائل النصية القصيرة ورسائل الوسائط المتعددة مسموح بها الرسائل النصية الواردة فقط = يُسمح فقط بالرسائل النصية الواردة فقط الرسائل القصيرة الصادرة فقط = يُسمح بالرسائل القصيرة الصادرة فقط لا يوجد = غير مسموح بنقل الرسائل النصية القصيرة/رسائل الوسائط المتعددة
السماح بالمزامنة أثناء التجوال	السماح بالمزامنة أثناء التجوال قيد التشغيل = مفعل مطفأة = معطلة = معطلة اختيار المستخدم = اختيار المستخدم
السماح بالتجوال الصوتي	السماح بالتجوال الصوتي قيد التشغيل = مفعل مطفأة = معطلة = معطلة اختيار المستخدم = اختيار المستخدم
استخدام النظام خادم وكيل http النظام البروكسي	يعتمد استخدام خادم وكيل HTTP، الذي توفره إعدادات النظام في الإعدادات، على الشبكة المتصلة (WiFi أو APN)

إدارة PIM

Gmail Exchange

معلومات: سيتم تطبيق هذا التكوين على تطبيق Gmail. لذا عليك الموافقة على Gmail وتثبيته.

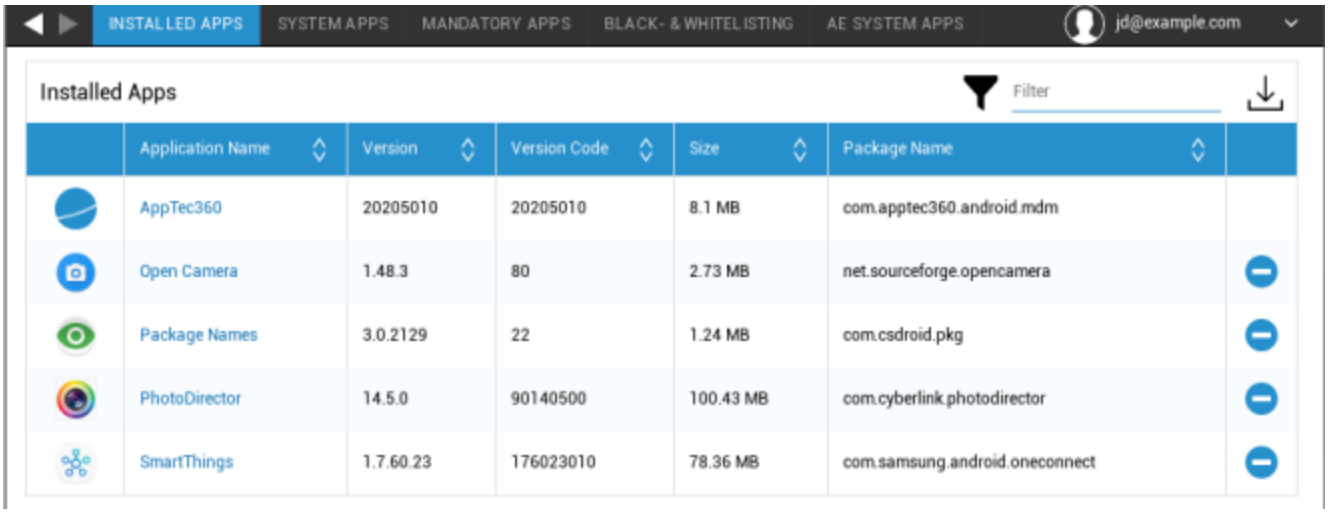
عنوان البريد الإلكتروني	عنوان البريد الإلكتروني للمستخدم المقدم يرجى ملاحظة "العناصر النائبة"، التي يمكنك استخدامها للعمل مع بيانات الاعتماد ولا تقوم بإجراء تغييرات يدوياً على كل جهاز بنقرة واحدة على يمكنك عرضها بنفسك
اسم مضيف الخادم	عنوان الخادم الخاص بخوادم Exchange الخاصة بك
اسم تسجيل الدخول	اسم تسجيل الدخول لجهاز المستخدم النهائي المعني، يرجى أيضًا ملاحظة "العناصر النائبة هنا
التوقيع	يمكن إرفاق توقيع (تلميح: تتطلب بعض الأجهزة تنسيق HTML للتوقيع)
عدد الأيام السابقة للمزامنة	عدد الأيام التي يتم فيها تحديد موعد مزامنة رسائل البريد الإلكتروني
معرّف الجهاز	سلسلة EAS DeviceID التي يتضمنها EAS DeviceID. هذه السلسلة هي جزء من بروتوكولات EAS وتوجد في بعض الأقاليم الأصلية
استخدام طبقة مآخذ التوصيل الآمنة (SSL)	استخدام اتصال SSL
قبول جميع الشهادات	جميع الشهادات مقبولة. الرجاء تحديد هذا الخيار، إذا كان خادم Exchange لديك يستخدم شهادة موقعة ذاتياً

إدارة التطبيقات

مدير تطبيقات المؤسسات

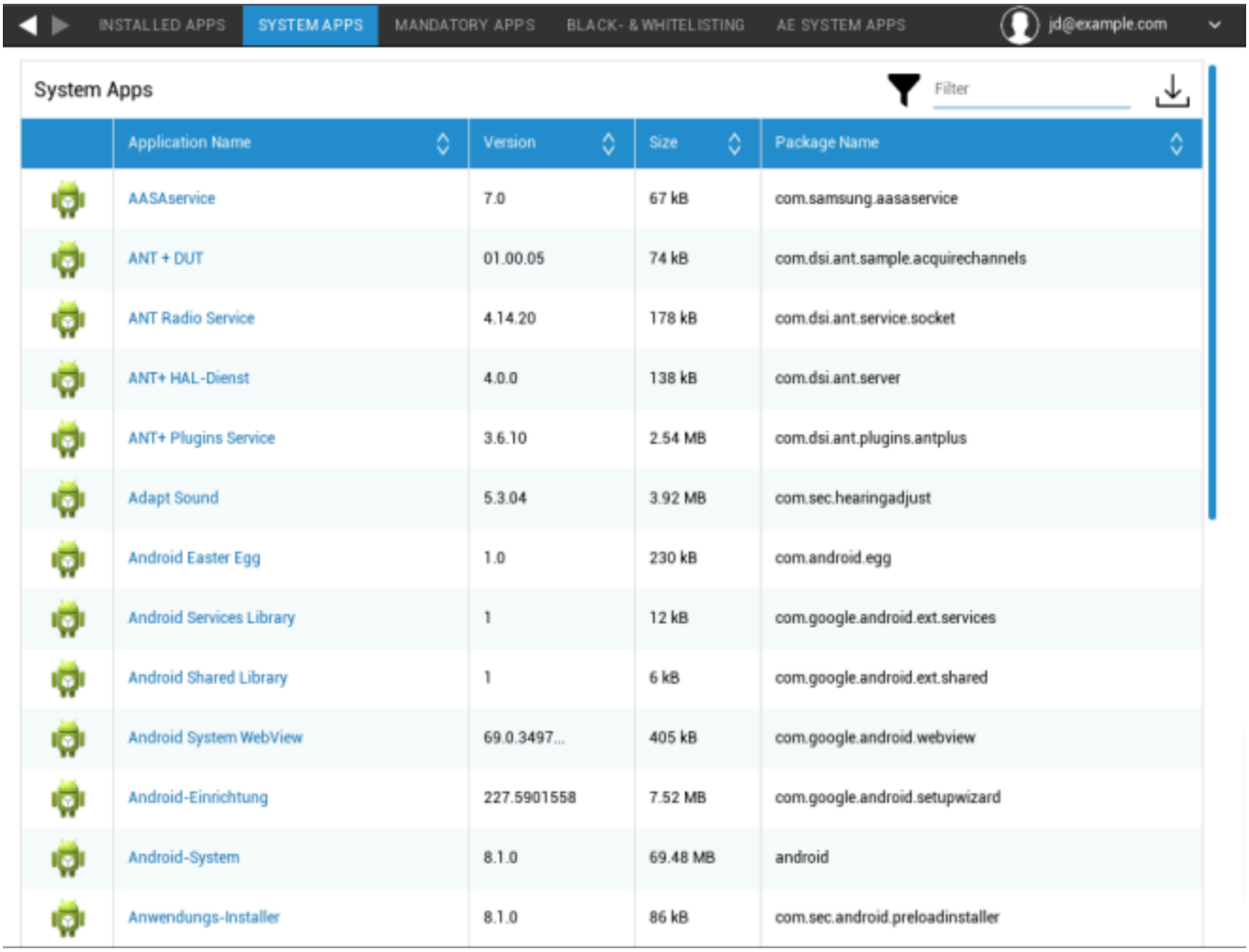
التطبيقات المثبتة (على مستوى الجهاز فقط)

هنا سيتم عرض جميع التطبيقات المثبتة حاليًا على جهاز المستخدم النهائي لك.



تطبيقات النظام (على مستوى الجهاز فقط)

تحت عنوان "تطبيقات النظام"، سيتم إدراج جميع التطبيقات والخدمات التي تم تثبيتها بالفعل على جهاز المستخدم النهائي من قبل الشركة المصنعة للجهاز.

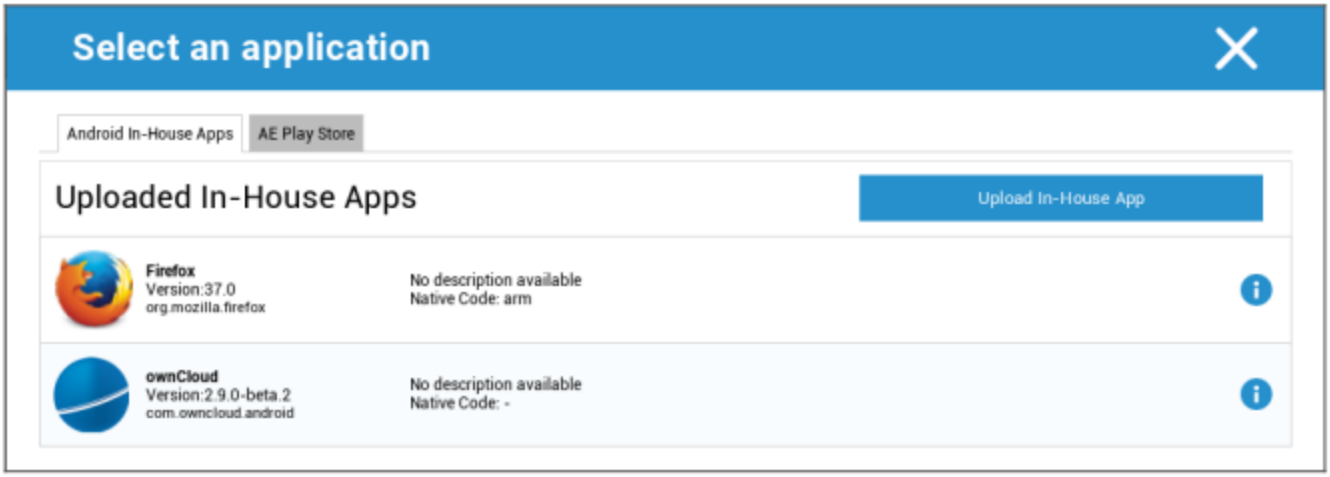


التطبيقات الإلزامية

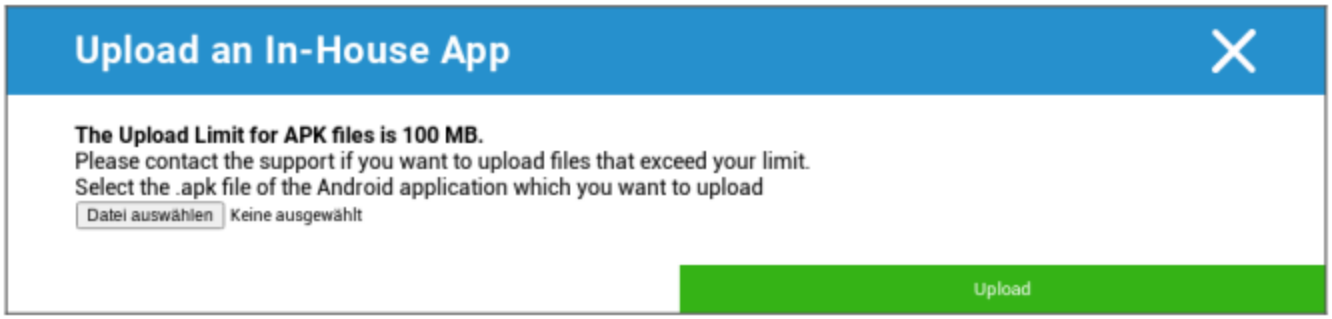
ضمن التطبيقات الإلزامية، يمكنك إنشاء التطبيقات المطلوبة الإلزامية. سيُطلب من المستخدم باستمرار تثبيت هذا التطبيق المعين.

من خلال، يمكن تعريف التطبيق المطلوب الإلزامي المطلوب.

يمكن أن يكون هذا تطبيقًا داخليًا من "تطبيقات Android الداخلية"، والتي قمت بتحميلها في الإعدادات العامة.

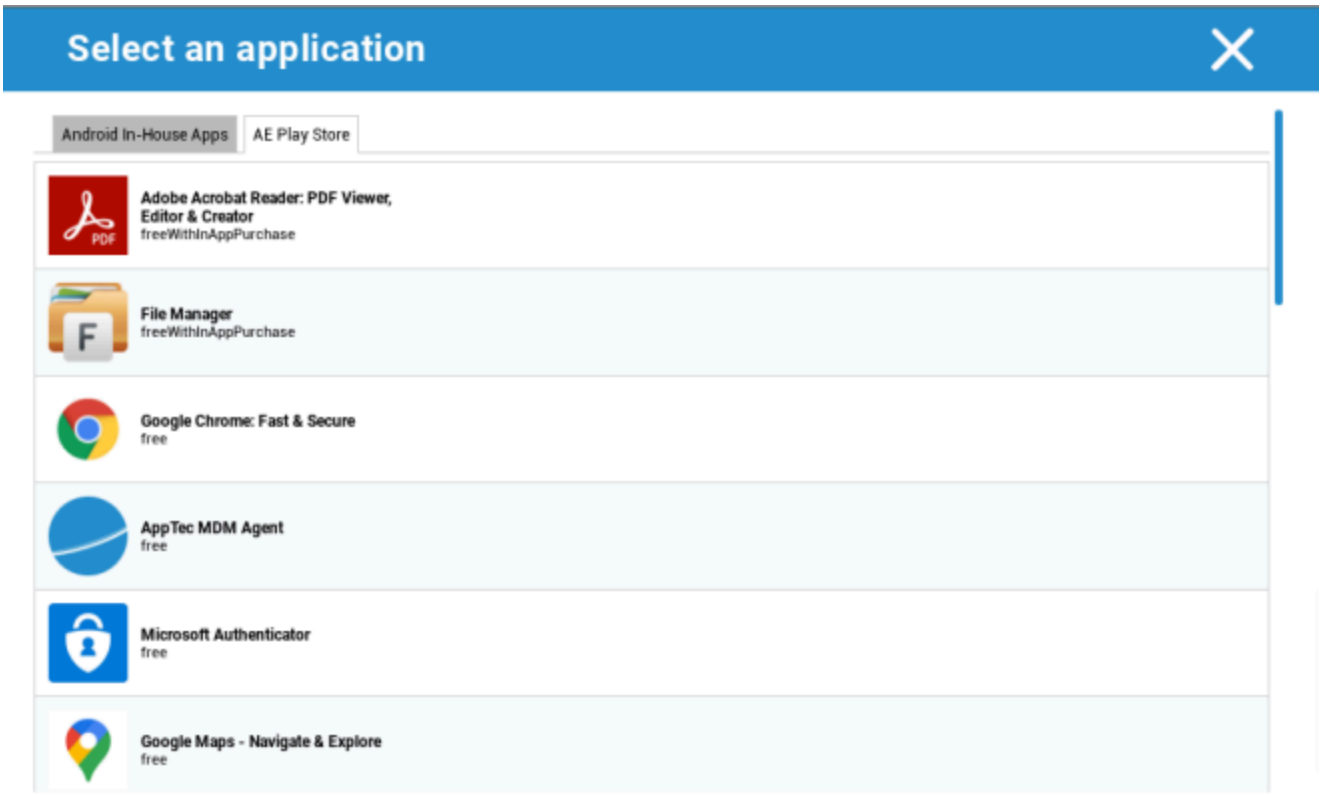


يمكنك أيضًا تحديد ملف apk وتحميله مباشرةً باستخدام "تحميل تطبيق داخلي".



إذا كنت تقوم بتثبيت تطبيق داخلي، سيكون لديك إمكانية تنشيط "التحديث المستمر". إذا تم تفعيل ذلك وقمت بتحديد إصدار أحدث في قاعدة بيانات التطبيق الداخلي، فسيتم تحديث التطبيق على الجهاز.

أو يمكن أن يكون تطبيق "AE Play Store" من متجر Google Work Play Store.



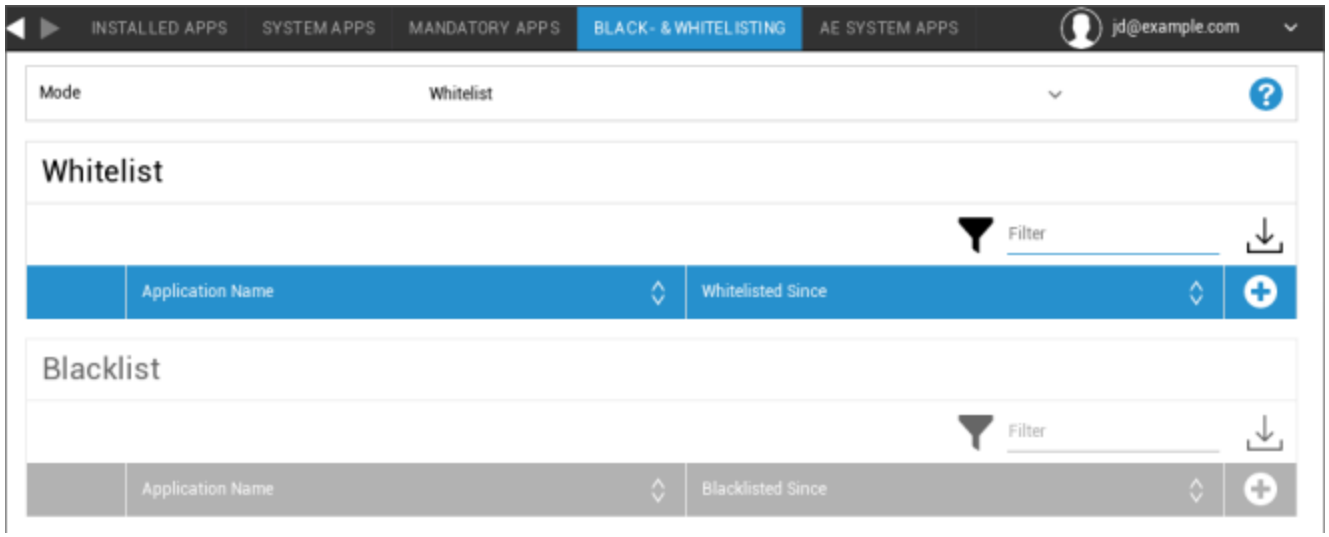
سيتم عرض "تطبيقات AE Play Store" المعتمدة فقط في علامة التبويب هذه.

للموافقة على "تطبيق AE Play Store" يرجى الانتقال إلى "الإعدادات العامة"> "إدارة التطبيقات"> "AE Play المتجر" وإضافة تطبيق عبر الزر الذي سيعيد توجيهك إلى علامة التبويب "تطبيقات متجر Play" (أو يمكنك الانتقال مباشرةً إلى علامة التبويب "تطبيقات متجر Play").

في علامة التبويب "تطبيقات متجر Play Store" يمكنك البحث عن التطبيقات. عند النقر على أحد التطبيقات، تُفتح صفحة التطبيق
وهنا يمكنك الموافقة على التطبيق بالنقر على "الموافقة".

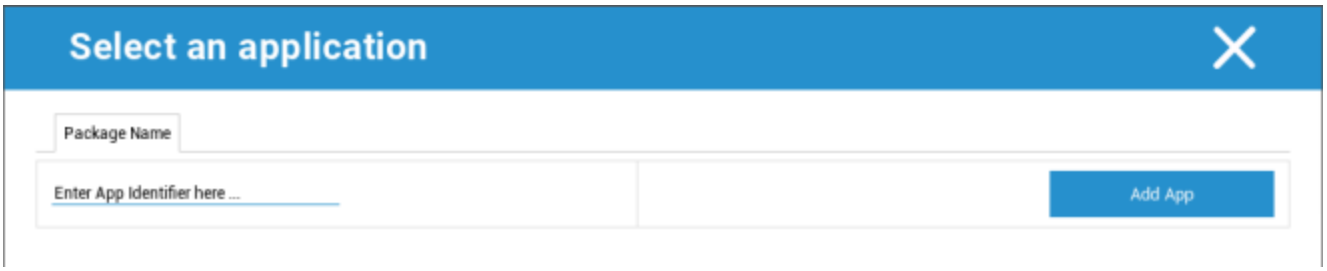
القائمة السوداء والبيضاء

ضمن "القائمة السوداء والقائمة البيضاء"، يمكنك الاختيار بين وضع "القائمة البيضاء" ووضع "القائمة السوداء".



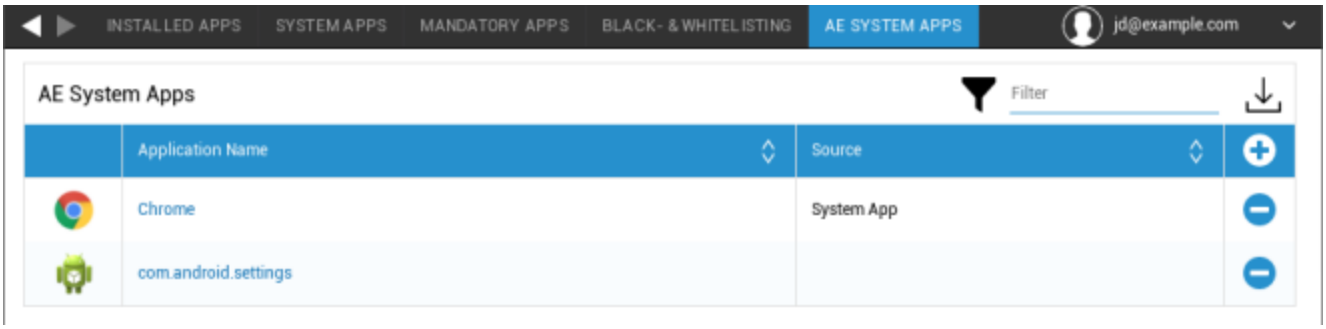
القائمة البيضاء	يمكن فقط تثبيت التطبيقات والخدمات التي تمت إضافتها إلى القائمة على جهاز المستخدم النهائي. إذا كانت مثبتة مسبقاً على جهاز المستخدم النهائي، فسيتم تفعيلها وتعيينها، بحيث يمكن للمستخدم تشغيلها.
	جميع التطبيقات الأخرى التي لم تتم إضافتها إلى القائمة لا يمكن تثبيتها على جهاز المستخدم النهائي. إذا كانت هذه التطبيقات مثبتة مسبقاً على جهاز المستخدم النهائي فسيتم إلغاء تنشيطها وتعيينها، بحيث لا يمكن للمستخدم تشغيلها.
القائمة السوداء	لا يمكن تثبيت التطبيقات والخدمات التي تمت إضافتها إلى القائمة على جهاز المستخدم النهائي. إذا كانت مثبتة مسبقاً على جهاز المستخدم النهائي فسيتم إلغاء تنشيطها وتعيينها، بحيث لا يمكن للمستخدم تشغيلها.
	يمكن تثبيت جميع التطبيقات الأخرى التي لم تتم إضافتها إلى القائمة على جهاز المستخدم النهائي. إذا كانت هذه التطبيقات مثبتة مسبقاً على جهاز المستخدم النهائي، فسيتم تفعيلها وتعيينها، بحيث يمكن للمستخدم تشغيلها.

عبر ال، يمكنك إضافة تطبيقات أو خدمات إضافية إلى القائمة المستخدمة حاليًا.
عبر ال، يمكنك إضافة تطبيقات أو خدمات إضافية إلى القائمة غير النشطة حاليًا.
يمكنك تحديد "اسم الحزمة":

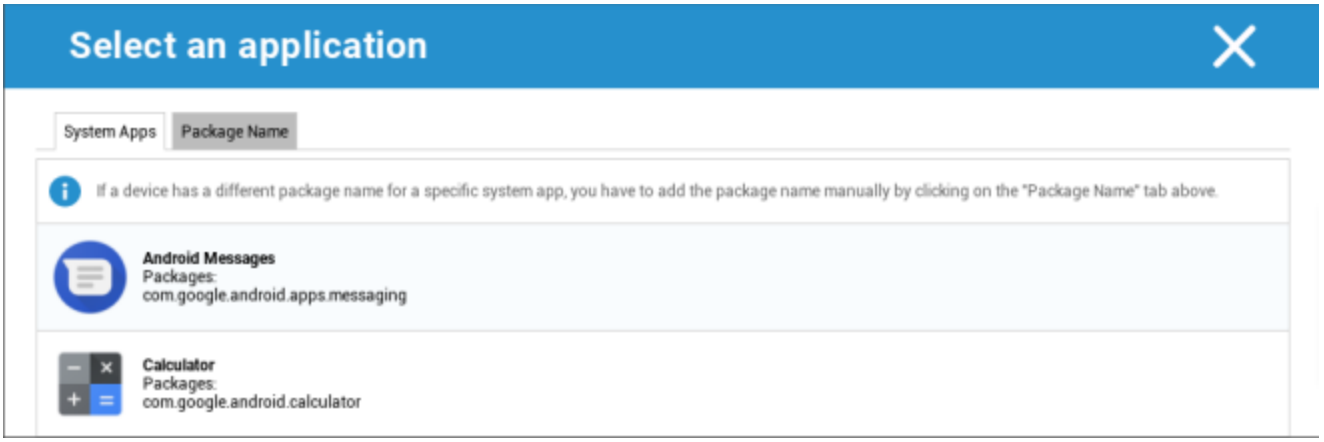

Select an application
Package Name
Enter App Identifier here ...
Add App

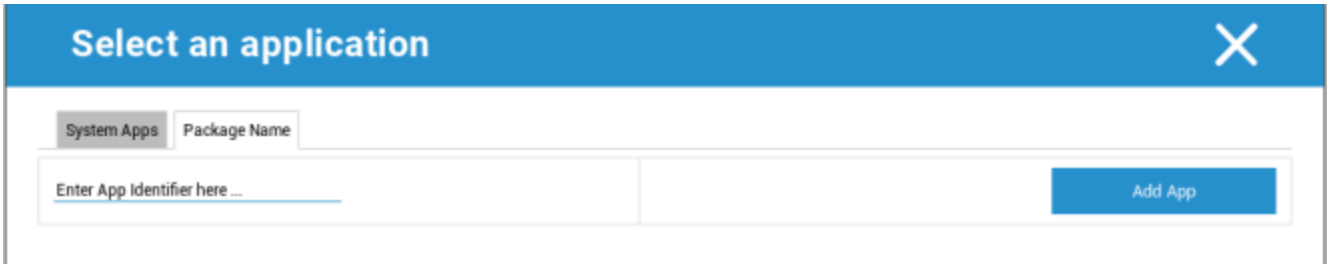
تطبيقات نظام AE

هنا يمكنك تحديد قائمة تحتوي على تطبيقات نظام محددة يجب تفعيلها على الأجهزة.



إذا نقرت على الزر، يمكنك الاختيار من قائمة تطبيقات النظام المحتملة التي توفرها Google أو إدخال اسم حزمة تطبيق النظام الذي يجب تفعيله مباشرةً.





يرجى الأخذ في الاعتبار أن تطبيقات النظام في القائمة المقدمة من Google هي فقط التطبيقات التي يمكن أن تكون تطبيقات نظام، ولكن ليس بالضرورة أن تكون تطبيقات نظام على أجهزتك.

ومع ذلك، فإن هذه القائمة تؤثر فقط على التطبيقات المثبتة مسبقاً فقط.

لن تؤثر إضافة التطبيقات غير المثبتة مسبقًا على أجهزتك على أجهزتك، بغض النظر عما إذا كان التطبيق من القائمة التي توفرها Google أو تم إدخال اسم حزمة التطبيق مباشرةً.

القيود والإعدادات

إعدادات إدارة التطبيق

هنا يمكنك تهيئة سلوك الجهاز فيما يتعلق بتحديثات التطبيق.

تكرار التحقق من التحديث	حدد الفاصل الزمني الذي سيبحث فيه عميل AppTec360 عن تحديثات التطبيق. القيمة الافتراضية هي 24 ساعة.
عتبة الواي فاي	سيتم تنزيل التطبيقات الأكبر من الحجم المحدد عبر Wi-Fi. إذا تم تحديد "Wi-Fi فقط"، فسيتم تنزيل جميع التطبيقات عبر Wi-Fi.

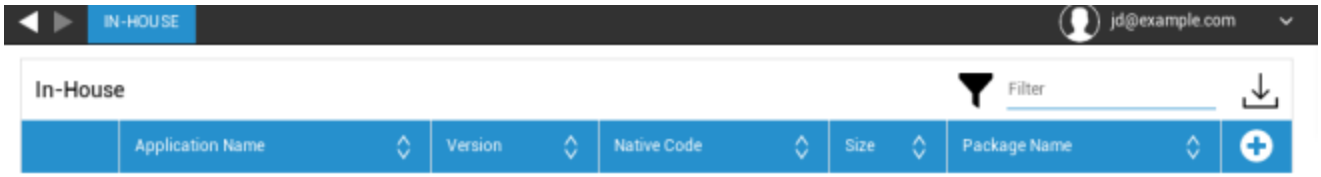
متجر تطبيقات المؤسسات

داخل الشركة

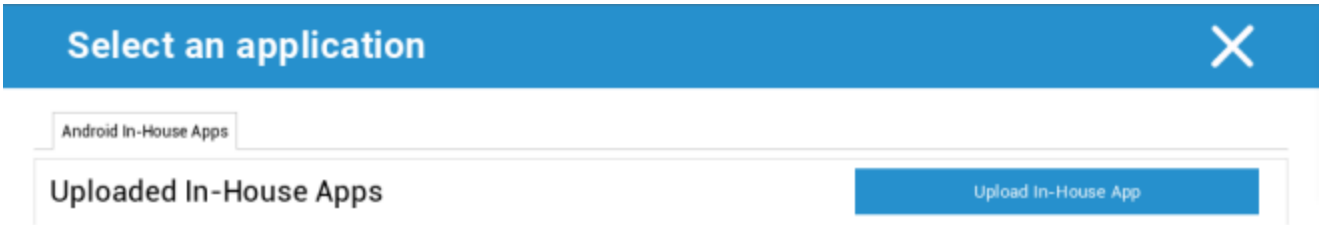
تحت نقطة "داخلياً"، يمكنك تحميل التطبيقات المطورة داخلياً وتوزيعها.

باستخدام الرمز، يمكنك توزيع تطبيقات إضافية داخل الشركة.

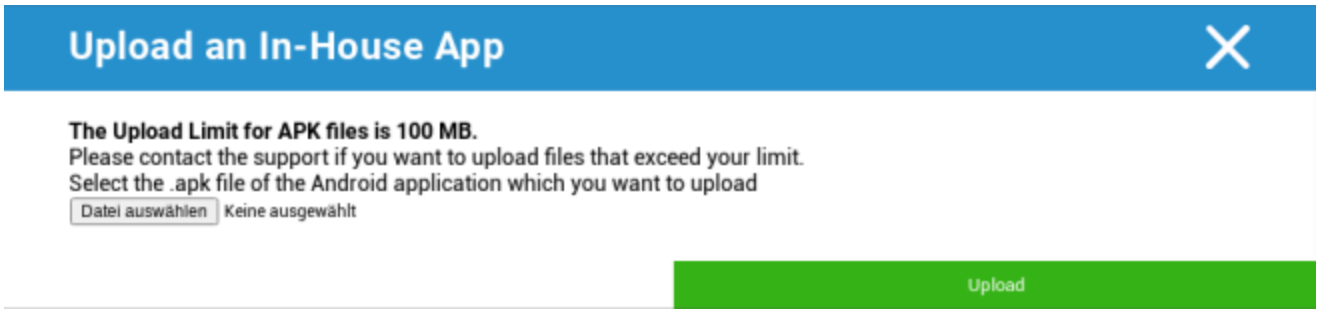
إذا كنت تقوم بتثبيت تطبيق داخلي، سيكون لديك إمكانية تفعيل "التحديث المستمر". إذا تم تفعيل هذا الأمر وقمت بتحديد إصدار أحدث في قاعدة بيانات التطبيق الداخلي، فسيتم تحديث التطبيق على الجهاز.



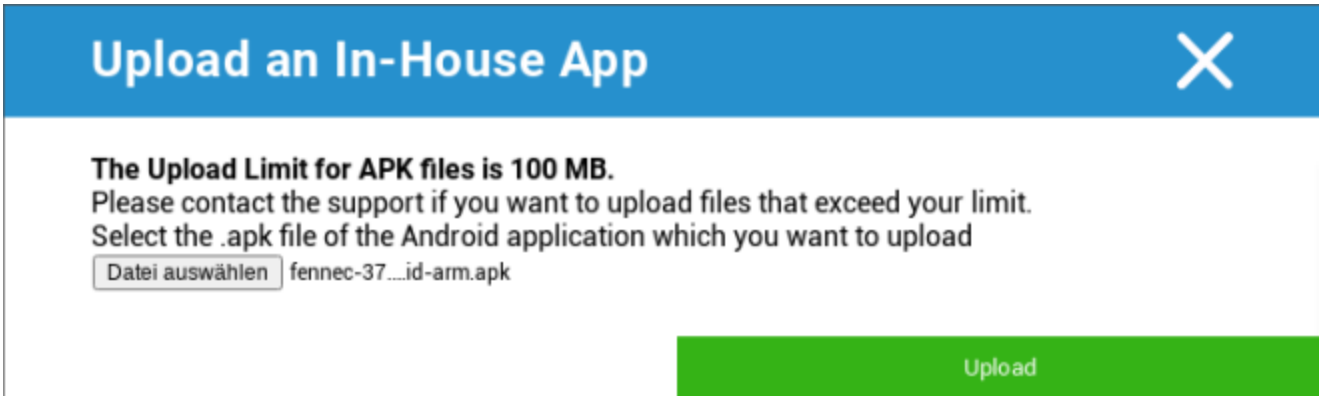
إذا لم تكن قد وزعت تطبيقات داخلية، فستتلقى بعد ذلك النظرة العامة التالية:



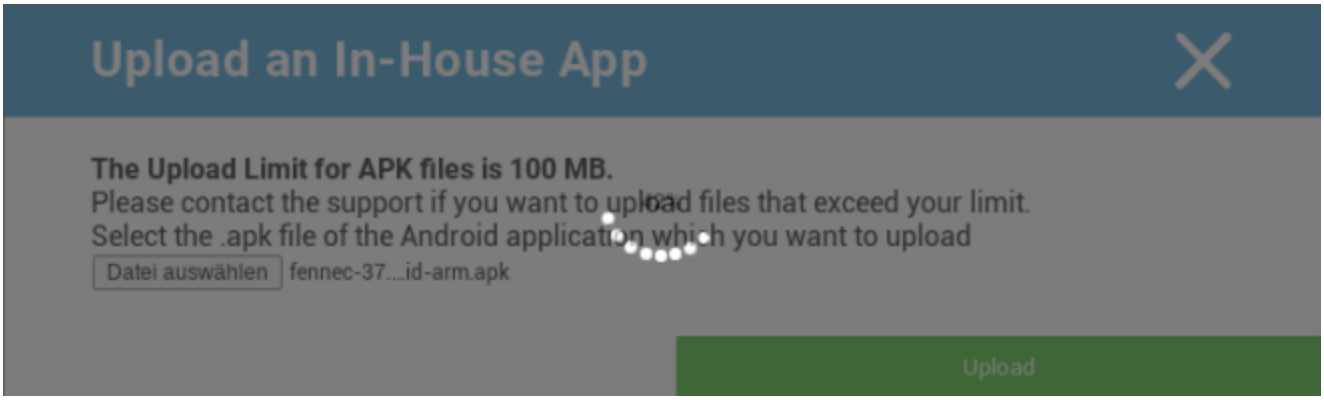
لهذا، انقر على "تحميل تطبيق داخلي"، وستتلقى بعد ذلك النظرة العامة التالية:



الآن، اختر باستخدام "بحث..." ملف .apk ثم انقر على "تحميل".



سيتم الآن تحميل تطبيقك، في منتصف الدائرة سترى مؤشر نسبة مئوية،
يوضح مقدار ما تم تحميله بالفعل من تطبيقك.



في حالة نجاح تحميل تطبيقك الداخلي الخاص بك، يمكنك بعد ذلك العثور على التطبيق الذي تم تحميله في كتالوج التطبيقات.

يتوفر للمستخدم الآن خيار الاطلاع على هذا التطبيق وتثبيته في متجر AppTec360 على جهاز المستخدم النهائي ، تحت فئة "في المنزل".

نظرًا لأن هذا لا يتضمن تطبيق Google PlayStore، لا يحتاج المستخدم إلى معرّف Google مخزّن على جهاز المستخدم النهائي الخاص به.

متجر Play Play للمؤسسات

متجر AE Play

هنا يمكنك إضافة تطبيقات إلى متجر Playstore الخاص بمؤسسات أندرويد. يرجى ملاحظة أنه يجب عليك الموافقة على
التطبيقات باستخدام حساب مسؤول AE الخاص بك قبل أن تتمكن من إضافتها.

للموافقة على تطبيق ما يرجى الاطلاع على التعليمات في التطبيقات الإلزامية.

وضع الكشك والتشغيل

وضع الكشك

يسمح لك وضع الكشك بتحديد تطبيق أو عنوان URL مسبقاً. بعد ذلك سيكون من الممكن حصرياً تشغيل/زيارة هذا التطبيق و/أو عنوان URL.

وبالمثل، يمكن إلغاء تنشيط أزرار الأجهزة المختلفة في وضع الكشك المتنوع.

بدء التشغيل التلقائي	بدء تشغيل وضع الكشك تلقائياً، بمجرد وصول الملف الشخصي إلى جهاز المستخدم النهائي
وضع الكشك المجدول؟	يمكنك تخطيط وقت لوضع الكشك، وسيبدأ هذا بعد ذلك وينتهي تلقائيًا، في الوقت الذي تحدده أنت
وقت البدء	وقت البدء
الوقت بالدقائق	الوقت بالدقائق، وبعد ذلك يجب أن ينتهي وضع الكشك مرة أخرى

نوع التطبيق

تطبيق واحد	إذا كنت ترغب في بدء تشغيل التطبيق في وضع الكشك، حدد "حزمة" ضمن "نوع التطبيق"
تطبيق الكشك	انقر هنا، من أجل تحديد التطبيق الذي يجب تشغيله في وضع الكشك ستجد النظرة العامة المعتادة لإدارة التطبيقات يمكنك الاختيار بين "متجر جوجل بلاي" و"تطبيقات أندرويد الداخلية" و"اسم الحزمة"

نوع التطبيق	
عنوان URL	إذا كنت تريد تشغيل عنوان URL في وضع الكشك، حدد "عنوان URL" ضمن "نوع التطبيق" ثم حدد عنوان URL الذي تريده
مسح المتصفح بعد عدم النشاط	هنا يمكنك تحديد فاصل زمني بالدقائق، وبعد ذلك يجب إعادة تشغيل وضع الكشك
مسح ذاكرة التخزين المؤقت للويب وملفات تعريف الارتباط	إذا قمت بتفعيل هذه الوظيفة، فبعد إعادة تشغيل وضع الكشك، سيتم مسح ذاكرة التخزين المؤقت للويب (ملفات تعريف الارتباط والصور المخزنة مؤقتًا)
سياسة نفس المنشأ	في حالة تفعيل هذه الوظيفة، يمكن للمستخدم تصفح الصفحات الفرعية لعنوان URL المحدد فقط على سبيل المثال، قمت بتحديد عنوان URL التالي:www.mypage.com بعد ذلك، يمكن للمستخدم تصفح الرابط التالي: www.mypage.com/subpage
عناوين URL المدرجة في القائمة البيضاء	هنا يمكنك الاحتفاظ بقائمة بيضاء، كل عناوين URL هذه مسموح بها 1 عنوان URL كحد أقصى لكل سطر يجب أن يبدأ عنوان URL ب http:/ أو https://
عناوين URL المدرجة في القائمة السوداء	هنا يمكنك الاحتفاظ بقائمة سوداء، جميع عناوين URL هذه غير مسموح بها 1 عنوان URL كحد أقصى لكل سطر يجب أن يبدأ عنوان URL ب http:/ أو https://
اتجاه الشاشة	يتعلق هذا الإعداد بتعديلات الشاشة تلقائي = تلقائي عمودي = تنسيق عمودي أفقي = الوضع الأفقي

تطبيق متعدد	إذا قمت بتحديد وضع الكشك "متعدد التطبيقات"، فسيتم فرض استخدام مشغّل AppTec360.
التطبيقات	التطبيق: اختر تطبيق Playstore أو تطبيق داخلي كتطبيق كشك. من الممكن أيضاً إدخال اسم الحزمة. يجب تثبيت تطبيق الكشك المحدد على الجهاز. تذكر تعيين تطبيق الكشك على أنه إلزامي. اختصار على الشاشة الرئيسية: إذا تم الضبط على "تشغيل" سيتم إنشاء اختصار على الشاشة الرئيسية. إذا تم الضبط على "إيقاف التشغيل" سيظل التطبيق يظهر في قائمة التطبيقات.

تم تمكين كلمة مرور الخروج	إذا قمت بتفعيل هذه الوظيفة، فمن الممكن للمستخدم، إنهاء وضع الكشك، بكلمة مرور تم تحديدها مسبقًا من قبلك
كلمة مرور الخروج	هذه هي كلمة المرور، التي تم تحديدها مسبقاً من قبلك
طي شريط الحالة تلقائيًا	في حالة التمكين، سيتم عرض شريط الحالة تلقائيًا بشكل مطوي. باستخدام هذا الخيار يمكن للمستخدمين رؤية المعلومات في شريط الحالة، ولكن لا يمكنهم الوصول إلى وظائفه
تعطيل شريط الحالة	يحتوي شريط الحالة على إشعارات واختصارات ومعلومات. متوفر فقط لأجهزة سامسونج المزودة بـ SAFE 4.0 أو أكبر.
تعطيل مفاتيح مستوى الصوت	تعطيل مفاتيح مستوى الصوت (متوفر فقط على أجهزة سامسونج المزودة ب SAFE 3.0 أو أعلى)
تعطيل مفتاح التشغيل/إيقاف التشغيل	تعطيل مفتاح التشغيل/إيقاف التشغيل (متوفر فقط على أجهزة سامسونج المزودة بـ SAFE 3.0 أو أعلى)
تعطيل زر الصفحة الرئيسية	تعطيل زر الصفحة الرئيسية. إذا تم تنشيط هذه الوظيفة، فلا يمكن إنهاء وضع الكشك إلا في وحدة تحكم AppTec360 (متوفر فقط على أجهزة Samsung المزودة بـ SAFE 3.0 أو أعلى)
تعطيل شريط التنقل	باستخدام هذا يمكنك تعطيل شريط التنقل (رجوع / قائمة) إذا تم تنشيط هذه الوظيفة، فلا يمكن إنهاء وضع الكشك إلا في وحدة تحكم AppTec360 (متوفر فقط على أجهزة Samsung المزودة بـ SAFE 3.0 أو أعلى)

مُشغِّل تطبيقات AppTec360

تمكين مشغل التطبيقات AppTec360	تشغيل: تمكين مشغّل AppTec360. يجب على المستخدم تعيينه كمشغل افتراضي مرة واحدة. ملاحظة: إذا تم تمكين وضع الكشك، وتم ضبط وضع الكشك على "تطبيق متعدد"، فسيتم فرض استخدام مشغل AppTec360.
أيقونات كبيرة	تشغيل: يعرض نسخة أكبر من أيقونات التطبيقات في المشغّل
إخفاء أيقونة تطبيق AppTec360	تشغيل: يخفي تطبيق AppTec360 بالكامل
إخفاء أيقونة متجر AppTec360	تشغيل: يخفي AppTec360 Enterprise AppStore بالكامل

إعدادات AppTec360

تمكين تطبيق إعدادات AppTec360 AppTec360	يوفر تطبيق إعدادات AppTec360 AppTec360 التحكم في اتصالات الواي فاي والبلوتوث
تمكين الإعدادات في التطبيق المتعدد وضع الكشك	في حالة التمكين، يمكن للمستخدمين الوصول إلى تطبيق إعدادات AppTec360 أثناء تنشيط وضع الكشك متعدد التطبيقات

جهاز التحكم عن بُعد

سبلاش توب

لبدء جلسة تحكم عن بُعد لجهازك، يجب تثبيت تطبيق "Splashtop Streamer" على الجهاز عن طريق إضافة التطبيق إلى **إدارة التطبيقات** ← **مدير تطبيقات المؤسسة** ← **التطبيقات الإلزامية**.

بعد ذلك، قم بتكوين الإعدادات التالية لسبلاشتوب:

تمكين سبلاش توب	في حالة التمكين، سيقوم AppTec360 بتهيئة تطبيق Splashtop للسماح بالتحكم عن بعد
نشر الكود	انتقل إلى https://my.splashtop.com وقم بتسجيل الدخول إلى حساب Splashtop الخاص بك. انقر على "إضافة كمبيوتر" وانسخ رمز النشر المكون من 12 رقمًا من الصفحة الناتجة.
تعيين بوابة النشر المخصص؟	نشر البوابة
نشر نطاق البوابة/ المضيف	نشر البوابة
التحقق من الشهادات	التحقق من الشهادات

بعد ذلك يمكنك استخدام الخيار Splashtop Remote Control في قائمة السياق (الترس بجوار شريط البحث، عند تحديد الجهاز أو النقر بزر الماوس الأيمن على الجهاز في الشجرة) لبدء جلسة التحكم عن بعد.

برنامج TeamViewer

لبدء جلسة تحكّم عن بُعد لجهازك، يجب تثبيت تطبيق "TeamViewer QuickSupport" على الجهاز عن طريق إضافة التطبيق إلى **إدارة التطبيقات** ← **مدير تطبيقات المؤسسة** ← **التطبيقات الإلزامية**.

بعد ذلك يمكنك استخدام الخيار **TeamViewer للتحكم عن بُعد** في قائمة السياق (الترس المجاور لشريط البحث، عند تحديد الجهاز أو النقر بزر الماوس الأيمن على الجهاز في الشجرة) لبدء جلسة التحكم عن بُعد.

إدارة المحتوى

صندوق المحتوى

هنا يمكنك تنشيط ContentBox.

بمجرد أن تقوم بتبديل "تمكين ContentBox" إلى "تشغيل"، سيتم تثبيت تطبيق ContentBox منفصل تلقائياً على جهاز المستخدم النهائي.

متصفح آمن

هنا يمكنك تهيئة إعدادات متصفح AppTec360 الآمن.

بمجرد تبديل القسم في "المتصفح الآمن" إلى "تشغيل"، سيتم تثبيت تطبيق متصفح منفصل تلقائيًا على جهاز المستخدم النهائي.

تتطلب كلمة مرور	مطالبة المستخدم بإعداد كلمة مرور واستخدامها للوصول إلى المتصفح.
الحد الأدنى لطول كلمة المرور المطلوبة	تعيين عدد الأحرف المطلوبة لكلمة المرور
جودة كلمة المرور المطلوبة	تعيين جودة كلمة المرور المطلوبة
تقييد التنزيلات / فتح في	
تقييد التحميلات	
تحميل القائمة البيضاء	قائمة بعناوين URL التي يُسمح بتحميلها دائماً.
السماح بالنسخ	السماح بنسخ النص أو قصه أو مشاركته داخل صفحات الويب.
السماح بالتقاط الشاشة	السماح بالتقاط لقطات الشاشة.
تواتر تنظيف البيانات	حدد التردد الذي يجب إزالة جميع بيانات المستخدم (السجل وذاكرة التخزين المؤقت وما إلى ذلك) تلقائيًا.
الإشارات المرجعية للشركة	ستظهر الإشارات المرجعية في مجلد "الإشارات المرجعية للشركة" في الإشارات المرجعية للمتصفحات. وهي غير قابلة للتحرير من قبل المستخدم.
إخفاء شريط العنوان	
القائمة البيضاء داخل المتصفح (بدون البوابة العالمية)	تمكين القائمة البيضاء لعناوين URL من جانب العميل. • يتم دائمًا إدراج الإشارات المرجعية للشركة في القائمة البيضاء • مدعومة لـ 100 عنوان URL فقط • يرجى استخدام البوابة العالمية لقائمة سوداء وبيضاء غير محدودة
عناوين URL المدرجة في القائمة البيضاء	قائمة بعناوين URL المسموح بها.
القائمة السوداء والقائمة البيضاء المستندة إلى البوابة	تتضمن القائمة السوداء المتطلبات التالية: • بوابة عالمية للتطبيق العالمي AppTec360 عاملة ("الإعدادات العامة" → "البوابة العالمية")

	• تكوين VPN عامل مع خادم DNS محدد ("الإعدادات العامة" → "البوابة العامة" → "إعدادات VPN") • تكوين القائمة السوداء ("الإعدادات العامة" → "البوابة العامة" → "القائمة السوداء للنطاق") • اتصال VPN صالح في ملف التعريف ("إدارة الاتصال" → "VPN")

واجهة برمجة التطبيقات الإضافية

Samsung KNOX

القيود

السماح لبطاقة SD	
السماح بالكتابة على بطاقة SD	
السماح بالتقاط الشاشة	
السماح للحافظة	
إعدادات النسخ الاحتياطي وبيانات التطبيق في Google Cloud	
استعادة الإعدادات من جوجل كلاود عند إعادة تثبيت أحد التطبيقات	
السماح بتصحيح أخطاء USB	
السماح بتقرير أعطال Google	
السماح بإعادة ضبط المصنع	
السماح بترقية OTA	
السماح بتخزين USB المضيف	في حالة التمكين، يمكن للمستخدم توصيل أي محرك أقراص قلمي (وحدة تخزين USB محمولة) أو قرص صلب خارجي أو قارئ بطاقات رقمية آمنة (SD)، ويتم تثبيته كمحرك تخزين على الجهاز.
السماح بمشغل وسائط USB (MTP، PTP)	
السماح بالميكروفون	تعطيل الميكروفون لتطبيقات الطرف الثالث
السماح بتقنية الاتصال قريب المدى (NFC)	
السماح بمصادر غير معروفة (تحميل جانبي لملف APK)	في حالة التمكين، يُسمح بالتحميل الجانبي للتطبيقات (ملفات APK). بمجرد تعطيل هذا الإعداد، يتعين على المستخدم تمكينه يدويًا عند إعادة السماح بتثبيت ملفات APK من مصادر غير معروفة.
السماح بإنشاء المستخدم	في حالة التمكين، يُسمح للمستخدم بإنشاء حسابات متعددة على الجهاز، على سبيل المثال حسابات الضيوف

البريد الإلكتروني

عنوان البريد الإلكتروني	
بروتوكول الخادم الوارد	
عنوان الخادم الوارد	
منفذ الخادم الوارد	
تسجيل الدخول إلى الخادم الوارد/اسم المستخدم	
كلمة مرور الخادم الوارد	
يستخدم الخادم الوارد SSL	
يستخدم الخادم الوارد TLS	
يقبل الخادم الوارد جميع الشهادات	
بروتوكول الخادم الصادر	
عنوان الخادم الصادر	
منفذ الخادم الصادر	
يستخدم الخادم الصادر بيانات اعتماد إضافية	إذا تم تعطيله، يستخدم النظام بيانات الاعتماد الواردة للخادم الصادر أيضاً.
تسجيل الدخول إلى الخادم الصادر/اسم المستخدم	
كلمة مرور الخادم الصادر	
يستخدم الخادم الصادر SSL	
يستخدم الخادم الصادر TLS	
يقبل الخادم الصادر جميع الشهادات	
تعيين التوقيع	
التوقيع	ملاحظة: بالنسبة لبعض الأجهزة، يجب تحديد التوقيع بتنسيق HTML.
إعلام المستخدم عند تلقي بريد إلكتروني جديد	

المبادلات

عنوان البريد الإلكتروني	
اسم مضيف الخادم	اسم المضيف لخادم Exchange
اسم تسجيل الدخول	اسم المستخدم المستخدم المستخدم لتسجيل الدخول إلى خادم Exchange Server
المجال	إذا تم تمكين تكوين بوابة ACL ولم يكن حقل المجال فارغًا، فستقوم بوابة AppTec360 العالمية بمصادقة الجهاز بالاسم التالي "اسم المجال/اسم تسجيل الدخول
كلمة المرور	
عدد الأيام السابقة للمزامنة	
تكرار مزامنة البريد الإلكتروني	
المزامنة أثناء التجوال	
تعيين التوقيع	
التوقيع	ملاحظة: بالنسبة لبعض الأجهزة، يجب تحديد التوقيع بتنسيق HTML.
الحساب الافتراضي	
استخدام طبقة مآخذ التوصيل الآمنة (SSL)	
استخدام أمان طبقة النقل (TLS)	
قبول جميع الشهادات	

شبكة APN

اسم العرض APN	
اسم نقطة الوصول	اسم شبكة APN
بروتوكول الخادم الصادر	
MCC - رمز البلد المتنقل	اتركها فارغة لاستخدام MMC لشريحة SIM المثبتة
MNC - كود شبكة الجوال	اتركه فارغاً لاستخدام mnc من بطاقة SIM المثبتة
عنوان الخادم	
رقم منفذ الخادم	
عنوان وكيل الخادم	
عنوان خادم رسائل الوسائط المتعددة	اتركه فارغاً للإعداد الافتراضي
رقم منفذ رسائل الوسائط المتعددة	اتركه فارغاً للإعداد الافتراضي
عنوان وكيل رسائل الوسائط المتعددة	اتركه فارغاً للإعداد الافتراضي
اسم المستخدم	
كلمة المرور	
نوع نقطة الوصول	الأنواع المقبولة هي "افتراضي"، "supl"، "mms".
	إذا تم تمرير لاغية أو فارغة، يتم استخدام "افتراضي، سوبيل، م م م س" افتراضيًا.
	اتركه فارغاً للافتراضي.
شبكة APN المفضلة	

بلوتوث

السماح باكتشاف الجهاز عبر البلوتوث	
السماح بإقران البلوتوث	
السماح بأجهزة سماعات البلوتوث	
السماح للأجهزة التي تعمل بالبلوتوث بدون استخدام اليدين	
السماح لأجهزة Bluetooth A2DP	A2DP، ملف تعريف توزيع الصوت المتقدم A2DP، يسمح ببث الصوت بين الأجهزة
السماح بالمكالمات الصادرة	
السماح بنقل البيانات عبر البلوتوث	
السماح بالربط عبر البلوتوث	
السماح بالاتصال بالكمبيوتر عبر البلوتوث	

الاتصال

السماح بالمكالمات الطارئة فقطالسماح بمكالمات الطوارئ فقطالسماح بشبكة Wi-Fi	
الحد الأدنى لمستوى أمان شبكة Wi-Fi	
منع المستخدم من إضافة شبكات Wi-Fi	لا يمكن تفعيل هذا القيد إلا إذا تم تعريف ملف تعريف Wi-Fi نشط واحد على الأقل ضمن إدارة الاتصال
السماح بالرسائل النصية القصيرة ورسائل الوسائط المتعددة	
السماح بالمزامنة أثناء التجوال	
السماح بالتجوال الصوتي	

نظام Android Enterprise – جهاز مُدار بالكامل مع ملف تعريف العمل (COPE)

شرح عام لـ COPE

COPE هو اختصار لـ COPE وهو اختصار لـ "**مملوكة للشركات مُمكّنة شخصياً**".

يسمح وضع COPE بتسجيل جهاز Android كجهاز **Android Enterprise - جهاز مُدار بالكامل** مع ملف تعريف **Android Enterprise - حاوية** مدمج.

يمكن أن يكون هذا إما جهاز Android مسجلاً بالفعل **كجهاز Android Enterprise - جهاز مُدار بالكامل** بنظام **Android Enterprise - جهاز** مُدار **بالكامل** والذي تم إعداد **حاوية Android Enterprise - حاوية** عليه بالإضافة إلى ذلك، أو جهاز Android مسجل حديثًا تم تسجيله مباشرة **كجهاز Android Enterprise - جهاز مُدار بالكامل بنظام Android Enterprise - حاوية** فوقه.

يتوفر وضع COPE للأجهزة التي تعمل بنظام Android 8 و9 و10 فقط

تكوين ملفات التعريف لأجهزة COPE

نظرًا لعدم وجود ملف تعريف تكوين لوضع COPE نفسه، يتم فصل تكوين **Android Enterprise - جهاز مُدار بالكامل** و **Android Enterprise - حاوية** إلى ملفين جانبيين ضمن ملف تعريف COPE. من الممكن التبديل بين ملفي التعريف لتهيئة كل ملف تعريف من خلال النقر على الزر المعني على الجانب الأيسر من وحدة التحكم:

يمكن تكوين كلا الملفين كما هو موضح لكل ملف تعريف على حدة:

أندرويد إنتربرايز - جهاز مُدار بالكامل

أندرويد إنتربرايز - الحاوية

العودة إلى جهاز AE المُدار بالكامل

يمكن إزالة ملف تعريف **Android Enterprise - Container** كما هو موضح في **إدارة الأجهزة المحمولة**.

من خلال إزالة ملف تعريف الحاوية، سيتم تحويل ملف تعريف COPE إلى ملف تعريف **Android Enterprise - جهاز مُدار بالكامل**.

مؤسسة أندرويد – تكوين الحاوية – تكوين الحاوية

اعتمادًا على ما إذا كنت قد حددت حاليًا ملف تعريف مجموعة أو جهاز، تختلف النظرة العامة ونقاطها الفرعية - يرجى مراعاة ذلك بعناية!

جنرال لواء

نظرة عامة على الملف الشخصي (على مستوى الملف الشخصي فقط)

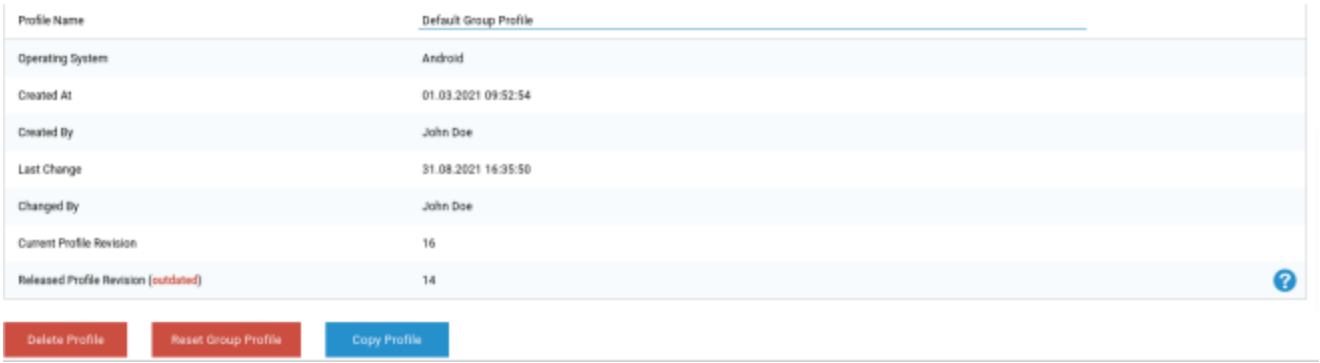
في حالة وجودك في ملف تعريف، ستتلقى نظرة عامة موجزة عن الملف الشخصي، فيما يتعلق بالاسم ونظام التشغيل وتاريخ الإنشاء والمؤلف وما إلى ذلك.

اسم الملف الشخصي	اسم الملف الشخصي - يمكن إعادة تسميته مباشرة هنا
نظام التشغيل	نظام تشغيل صالح للملف الشخصي
تم إنشاؤها في	تاريخ الإنشاء
تم إنشاؤها بواسطة	تم إنشاؤها بواسطة
آخر تغيير	تاريخ آخر تغيير
تم التغيير بواسطة	المستخدم الذي أجرى آخر تغييرات على ملف التعريف هذا
مراجعة الملف الشخصي الحالي	عدد المرات التي تم فيها تحديث الملف الشخصي بالفعل
مراجعة الملف الشخصي الصادر	عدد المرات التي تم فيها تحديث ملف التعريف بالفعل وتم تعيين أجهزة له

حذف الملف الشخصي	حذف الملف الشخصي
إعادة تعيين ملف تعريف المجموعة	إعادة تعيين ملف تعريف المجموعة
ملف تعريف النسخ	ملف تعريف النسخ

نظرة عامة على ملف تعريف المجموعة (على مستوى المجموعة فقط)

عند فتح الملف الشخصي للمجموعة، ستحصل على نظرة عامة سريعة على الملف الشخصي.



اسم الملف الشخصي	اسم الملف الشخصي (يمكن تغييره هنا)
نظام التشغيل	نظام التشغيل الذي تم إنشاء ملف التعريف له
تم إنشاؤها في	وقت الإنشاء
تم إنشاؤها بواسطة	منشئ الملف الشخصي
آخر تغيير	وقت آخر تغيير في الملف الشخصي
تم التغيير بواسطة	الحساب الذي أجرى التغييرات الأخيرة
مراجعة الملف الشخصي الحالي	مراجعة حالة الملف الشخصي المحفوظة
مراجعة الملف الشخصي الصادر	مراجعة الملف الشخصي المعين ("تعيين الآن"). إذا كانت التسمية تظهر "(قديم)" خلف النص، فهذا يعني أنك قمت بحفظ ملف التعريف ولكنك لم تعيّنه بعد، لذا ستظل الأجهزة تحصل على الإصدار الأقدم.

نظرة عامة على الجهاز (على مستوى الجهاز فقط)

في حالة وجودك على أحد الأجهزة، ستتلقى ملخصاً عاماً للجهاز المحدد، ويتضمن ما يلي

اسم الجهاز	اسم الجهاز
الموقع	إحداثيات الموقع
رقم الهاتف	رقم الهاتف
التطبيقات الإلزامية المعينة	عدد التطبيقات الإلزامية المعينة
إصدار نظام التشغيل	إصدار نظام التشغيل الخاص بالجهاز
نظام التشغيل	نظام التشغيل (أندرويد إنتربرايز)
الرقم التسلسلي	الرقم التسلسلي للجهاز
ملكية الجهاز	جهاز الشركة أو الجهاز الخاص
نوع الجهاز	جهاز AE Work المُدار من قبل AE
متجذر	الحالة، التي تشير إلى ما إذا كان الجهاز قد تم تجذيره
متوافق	متوافق مع المبادئ التوجيهية
عنوان IP	عنوان IP الخاص بالجهاز
آخر ظهور	النقطة الزمنية، عندما كان الجهاز متصلاً بـ AppTec لآخر مرة
الدفعة الأخيرة	النقطة الزمنية، عندما تم إرسال آخر دفعة إلى الجهاز
تعيين المستخدم	المستخدم أو المجموعة التي تم تعيين هذا الجهاز لها

مراجعة التكوين

هنا تتلقى نظرة عامة على ملف تعريف المجموعة المعين للجهاز.

إذا نقرت على ملف تعريف المجموعة، ستحصل على وصول مباشر إلى ملف التعريف هذا ويمكنك إجراء الإعدادات.

باستخدام هذا الرمز، يمكنك إعادة التطبيقات الموزعة إلى إعدادات ملف تعريف المجموعة.

باستخدام هذا الرمز، يمكنك إعادة جميع التطبيقات المستخدمة إلى إعدادات ملف تعريف المجموعة.

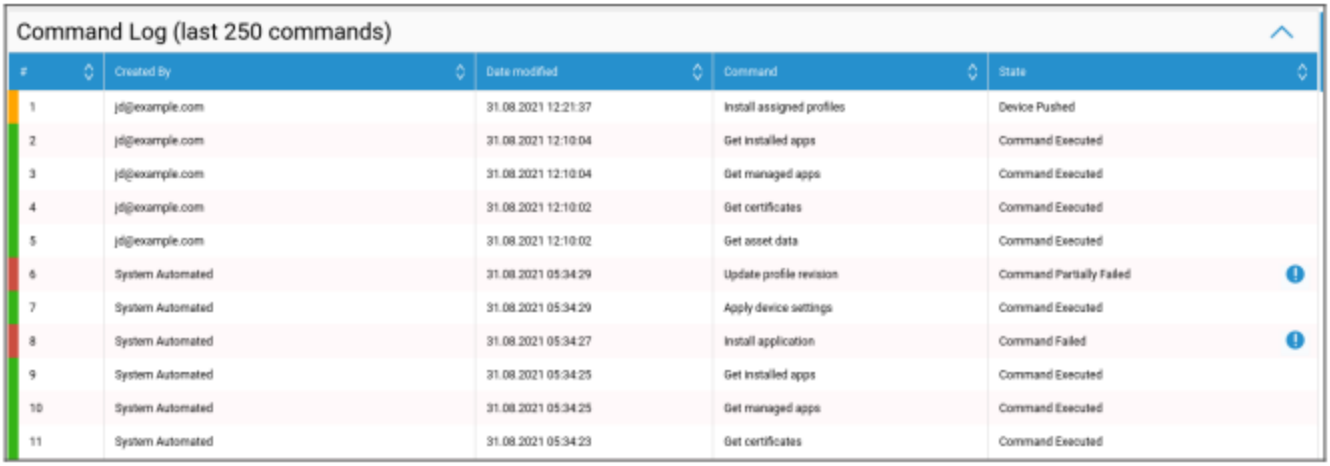
تشير عبارة "تتوفر مراجعة أحدث" إلى أن ملف تعريف المجموعة قد تم تغييره وحفظه ولكن لم يتم تعيينه. يجب تعيين ملف تعريف المجموعة باستخدام "تعيين الآن" على مستوى المجموعة لتطبيق التغييرات على الأجهزة.

سجل الجهاز (على مستوى الجهاز فقط)

ستتلقى هنا سجلات الجهاز المختلفة. إذا لزم الأمر، يمكنك معرفة سبب الخطأ مباشرةً من هنا.

سجل الأوامر

هنا يمكنك معرفة الأوامر التي تم إصدارها للجهاز وما هي حالتها.



حالات الأوامر المحتملة

تم دفع الجهاز	تم إرسال طلب دفع إلى خدمة الدفع (مثل APNS) لإخبار الجهاز بالاتصال مرة أخرى بخادم EMM.
تم إنشاء الأمر	تم إنشاء الأمر في النظام.
تم إرسال الأمر	تم إرسال الأمر إلى الجهاز بعد اتصاله بالخادم.
تم تنفيذ الأمر	تم تنفيذ الأمر بنجاح.
فشل الأمر	فشل الأمر. *
فشل الأمر جزئياً	اعتمادًا على نظام تشغيل الجهاز قد يتم تجميع بعض الأوامر معًا. في هذا فشلت بعض أجزاء مجموعة الأوامر هذه. *
تم تنفيذ الأمر، وفشل الأمر في النهاية	تم تنفيذ الأمر ولكن ربما لم يتم تنفيذه.
إعادة دفع الأمر	تم إعادة دفع الأمر من قبل مستخدم.
مهملة	تم تجاهل الأمر. على سبيل المثال لأنه تم استبداله بأمر آخر أو تم إعادة تسجيل الجهاز وإزالة الأوامر القديمة

*إذا كانت هناك علامة تعجّب خلف الرسالة، يمكنك الحصول على مزيد من المعلومات من خلال تمرير مؤشر الماوس فوق الرمز.

إعدادات الجهاز

تهيئة العميل

هنا يمكنك إجراء التكوينات التالية على جهاز Android الخاص بك:

وقت عدم الامتثال	مهلة استجابة المستخدم التي يتم بعدها تطبيق إجراء الإنفاذ.
إجراء الإنفاذ بعد انتهاء مهلة الامتثال	إجراء الإنفاذ عندما لا يقوم المستخدم بتنفيذ إجراءات تؤدي إلى حالة الجهاز المتوافق
تواتر جمع البيانات	التواتر الذي سيتم به جمع معلومات الجهاز/النظام العالمي لتحديد المواقع
تردد نبضات قلب الجهاز	الفاصل الزمني الذي يجب أن يتصل فيه الجهاز بخادم AppTec دقيقة واحدة 1 دقيقة كحد أقصى. 24 ساعة
تمكين تحديثات الموقع	في حالة تفعيله، يرسل الجهاز تحديثات الموقع إلى خادم AppTec
وقت تحديث الموقع	يحدد الفترات الزمنية التي يرسل فيها الجهاز تحديثات الموقع إلى AppTec
استخدام دقة الموقع الجغرافي من Google لتحديث الموقع الجغرافي	إذا تم تنشيطه، فسيتم استخدام موقع الشبكة لتحديثات الموقع (إذا تم إلغاء تنشيطه ضمن "القيود"، فلن يؤثر هذا الإعداد على أي شيء)
استخدام موقع GPS لتحديث الموقع	في حالة تفعيله، سيتم استخدام GPS لتحديثات الموقع الجغرافي
السماح بالمواقع الوهمية (الوهمية)	السماح بتزوير معلومات الموقع الجغرافي عبر تطبيقات الطرف الثالث
إجراء فقدان الاتصال المفقود	في حالة التمكين، يمكنك تحديد إجراء في حالة عدم حصول الجهاز على اتصال بخادم MDM في الفاصل الزمني لنبض القلب. على سبيل المثال، إذا كان وقت نبض القلب للجهاز 5 دقائق، فإنه يتصل بالخادم في الساعة 10:35 صباحاً. بعد ذلك يغادر الجهاز نطاق Wi-Fi. سيفشل نبض القلب التالي في الساعة 10:40 صباحاً، وسيتم تنفيذ الإجراء المحدد.
الإجراء	الإجراء الذي يجب اتخاذه، بمجرد أن يصبح الجهاز غير متوافق. • Lock جهاز Lock = جهاز القفل • مسح الجهاز = ستتم استعادة الجهاز إلى إعدادات المصنع • مسح الجهاز وبطاقة SD = ستتم استعادة الجهاز إلى إعدادات المصنع وسيتم حذف تخزين بطاقة SD
العتبة	يمكنك تحديد عتبة من نبضات القلب الفاشلة الضرورية لتشغيل الإجراء المحدد.

وضع إنفاذ السياسة	افتراضي:	ستتم مطالبة المستخدمين بشكل دوري بتنفيذ الإجراءات المعلقة

	تطبيق السياسات الكسولة	لن يُطلب من المستخدمين أبداً تنفيذ الإجراءات المعلقة. سيتم عرض جميع الإجراءات المفتوحة في AppTec Client
	إنفاذ السياسة الصارمة:	سيُطلب من المستخدمين دون توقف تنفيذ الإجراءات المعلقة
قفل إصدار AppTec		في حالة التمكين، يمكن تحديد رمز إصدار لتطبيق AppTec. سيقوم عميل AppTec بالتحديث إلى الإصدار المحدد فقط. سيتم تجاهل الإصدارات الأحدث. لا يمكن إجراء ترقية إلى إصدار أقل.
رمز الإصدار		رمز الإصدار لتطبيق AppTec المراد تأمينه عليه.
تعطيل تنبيهات AppTec		إذا تم تعطيل عميل AppTec فلن يظهر إشعار في شريط الإشعارات. وبالتالي يمكن للمستخدمين إغلاق عميل AppTec عبر مدير المهام. إذا تم إغلاق عميل AppTec، فلن تعمل العديد من الميزات بما في ذلك وضع الكشك وقائمة التطبيقات السوداء/القائمة البيضاء بشكل صحيح. توفر أجهزة Samsung آلية حماية لعميل AppTec Client. يتم تعطيل الإشعار بشكل افتراضي على أجهزة سامسونج التي تدعم واجهات برمجة تطبيقات KNOX. يجب عدم تعطيل الإشعار في الأجهزة التي تعمل بنظام Android 8.0 أو أعلى.

ورق حائط

تعيين خلفية مخصصة	تمكين/تعطيل الخلفية المخصصة
ورق حائط	اضبط وضع الخلفية لاستخدام رمز لوني أو صورة
تحديد اللون	حدد لون الخلفية كقيمة سداسي عشري، على سبيل المثال #000000 للأسود أو #ffffffffff للأبيض
تعيين الصورة كخلفية	قم بتحميل ملف الصورة التي تريد استخدامها كخلفية

إدارة الأصول (على مستوى الجهاز فقط)

معلومات الجهاز

الطراز	تسمية طراز الجهاز
نظام التشغيل	نظام التشغيل
إصدار نظام التشغيل	إصدار نظام التشغيل
الرقم التسلسلي	الرقم التسلسلي
اسم الجهاز	اسم الجهاز
حالة البطارية	حالة البطارية
الذاكرة الحرة/إجمالي الذاكرة الحرة	الذاكرة الحرة/الإجمالية
خزنة سامسونج	واجهة Samsung SAFE، مطلوبة لمجموعة متنوعة من خيارات الإعدادات
بطاقة SD متوفرة	بطاقة SD متوفرة
مضاهاة بطاقة SD	محاكاة بطاقة SD
بطاقة SD قابلة للإزالة	بطاقة SD قابلة للإزالة
ذاكرة SD الحرة/إجمالي الذاكرة الحرة	ذاكرة بطاقة SD الحرة/إجمالي ذاكرة بطاقة SD الحرة

الواي فاي

عنوان IP	عنوان IP للجهاز
واي فاي ماك	عنوان MAC الواي فاي

خلوي

الحالة	الحالة (بطاقة SIM مثبتة)
رقم الهاتف	رقم الهاتف
التجوال (الصوت/البيانات)	التجوال للصوت/البيانات
حالة التجوال	حالة التجوال الحالية
عنوان IP	عنوان IP
المشغل/الناقل	المشغل/الناقل
التكنولوجيا الخلوية	التكنولوجيا الخلوية
IMEI	رقم IMEI
ICCID	هذا هو المعرف الخاص ببطاقة SIM، وغالبًا ما تكون أيضًا بطاقة ذكية أو بطاقة دائرة متكاملة (ICC)
IMSI	توفر الهوية الدولية للمشتركين في الهاتف المحمول (IMSI) في شبكات GSM وUMTS للهواتف المحمولة تعريفاً محدداً لمستخدمي الشبكة يتكون IMSI من 15 رقماً كحد أقصى ويتم تكوينه بالطريقة التالية: • رمز البلد المتنقل (MCC)، 3 أرقام • رمز شبكة الهاتف المحمول (MNC)، 2 أو 3 أرقام • رقم تعريف مشترك الهاتف المحمول (MSIN)، من 1-10 أرقام
MCC/ MNC الحالية	انظر "SIM MCC/MNC"
SIM MCC/MNC	رمز البلد المتنقل هو مُعرِّف قطري محدد، وضعه الاتحاد الدولي للاتصالات وفقاً للمعيار E.212. يعمل هذا بالاقتران مع رمز شبكة الهاتف المحمول (MNC) لتحديد هوية شبكة الهاتف المحمول. يعني رمز البلد/رمز شبكة الهاتف المحمول الخاص ببطاقة SIM. إذا كنت تقوم بالتجوال في شبكة جوال أخرى، فمن المنطقي أن يكون "MCC/ MNC الحالي" و "MCC/ MNC لشريحة SIM"، مختلفين.

بلوتوث

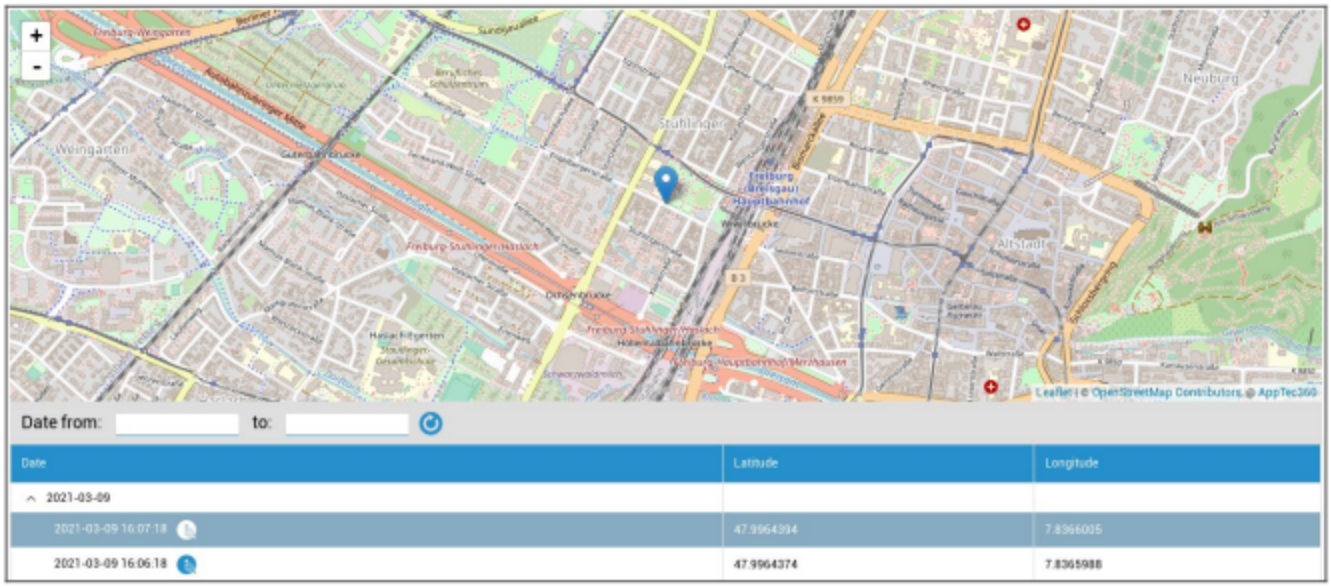
بلوتوث ماك	عنوان MAC للبلوتوث

إدارة الأمن

مكافحة السرقة (على مستوى الجهاز فقط)

معلومات GPS (على مستوى الجهاز فقط)

هنا يمكنك تحديد موقع الجهاز الحالي/الأخير. يمكن حماية تحديد الموقع باستخدام كلمة مرور واحدة أو حتى كلمتي مرور - انظر: الإعدادات العامة - الخصوصية - الوصول إلى نظام تحديد المواقع العالمي (GPS)



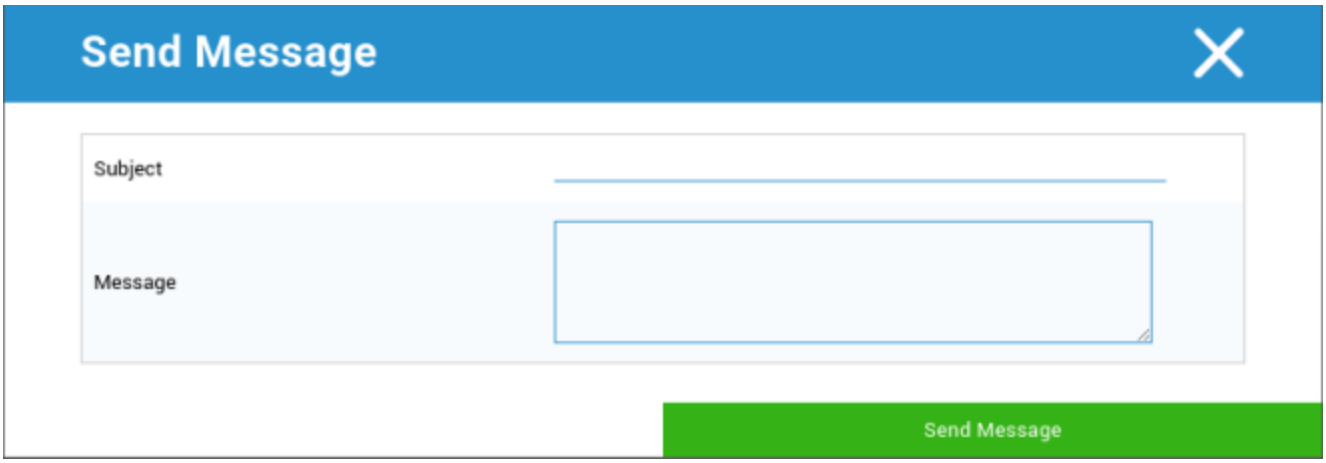
المسح والقفل (على مستوى الجهاز فقط)

ضمن "المسح والقفل"، يمكنك تنفيذ الإجراءات الثلاثة التالية:

مسح كامل	تتم استعادة الجهاز مرة أخرى إلى إعدادات المصنع (يتم حذف بيانات الشركة وكذلك البيانات الشخصية). يعمل فقط مع ملف تعريف العمل المحسّن
مسح المؤسسات	تتم إزالة بيانات الشركة فقط من جهاز المستخدم النهائي (جميع التطبيقات والبيانات وما إلى ذلك التي تم توفيرها بواسطة AppTec)
قفل الشاشة	يتم تنشيط قفل الشاشة، ويكفي إلغاء قفل الجهاز باستخدام كلمة مرور الجهاز/رقم التعريف الشخصي

الرسالة (على مستوى الجهاز فقط)

هنا يمكنك ملء الموضوع والرسالة وإرسالها إلى جهاز المستخدم النهائي



تهيئة الأمان

رمز مرور الجهاز

تحت "رمز المرور" يمكنك تفويض كلمة مرور الجهاز، وتتوفر لك خيارات الإعداد التالية

الحد الأدنى لطول كلمة المرور	ينشئ، الحد الأدنى لعدد الرموز التي يجب أن تحتويها كلمة المرور	
جودة كلمة المرور	غير محدد	لا تتضمن هذه السياسة أي متطلبات لكلمة المرور.
	البيومترية ضعيفة	تسمح هذه السياسة بتكنولوجيا التعرف البيومترية منخفضة الأمان. وهذا يعني التقنيات التي يمكن أن تتعرف على هوية الفرد إلى حوالي 3 أرقام من رقم التعريف الشخصي (الكشف الخاطئ أقل من 1 من كل 1000).
	شيء ما	تتطلب هذه السياسة تعيين نوع من كلمة المرور أو النمط الذي يجب تعيينه، ولكنها لا تفرض أي قواعد محددة.
	حروف الهجاء	يجب أن يكون المستخدم قد أدخل كلمة مرور تحتوي على الأقل على أحرف أبجدية (أو رموز أخرى).
	أبجدي رقمي	يجب أن يكون المستخدم قد أدخل كلمة مرور تحتوي على الأقل على كل من الأحرف الرقمية والأبجدية (أو رموز أخرى).
	مجمع	يجب أن يكون المستخدم قد أدخل كلمة مرور تحتوي على الأقل على حرف ورقم عددي ورمز خاص، بشكل افتراضي. باستخدام هذه النوعية من كلمات المرور، يمكن تقييد كلمات المرور بحيث تحتوي على مجموعات مختلفة من الأحرف، مثل حرف كبير على الأقل، إلخ.
الحد الأدنى لطول كلمة المرور	قم بتعيين عدد الأحرف المطلوبة لكلمة المرور. على سبيل المثال، يمكنك أن تطلب أن يكون رقم التعريف الشخصي أو كلمات المرور ستة أحرف على الأقل.	
الحد الأدنى من الأرقام العددية المطلوبة في كلمة المرور	الحد الأدنى من الأرقام العددية المطلوبة في كلمة المرور	
الحد الأدنى من الأحرف الصغيرة المطلوبة في كلمة المرور	الحد الأدنى من الأحرف الصغيرة المطلوبة في كلمة المرور	
الحد الأدنى من الأحرف الكبيرة المطلوبة في كلمة المرور	الحد الأدنى من الأحرف الكبيرة المطلوبة في كلمة المرور	
الحد الأدنى من الأحرف غير	الحد الأدنى من الأحرف غير الأحرف المطلوبة في كلمة المرور	

المطلوبة في كلمة المرور	
الحد الأدنى من الرموز المطلوبة في كلمة المرور	الحد الأدنى من الرموز المطلوبة في كلمة المرور

الحد الأقصى لقفل وقت عدم النشاط	الحد الأقصى لعدم نشاط المستخدم حتى قفل الوقت
مهلة انتهاء صلاحية كلمة المرور	ينشأ، وبعد هذه الفترة الزمنية تنتهي صلاحية كلمة المرور ويجب إصدار كلمة مرور جديدة
تقييد سجل كلمات المرور	عدد كلمات المرور المستخدمة سابقاً غير المسموح بها
الحد الأقصى لمحاولات كلمة المرور الفاشلة	يحدد، كم مرة يمكن إدخال كلمة مرور بشكل غير صحيح، قبل أن يتم إجراء مسح كامل للجهاز
السماح بالمصادقة البيومترية	تمكين المصادقة عبر بصمة الإصبع أو مسح قزحية العين. فقط لنظام Samsung KNOX 2.1 والإصدارات الأحدث

رمز مرور الحاوية

تحت "رمز المرور" يمكنك تفويض كلمة مرور الحاوية، وخيارات الإعداد التالية متاحة لك

الحد الأدنى لطول كلمة المرور	ينشئ، الحد الأدنى لعدد الرموز التي يجب أن تحتويها كلمة المرور	
جودة كلمة المرور	غير محدد	لا تتضمن هذه السياسة أي متطلبات لكلمة المرور.
	البيومترية ضعيفة	تسمح هذه السياسة بتكنولوجيا التعرف البيومترية منخفضة الأمان. وهذا يعني التقنيات التي يمكن أن تتعرف على هوية الفرد إلى حوالي 3 أرقام من رقم التعريف الشخصي (الكشف الخاطئ أقل من 1 من كل 1000).
	شيء ما	تتطلب هذه السياسة تعيين نوع من كلمة المرور أو النمط الذي يجب تعيينه، ولكنها لا تفرض أي قواعد محددة.
	حروف الهجاء	يجب أن يكون المستخدم قد أدخل كلمة مرور تحتوي على الأقل على أحرف أبجدية (أو رموز أخرى).
	أبجدي رقمي	يجب أن يكون المستخدم قد أدخل كلمة مرور تحتوي على الأقل على كل من الأحرف الرقمية والأبجدية (أو رموز أخرى).
	مجمع	يجب أن يكون المستخدم قد أدخل كلمة مرور تحتوي على الأقل على حرف ورقم عددي ورمز خاص، بشكل افتراضي. باستخدام هذه النوعية من كلمات المرور، يمكن تقييد كلمات المرور بحيث تحتوي على مجموعات مختلفة من الأحرف، مثل حرف كبير على الأقل، إلخ.
الحد الأدنى لطول كلمة المرور	قم بتعيين عدد الأحرف المطلوبة لكلمة المرور. على سبيل المثال، يمكنك أن تطلب أن يكون رقم التعريف الشخصي أو كلمات المرور ستة أحرف على الأقل.	
الحد الأدنى من الأرقام العددية المطلوبة في كلمة المرور	الحد الأدنى من الأرقام العددية المطلوبة في كلمة المرور	
الحد الأدنى من الأحرف الصغيرة المطلوبة في كلمة المرور	الحد الأدنى من الأحرف الصغيرة المطلوبة في كلمة المرور	
الحد الأدنى من الأحرف الكبيرة المطلوبة في كلمة المرور	الحد الأدنى من الأحرف الكبيرة المطلوبة في كلمة المرور	

الحد الأدنى من الأحرف غير الأحرف المطلوبة في كلمة المرور	الحد الأدنى من الأحرف غير الأحرف المطلوبة في كلمة المرور
الحد الأدنى من الرموز المطلوبة في كلمة المرور	الحد الأدنى من الرموز المطلوبة في كلمة المرور

الحد الأقصى لقفل وقت عدم النشاط	الحد الأقصى لعدم نشاط المستخدم حتى قفل الوقت
مهلة انتهاء صلاحية كلمة المرور	ينشأ، وبعد هذه الفترة الزمنية تنتهي صلاحية كلمة المرور ويجب إصدار كلمة مرور جديدة
تقييد سجل كلمات المرور	عدد كلمات المرور المستخدمة سابقاً غير المسموح بها
الحد الأقصى لمحاولات كلمة المرور الفاشلة	يحدد، كم مرة يمكن إدخال كلمة مرور بشكل غير صحيح، قبل أن يتم إجراء مسح كامل للجهاز

مضاد الفيروسات

المسح التلقائي	تمكين عمليات الفحص التلقائي الدورية
فترة المسح الضوئي	الفترة الفاصلة للفحص (سريع / كامل)
المسح التلقائي الكامل	تمكين الفحص التلقائي الكامل
التحديثات التلقائية	تمكين التحديثات التلقائية
تحديث فترة التحقق من التحديث	كم مرة يجب تحديث التطبيق وقاعدة البيانات الخاصة به (الفيروسات / التعليمات البرمجية التالفة)
حماية التطبيق	تمكين الفحص التلقائي للتطبيق
حماية بطاقة SD	تمكين الفحص التلقائي لبطاقة SD
تحديث Wi-Fi فقط	عند التمكين، لن يتم تطبيق التحديثات إلا عند اتصال الجهاز بشبكة Wi-Fi بنجاح

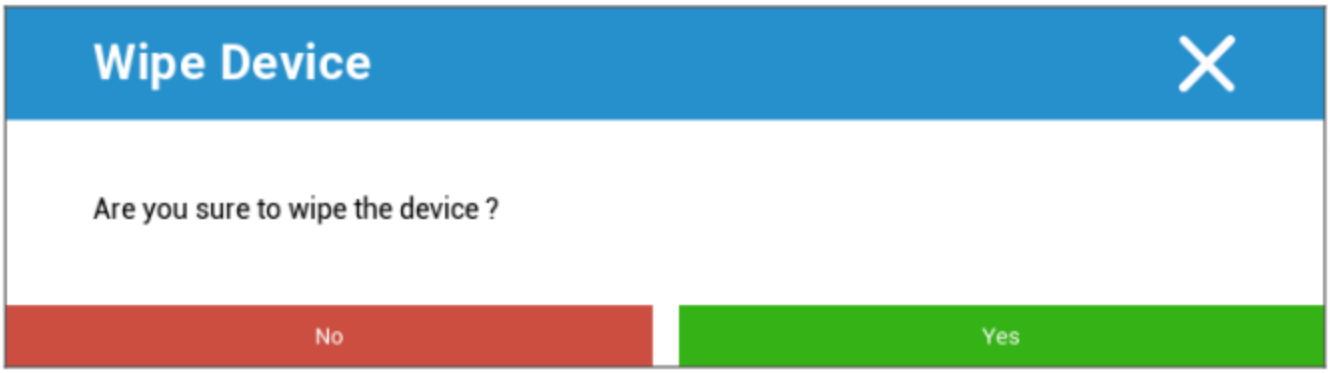
نهاية العمر الافتراضي (على مستوى الجهاز فقط)

المسح (على مستوى الجهاز فقط)

ضمن "المسح"، يمكنك استعادة الجهاز إلى إعدادات المصنع (فقط في ملف تعريف العمل المحسّن).

هنا سيتم حذف بيانات الشركة وكذلك البيانات الخاصة على جهاز المستخدم النهائي.

بالنقر على "رمز الطرح" تتلقى الرسالة التالية:



باستخدام "نعم" يمكنك إجراء المسح.

تحت عنوان "تقرير المسح" يمكن عرض العناصر التالية

ممسوح بواسطة	تاريخ من قام بالمسح
التاريخ	التاريخ
الحالة	الحالة (على سبيل المثال، إذا تم إجراء المسح بنجاح)

إعدادات التقييد

القيود

هنا، يمكن تقييد وحظر مجموعة متنوعة من الأشياء.

إنفاذ الامتثال	وضع مطالبة المستخدم - سيُطلب من المستخدم تنفيذ الإجراءات اللازمة. حاوية قفل الوضع - إخفاء جميع التطبيقات حتى يتم استيفاء جميع المتطلبات
سياسة إذن وقت التشغيل	مطالبة المستخدم بطلبات الأذونات الجديدة منح طلبات الإذن الجديدة الجديدة دائماً رفض طلبات الإذن الجديدة دائمًا تحذير: تواجه بعض التطبيقات مشاكل في التعرف على الأذونات إذا تم تعيينها تلقائياً. إذا كنت تمنح الأذونات دائمًا وواجهت مشاكل مع التطبيقات التي تقول أن الأذونات مفقودة، فقم بتعيين هذا على "مطالبة المستخدم" وأعد تثبيت التطبيق
السماح بالحافظة الصادرة	يسمح بالنسخ واللصق من داخل الحاوية إلى خارجها
السماح بتحديد هوية المتصل	إظهار اسم المكالمة الواردة بناءً على جهات الاتصال في الحاوية
السماح بالبحث عن جهة الاتصال القرار	يسمح بالبحث عن الأسماء في جهات اتصال الحاوية عند إجراء المكالمات
السماح بمشاركة جهات اتصال Bluetooth	يسمح بالوصول إلى حاوية الاتصال في السيارة
عدم السماح بشعاع NFC الصادر	تعطيل NFC للحاوية
السماح بمصادر غير معروفة	في حالة التمكين، يمكن للمستخدمين تحميل التطبيقات بشكل جانبي عن طريق تثبيت ملف .apk.
السماح بتصحيح أخطاء USB	إذا تم تمكينه، يمكن للمستخدمين تمكين تصحيح أخطاء USB.
عدم السماح بتعديل الحساب	عدم السماح بإنشاء حسابات في الحاوية وحذفها وتعديلها في الحاوية ضع في اعتبارك أن بعض التطبيقات تحتاج إلى إنشاء حسابات أو تعديلها لتعمل كما هو متوقع

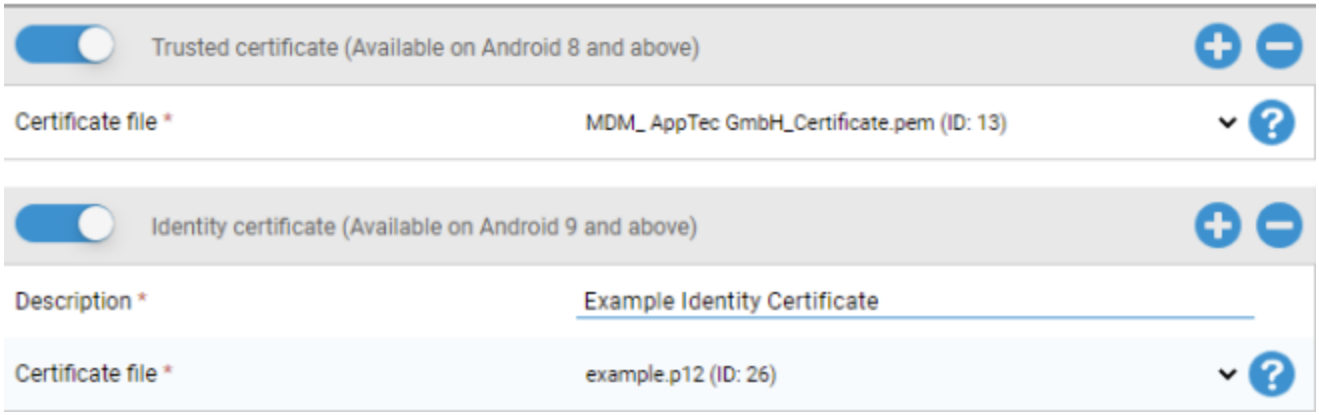
قيود ملف تعريف العمل. متوفر فقط على الأجهزة التي تعمل بنظام Android 11 والإصدارات الأحدث، مع ملف تعريف العمل المحسّن	
تعطيل الكاميرا	يحدد ما إذا كانت الكاميرا غير مسموح بها في ملف تعريف العمل.

عدم السماح بالبلوتوث	يحدد ما إذا كان البلوتوث غير مسموح به في ملف تعريف العمل.
تمكين حماية إعادة ضبط المصنع	قم بتنشيط هذا لتجاوز حماية إعادة ضبط المصنع لنظام Android إلى حساب Google الذي قمت بتحديده في "الإعدادات العامة" → "تكوين Android Enterprise" → "Android" → "حماية إعادة ضبط المصنع" إذا تم تمكين هذا الأمر وقمت بإعادة ضبط الجهاز، فسيتعين عليك تقديم حساب Google المكوّن لإعداد الجهاز مرة أخرى.
تحديث نظام التحكم في نظام التشغيل	قم بتمكين هذا لتعيين سلوك التحديث إلى تلقائي أو مؤجل أو مؤجل.
تحديث السياسة	تلقائي: يتم التثبيت تلقائياً بمجرد توفر تحديث. نافذ: التثبيت التلقائي ضمن نافذة الصيانة اليومية. يؤدي هذا أيضًا إلى تكوين تطبيقات Play ليتم تحديثها داخل النافذة. يوصى بهذا بشدة لأجهزة الأكشاك لأن هذه هي الطريقة الوحيدة التي يمكن من خلالها تحديث التطبيقات المثبتة باستمرار في المقدمة بواسطة Play. التأجيل: تأجيل التثبيت التلقائي بحد أقصى 30 يومًا.

قيود الملف الشخصي الشخصي. متوفر فقط على أجهزة Android 11 والإصدارات الأحدث، مع ملف تعريف العمل المحسّن	
تعطيل الكاميرا	يحدد ما إذا كانت الكاميرا غير مسموح بها في الملف الشخصي.
عدم السماح بالبلوتوث	يحدد ما إذا كان البلوتوث غير مسموح به في الملف الشخصي.
السماح بمصادر غير معروفة	في حالة التمكين، يمكن لمستخدمي ملف تعريف العمل تحميل التطبيقات بشكل جانبي عن طريق تثبيت ملف .apk.

إدارة الشهادات

هنا يمكنك توزيع الشهادات الموثوقة وشهادات الهوية على أجهزتك. مطلوب Android 8 أو أعلى لتوزيع الشهادات الموثوقة و Android 9 أو أعلى لتوزيع شهادات الهوية.



باستخدام "+" يمكنك إضافة شهادات متعددة.

يجب أن تكون الشهادات الموثوقة بتنسيق PEM.

يجب أن تكون شهادات الهوية بتنسيق PKCS12.

إدارة الاتصال

الواي فاي

بالنسبة لهذا الإعداد، قم بإجراء التهيئة المسبقة لأجهزة المستخدم النهائي، للوصول إلى نقاط الوصول الداخلية

معرّف مجموعة الخدمات (SSID)	SSID للشبكة التي سيتم الاتصال بها
الشبكة الخفية	تنشيط، في حالة عدم قيام نقطة الوصول إلى نقطة الوصول ببث SSID

نوع الأمان

إنشاء نوع أمان نقطة الوصول

WEP

كلمة المرور	كلمة المرور الخاصة بـ AP

WPA/WPA2

كلمة المرور	كلمة المرور الخاصة بـ AP

802.1x EAP 802.1x

طريقة EAP-Method

الأشخاص ذوو الإعاقة	الهوية	الهوية
	كلمة المرور	كلمة المرور

PEAP	بروتوكول المصادقة في المرحلة 2	لا شيء	لا يوجد بروتوكول إضافي
		MSCHAPV2	بروتوكول MSCHAPV2
		GTC	بروتوكول GTC
	شهادة المرجع المصدق (CA)	شهادة المرجع المصدق (CA)	
	الهوية	الهوية	
	هوية مجهولة	هوية مجهولة	
	كلمة المرور	كلمة المرور	

TTLS	بروتوكول المصادقة في المرحلة 2	لا شيء	لا يوجد بروتوكول إضافي
		برنامج مساعدة الشعب الفلسطيني	بروتوكول PAP
		MSCHAP	بروتوكول MSCHAP
		MSCHAPV2	بروتوكول MSCHAPV2
		GTC	بروتوكول GTC
	شهادة المرجع المصدق (CA)	شهادة المرجع المصدق (CA)	
	الهوية	الهوية	
	هوية مجهولة	هوية مجهولة	
	كلمة المرور	كلمة المرور	

TLS	شهادة المرجع المصدق (CA)	شهادة المرجع المصدق (CA)
	الهوية	الهوية
	كلمة المرور	كلمة المرور

VPN

اسم الاتصال	اسم اتصال VPN

نوع VPN

VPN

عميل VPN

عميل AppTec VPN	
تكوين البوابة	حدد تكوين الشبكة الخاصة الافتراضية للبوابة (انظر **الإعدادات العامة > البوابة العامة > إعدادات الشبكة الخاصة الافتراضية**)
دائماً على VPN	تمكين الإغلاق الأصلي
تمكين تأمين AppTec Lockdown	تمكين تأمين AppTec Lockdown

مدمج (متوفر فقط على أجهزة سامسونج)			
نوع الاتصال	PPTP	الخادم	الخادم
		تمكين تشفير PPTP PPTP	تمكين تشفير PPTP PPTP
	L2TP / IPSec PSK	الخادم	الخادم
		المفتاح المشترك المسبق IPSec	المفتاح المشترك المسبق IPSec
		تمكين L2TP سري L2TP	تمكين L2TP سري L2TP
		L2TP سري L2TP	L2TP سري L2TP
	IPSec XAuth PSK	الخادم	الخادم
		معرّف IPSec	معرّف IPSec
		المفتاح المشترك المسبق IPSec	المفتاح المشترك المسبق IPSec
نطاقات بحث DNS	نطاقات بحث DNS		
إعدادات الخبراء	خوادم DNS	خوادم DNS	
	مسارات إعادة التوجيه	مسارات إعادة التوجيه	

فتح VPN			
الخادم	الخادم		
ملف تعريف OpenVPN	ملف تعريف OpenVPN		
تطبيق OpenVPN	OpenVPN للأندرويد (موصى به)		
	اتصال OpenVPN		
إعدادات الخبراء	خوادم DNS	خوادم DNS	
	مسارات إعادة التوجيه	مسارات إعادة التوجيه	

سامسونج / سترونج سوان			
نوع الاتصال	PPTP	الخادم	الخادم
		اسم المستخدم	اسم المستخدم
		كلمة المرور	كلمة المرور
		تمكين تشفير PPTP PPTP	تمكين تشفير PPTP PPTP
	L2TP / IPSec PSK	الخادم	الخادم
		المفتاح المشترك المسبق IPSec	المفتاح المشترك المسبق IPSec
		اسم المستخدم	اسم المستخدم
		كلمة المرور	كلمة المرور
		تمكين L2TP سري L2TP	L2TP سري L2TP
	IPSec XAuth PSK	الخادم	الخادم
		معرّف IPSec	معرّف IPSec
		المفتاح المشترك المسبق IPSec	المفتاح المشترك المسبق IPSec
		اسم المستخدم	اسم المستخدم
		كلمة المرور	كلمة المرور
إعدادات الخبراء	خوادم DNS	خوادم DNS	
	مسارات إعادة التوجيه	مسارات إعادة التوجيه	

Cisco Any Connect من Cisco Any Connect		
الخادم	الخادم	
وضع الشهادة	معاق	معاق
	أوتوماتيكي	أوتوماتيكي
إعدادات الخبراء	خوادم DNS	خوادم DNS
	مسارات إعادة التوجيه	مسارات إعادة التوجيه

لكل تطبيق VPN

عميل VPN

عميل AppTec VPN		
تكوين البوابة	حدد تكوين الشبكة الخاصة الافتراضية للبوابة (انظر **الإعدادات العامة > البوابة العامة > إعدادات الشبكة الخاصة الافتراضية**)	
تطبيقات VPN	تطبيقات VPN	
دائماً على VPN	تمكين الإغلاق الأصلي	دائماً على VPN
تمكين تأمين AppTec Lockdown	تمكين تأمين AppTec Lockdown	

سامسونج / سترونج سوان			
نوع الاتصال	PPTP	الخادم	الخادم
		تطبيقات VPN	تطبيقات VPN
		اسم المستخدم	اسم المستخدم
		كلمة المرور	كلمة المرور
		تمكين تشفير PPTP PPTP	تمكين تشفير PPTP PPTP
	L2TP / IPSec PSK	الخادم	الخادم
		تطبيقات VPN	تطبيقات VPN
		المفتاح المشترك المسبق IPSec	المفتاح المشترك المسبق IPSec
		اسم المستخدم	اسم المستخدم
		كلمة المرور	كلمة المرور
		تمكين L2TP سري L2TP	L2TP سري L2TP
	IPSec XAuth PSK	الخادم	الخادم
		تطبيقات VPN	تطبيقات VPN
		معرّف IPSec	معرّف IPSec
		المفتاح المشترك المسبق IPSec	المفتاح المشترك المسبق IPSec
		اسم المستخدم	اسم المستخدم
		كلمة المرور	كلمة المرور
إعدادات الخبراء	خوادم DNS	خوادم DNS	
	مسارات إعادة التوجيه	مسارات إعادة التوجيه	

القيود

يمكنك هنا تعيين القيود، فيما يتعلق بإدارة الاتصال، فيما يتعلق بإدارة الاتصال

السماح بتجوال البيانات	السماح ببيانات الجوال أثناء التجوال
فرض تجوال البيانات	إذا تم تفعيله، يتم تفعيل التجوال لبيانات الهاتف المحمول بشكل دائم (غير مستحسن!) يحل هذا الإعداد محل إعداد "السماح بتجوال البيانات"!
استخدام النظام خادم وكيل http النظام البروكسي	يعتمد استخدام خادم وكيل HTTP، الذي توفره إعدادات النظام في الإعدادات، على الشبكة المتصلة (WiFi أو APN)

إدارة PIM

Gmail Exchange

معلومات: سيتم تطبيق هذا التكوين على تطبيق Gmail. لذا عليك الموافقة على Gmail وتثبيته.

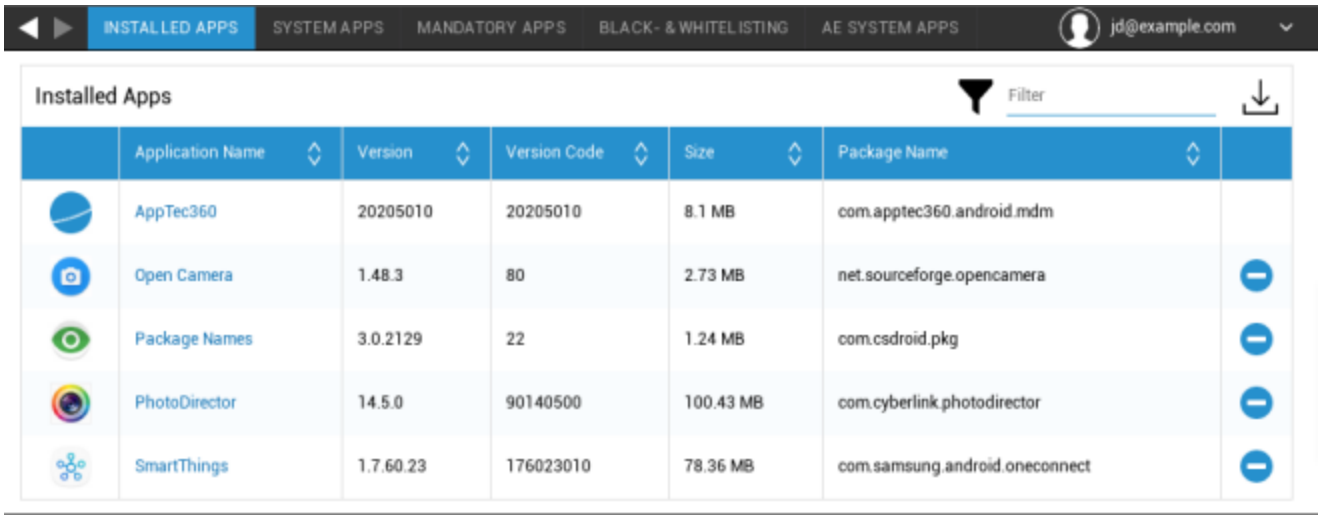
عنوان البريد الإلكتروني	عنوان البريد الإلكتروني للمستخدم المقدم يرجى ملاحظة "العناصر النائبة"، التي يمكنك استخدامها للعمل مع بيانات الاعتماد ولا تقوم بإجراء تغييرات يدوياً على كل جهاز بنقرة واحدة على يمكنك عرضها بنفسك
اسم مضيف الخادم	عنوان الخادم الخاص بخوادم Exchange الخاصة بك
اسم تسجيل الدخول	اسم تسجيل الدخول لجهاز المستخدم النهائي المعني، يرجى أيضًا ملاحظة "العناصر النائبة هنا
التوقيع	يمكن إرفاق توقيع (تلميح: تتطلب بعض الأجهزة تنسيق HTML للتوقيع)
عدد الأيام السابقة للمزامنة	عدد الأيام التي يتم فيها تحديد موعد مزامنة رسائل البريد الإلكتروني
معرّف الجهاز	سلسلة EAS DeviceID التي يتضمنها EAS DeviceID. هذه السلسلة هي جزء من بروتوكولات EAS وتوجد في بعض الأقاليم الأصلية
استخدام طبقة مآخذ التوصيل الآمنة (SSL)	استخدام اتصال SSL
قبول جميع الشهادات	جميع الشهادات مقبولة. الرجاء تحديد هذا الخيار، إذا كان خادم Exchange لديك يستخدم شهادة موقعة ذاتياً
السماح بالحسابات غير المُدارة	السماح للمستخدمين بإضافة أو إزالة أي حساب Exchange، بخلاف الحساب المحدد في هذا التكوين المُدار. إذا تم تمكين هذا الإعداد، لا يمكنك منع المستخدمين من إضافة حسابات Exchange أخرى إلى Gmail. كما لا يمكنك التحكم في مشاركة البيانات بين التطبيقات الأخرى وحسابات Exchange التي يضيفها المستخدمون. يجب تمكين هذا الإعداد فقط إذا كان المستخدمون لديك بحاجة إلى الاحتفاظ بأكثر من حساب تبادل عمل واحد في Gmail.
شهادة العميل	شهادة العميل. مطلوبة فقط إذا كان خادم البريد الخاص بك يتوقع وجودها.

إدارة التطبيقات

مدير تطبيقات المؤسسات

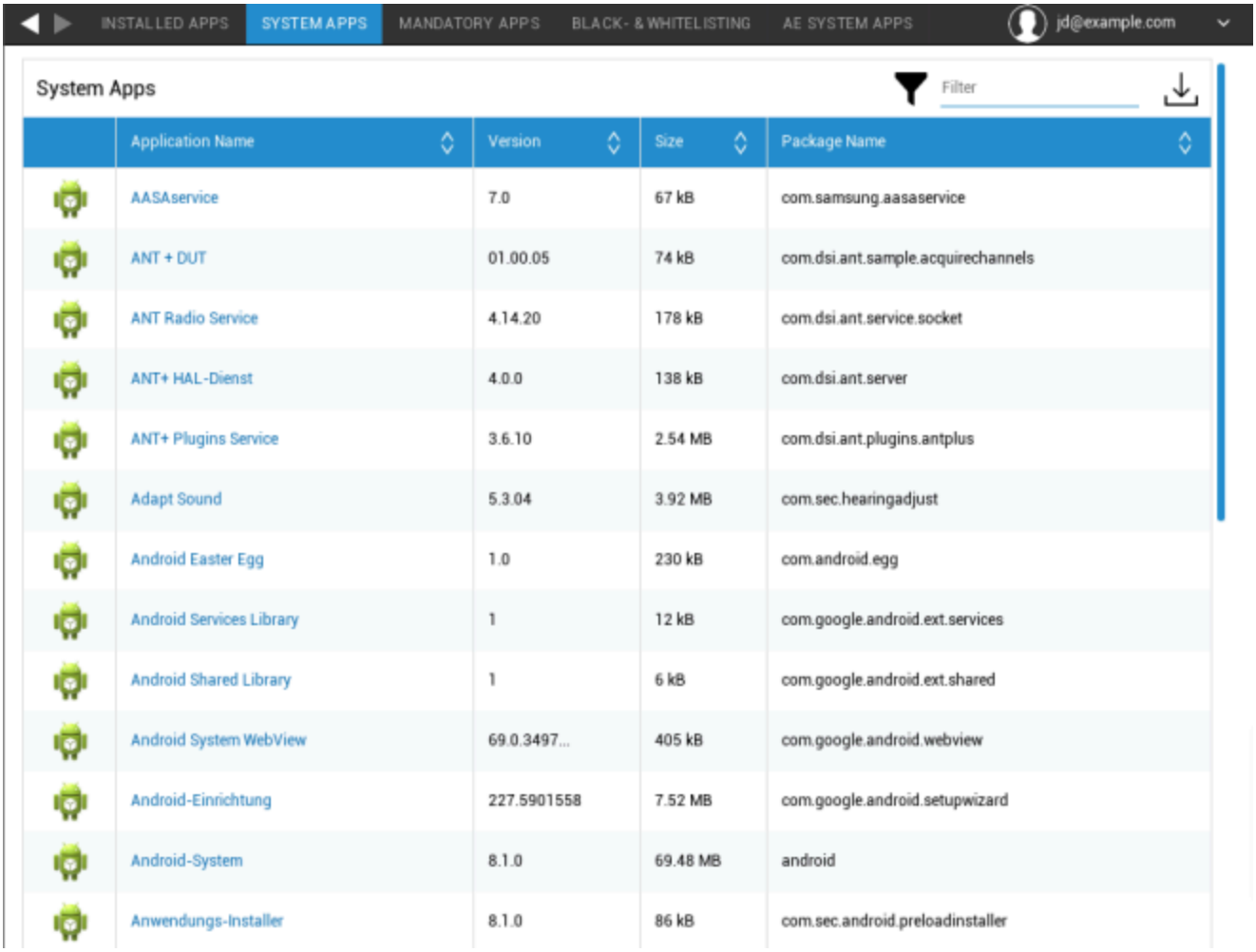
التطبيقات المثبتة (على مستوى الجهاز فقط)

هنا سيتم عرض جميع التطبيقات المثبتة حاليًا في الحاوية لك.



تطبيقات النظام (على مستوى الجهاز فقط)

تحت عنوان "تطبيقات النظام"، سيتم إدراج جميع التطبيقات والخدمات التي تم تثبيتها بالفعل على جهاز المستخدم النهائي من قبل الشركة المصنعة للجهاز.

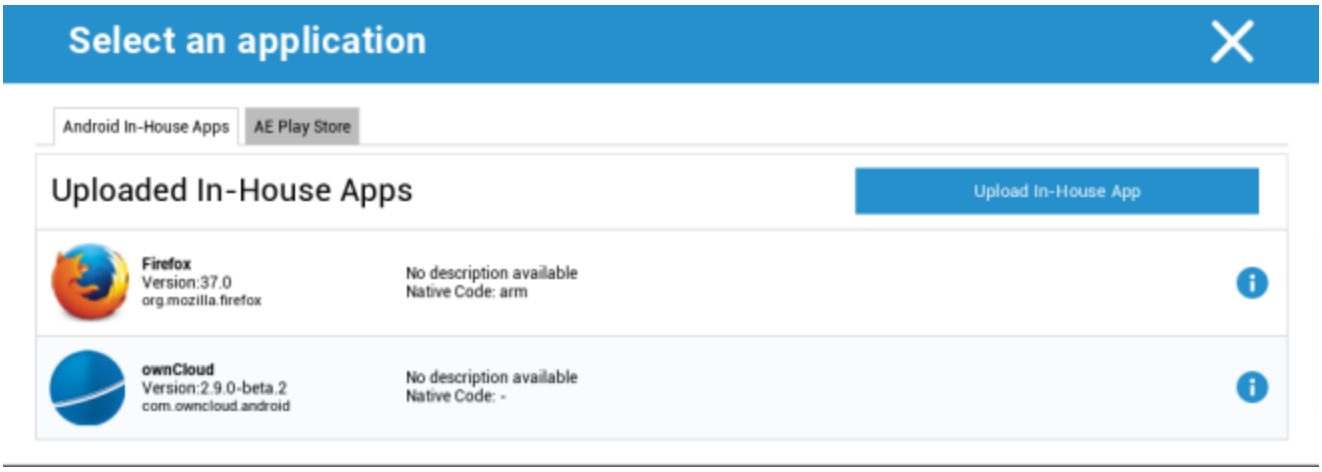


التطبيقات الإلزامية

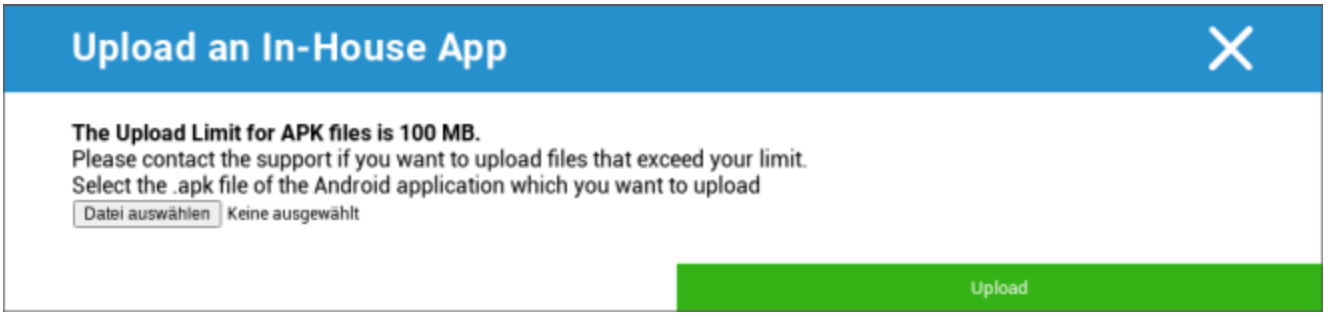
ضمن التطبيقات الإلزامية، يمكنك إنشاء التطبيقات المطلوبة الإلزامية. سيُطلب من المستخدم باستمرار تثبيت هذا التطبيق المخصص، إذا كان تطبيقًا داخليًا. سيتم تثبيت تطبيقات متجر Play Store تلقائيًا.

من خلال، يمكن تعريف التطبيق المطلوب الإلزامي المطلوب.

يمكن أن يكون هذا تطبيقًا داخليًا من "تطبيقات Android الداخلية"، والتي قمت بتحميلها في الإعدادات العامة.

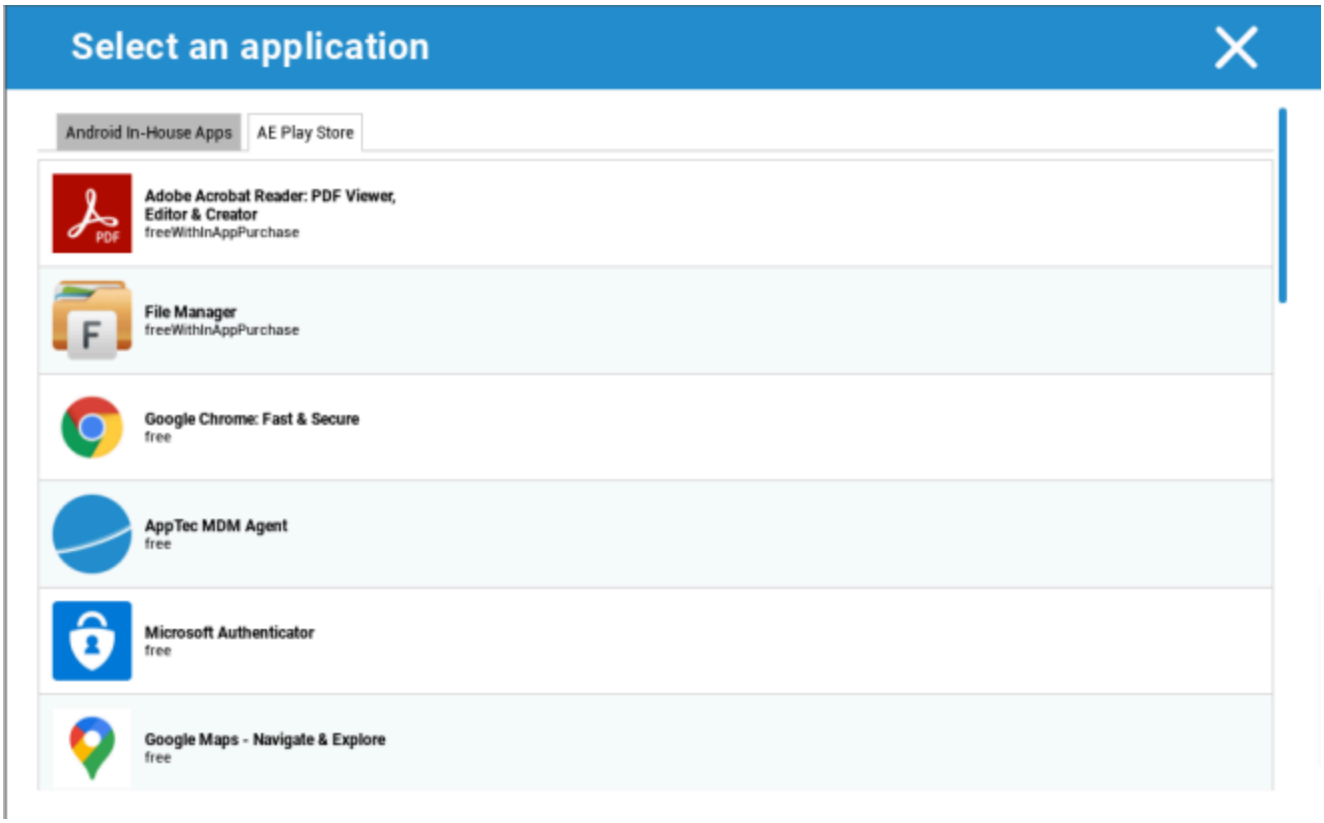


يمكنك أيضًا تحديد ملف apk وتحميله مباشرةً باستخدام "تحميل تطبيق داخلي".



إذا كنت تقوم بتثبيت تطبيق داخلي، سيكون لديك إمكانية تنشيط "التحديث المستمر". إذا تم تفعيل ذلك وقمت بتحديد إصدار أحدث في قاعدة بيانات التطبيق الداخلي، فسيتم تحديث التطبيق على الجهاز.

أو يمكن أن يكون تطبيق "AE Play Store" من متجر Google Work Play Store.



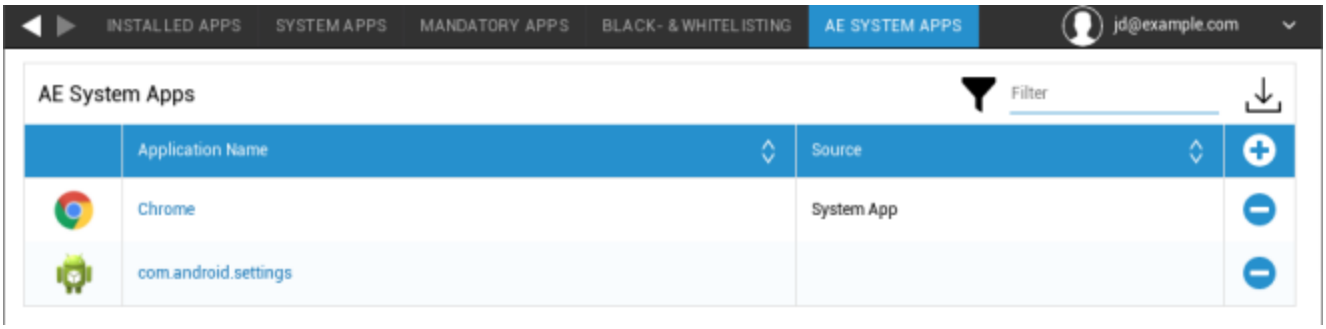
سيتم عرض "تطبيقات AE Play Store" المعتمدة فقط في علامة التبويب هذه.

للموافقة على "تطبيق AE Play Store" يرجى الانتقال إلى "الإعدادات العامة"> "إدارة التطبيقات"> "AE Play المتجر" وإضافة تطبيق عبر الزر الذي سيعيد توجيهك إلى علامة التبويب "تطبيقات متجر Play" (أو يمكنك الانتقال مباشرةً إلى علامة التبويب "تطبيقات متجر Play").

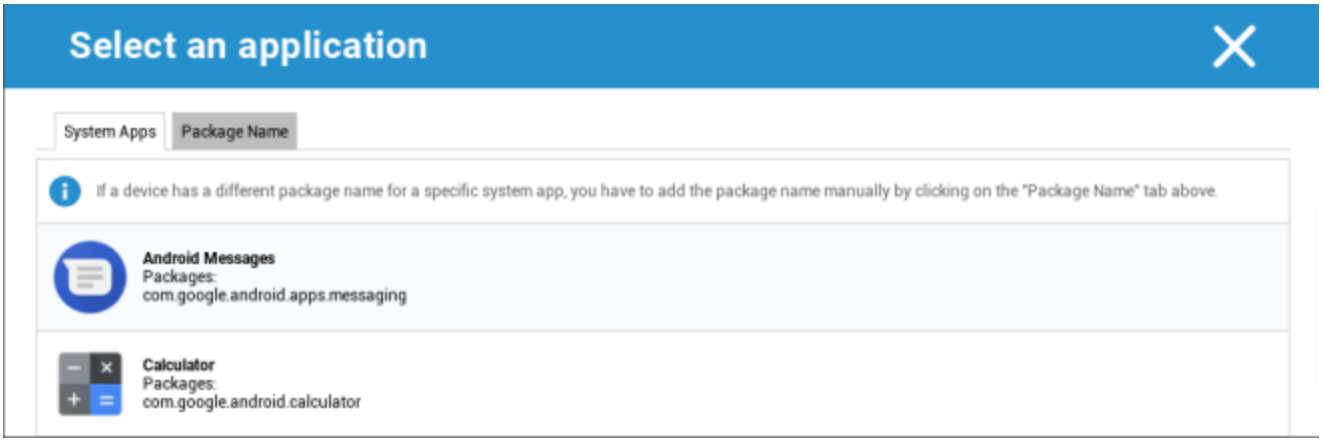
في علامة التبويب "تطبيقات متجر Play Store" يمكنك البحث عن التطبيقات. عند النقر على أحد التطبيقات، تُفتح صفحة التطبيق، وهنا يمكنك الموافقة على التطبيق بالنقر على "موافقة".

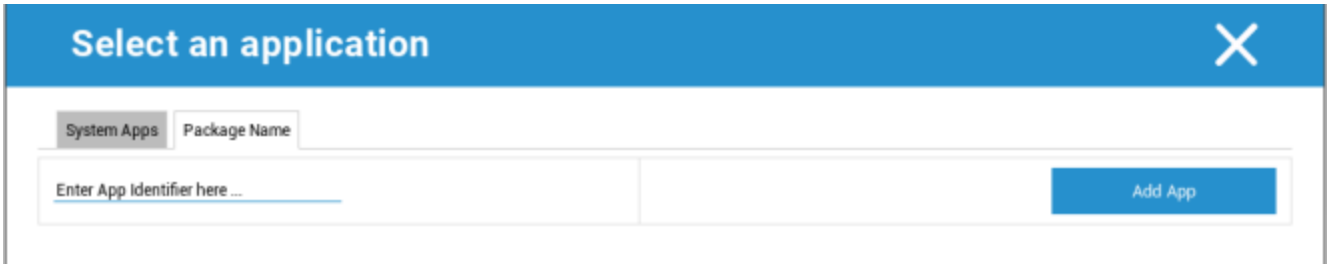
تطبيقات نظام AE

هنا يمكنك تحديد قائمة تحتوي على تطبيقات نظام محددة يجب تفعيلها على الأجهزة.



إذا نقرت على الزر، يمكنك الاختيار من قائمة تطبيقات النظام المحتملة التي توفرها Google أو إدخال اسم حزمة تطبيق النظام الذي يجب تفعيله مباشرةً.





يرجى الأخذ في الاعتبار أن تطبيقات النظام في القائمة المقدمة من Google هي فقط التطبيقات التي يمكن أن تكون تطبيقات نظام، ولكن ليس بالضرورة أن تكون تطبيقات نظام على أجهزتك.

ومع ذلك، فإن هذه القائمة تؤثر فقط على التطبيقات المثبتة مسبقاً فقط.

لن تؤثر إضافة التطبيقات غير المثبتة مسبقًا على أجهزتك على أجهزتك، بغض النظر عما إذا كان التطبيق من القائمة التي توفرها Google أو تم إدخال اسم حزمة التطبيق مباشرةً.

القيود والإعدادات

إعدادات إدارة التطبيق

هنا يمكنك تهيئة سلوك الجهاز فيما يتعلق بتحديثات التطبيق.

تكرار التحقق من التحديث	حدد الفاصل الزمني الذي سيبحث فيه عميل AppTec Client عن تحديثات التطبيق. القيمة الافتراضية هي 24 ساعة.
عتبة الواي فاي	سيتم تنزيل التطبيقات الأكبر من الحجم المحدد عبر Wi-Fi. إذا تم تحديد "Wi-Fi فقط"، فسيتم تنزيل جميع التطبيقات عبر Wi-Fi.

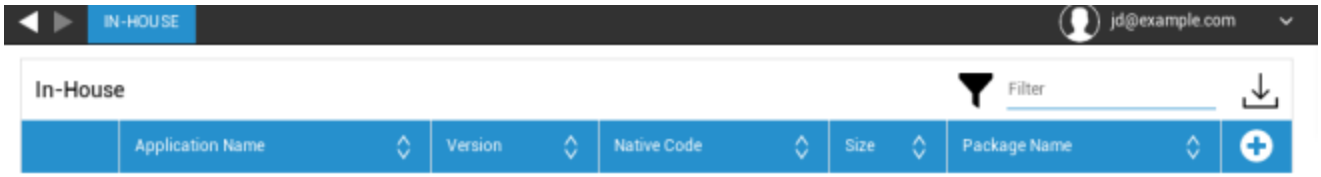
متجر تطبيقات المؤسسات

داخل الشركة

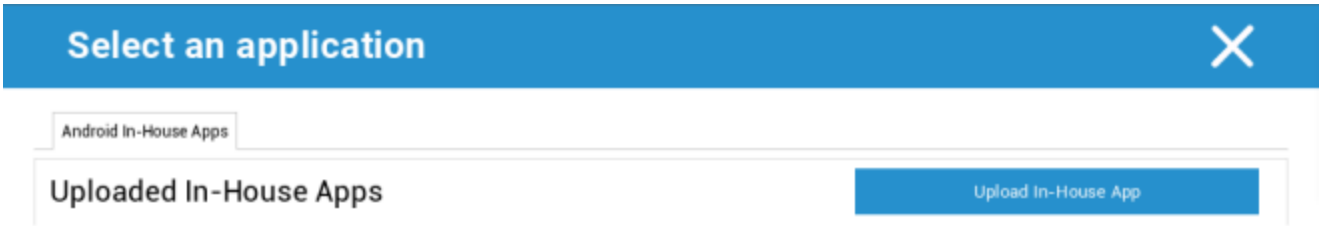
تحت نقطة "داخلياً"، يمكنك تحميل التطبيقات المطورة داخلياً وتوزيعها.

باستخدام الرمز، يمكنك توزيع تطبيقات إضافية داخل الشركة.

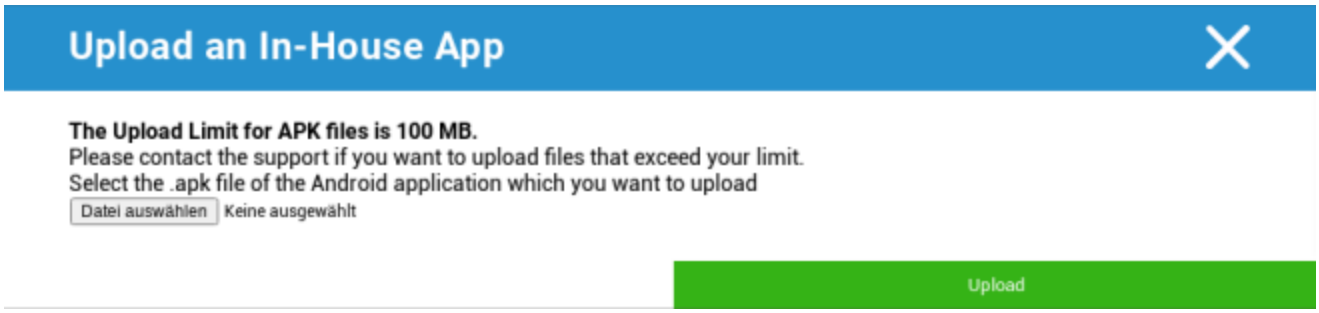
إذا كنت تقوم بتثبيت تطبيق داخلي، سيكون لديك إمكانية تنشيط "التحديث المستمر". إذا تم تفعيل ذلك وقمت بتحديد إصدار أحدث في قاعدة بيانات التطبيق الداخلي، فسيتم تحديث التطبيق على الجهاز.



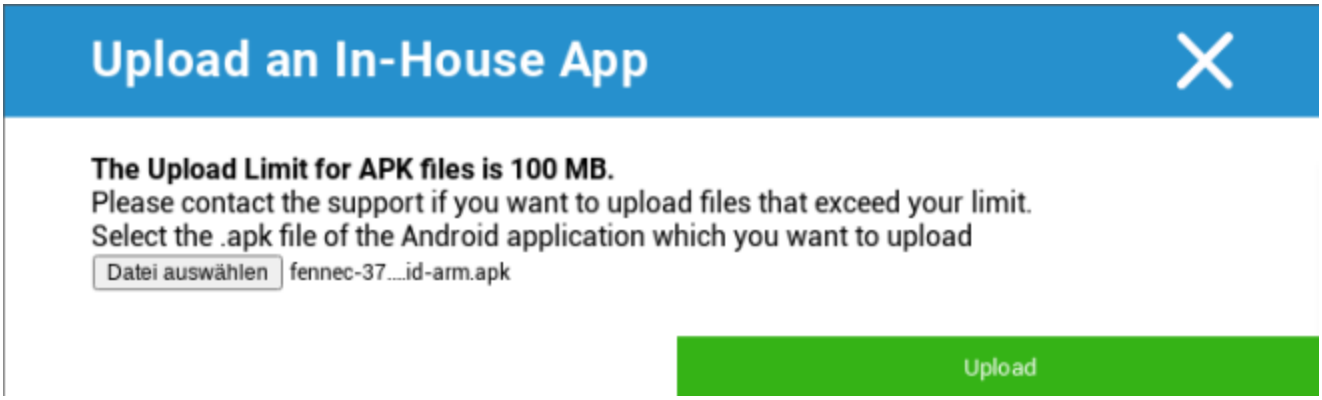
إذا لم تكن قد وزعت تطبيقات داخلية، فستتلقى بعد ذلك النظرة العامة التالية:



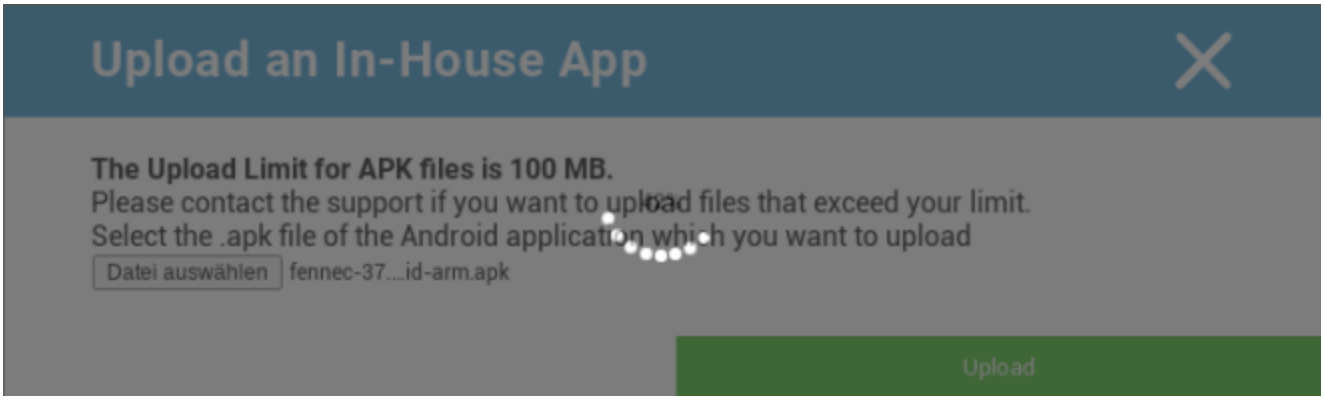
لهذا، انقر على "تحميل تطبيق داخلي"، وستتلقى بعد ذلك النظرة العامة التالية:



الآن، اختر باستخدام "بحث..." ملف .apk ثم انقر على "تحميل".



سيتم الآن تحميل تطبيقك، في منتصف الدائرة سترى مؤشر نسبة مئوية في منتصف الدائرة، يوضح مقدار ما تم تحميله بالفعل من تطبيقك.



في حالة نجاح تحميل تطبيقك الداخلي، يمكنك بعد ذلك العثور على التطبيق الذي تم تحميله في كتالوج التطبيقات.

يتوفر للمستخدم الآن خيار الاطلاع على هذا التطبيق وتثبيته في متجر AppTec على جهاز المستخدم النهائي، تحت فئة "في المنزل".

نظرًا لأن هذا لا يتضمن تطبيق Google PlayStore، لا يحتاج المستخدم إلى معرّف Google مخزّن على جهاز المستخدم النهائي الخاص به.

متجر Play Play للمؤسسات

متجر AE Play

هنا يمكنك إضافة تطبيقات إلى متجر Playstore الخاص بمؤسسات Android. يرجى ملاحظة أنه يجب عليك الموافقة على التطبيقات باستخدام حساب مسؤول AE الخاص بك قبل أن تتمكن من إضافتها.

للموافقة على تطبيق ما يرجى الاطلاع على التعليمات في التطبيقات الإلزامية.

إدارة المحتوى

صندوق المحتوى

هنا يمكنك تنشيط ContentBox.

بمجرد تبديل "تمكين ContentBox" إلى "تشغيل"، سيتم تثبيت تطبيق ContentBox منفصل تلقائياً على جهاز المستخدم النهائي.

متصفح آمن

هنا يمكنك تكوين إعدادات متصفح AppTec Secure Browser.

بمجرد أن تقوم بتبديل القسم في "المتصفح الآمن" إلى "تشغيل"، سيتم تثبيت تطبيق متصفح منفصل تلقائيًا على جهاز المستخدم النهائي.

تتطلب كلمة مرور	مطالبة المستخدم بإعداد كلمة مرور واستخدامها للوصول إلى المتصفح.
الحد الأدنى لطول كلمة المرور المطلوبة	تعيين عدد الأحرف المطلوبة لكلمة المرور
جودة كلمة المرور المطلوبة	تعيين جودة كلمة المرور المطلوبة
تقييد التنزيلات / فتح في	
تقييد التحميلات	
تحميل القائمة البيضاء	قائمة بعناوين URL التي يُسمح بتحميلها دائماً.
السماح بالنسخ	السماح بنسخ النص أو قصه أو مشاركته داخل صفحات الويب.
السماح بالتقاط الشاشة	السماح بالتقاط لقطات الشاشة.
تواتر تنظيف البيانات	حدد التردد الذي يجب إزالة جميع بيانات المستخدم (السجل وذاكرة التخزين المؤقت وما إلى ذلك) تلقائيًا.
الإشارات المرجعية للشركة	ستظهر الإشارات المرجعية في مجلد "الإشارات المرجعية للشركة" في الإشارات المرجعية للمتصفحات. وهي غير قابلة للتحرير من قبل المستخدم.
إخفاء شريط العنوان	
القائمة البيضاء داخل المتصفح (بدون البوابة العالمية)	تمكين القائمة البيضاء لعناوين URL من جانب العميل. • يتم دائمًا إدراج الإشارات المرجعية للشركة في القائمة البيضاء • مدعومة لـ 100 عنوان URL فقط • يرجى استخدام البوابة العالمية لقائمة سوداء وبيضاء غير محدودة
عناوين URL المدرجة في القائمة البيضاء	قائمة بعناوين URL المسموح بها.
القائمة السوداء والقائمة البيضاء المستندة إلى البوابة	تتضمن القائمة السوداء المتطلبات التالية: • بوابة عالمية للتطبيقات من AppTec تعمل ("الإعدادات العامة" → "البوابة العالمية")

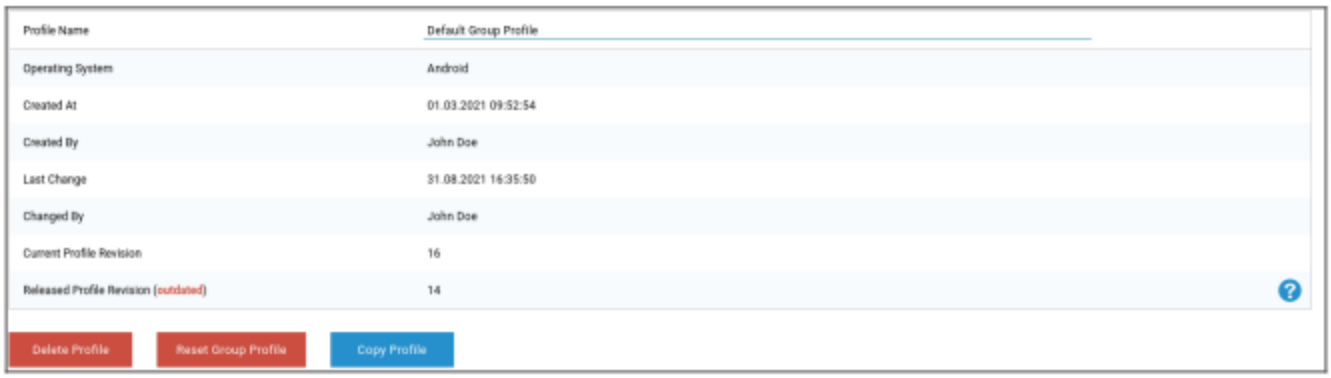
	• تكوين VPN عامل مع خادم DNS محدد ("الإعدادات العامة" → "البوابة العامة" → "إعدادات VPN") • تكوين القائمة السوداء ("الإعدادات العامة" → "البوابة العامة" → "القائمة السوداء للنطاق") • اتصال VPN صالح في ملف التعريف ("إدارة الاتصال" → "VPN")

تهيئة أندرويد

جنرال لواء

نظرة عامة على ملف تعريف المجموعة (على مستوى المجموعة فقط)

عند فتح الملف الشخصي للمجموعة، ستحصل على نظرة عامة سريعة على الملف الشخصي.



اسم الملف الشخصي	اسم الملف الشخصي (يمكن تغييره هنا)
نظام التشغيل	نظام التشغيل الذي تم إنشاء ملف التعريف له
تم إنشاؤها في	وقت الإنشاء
تم إنشاؤها بواسطة	منشئ الملف الشخصي
آخر تغيير	وقت آخر تغيير في الملف الشخصي
تم التغيير بواسطة	الحساب الذي أجرى التغييرات الأخيرة
مراجعة الملف الشخصي الحالي	مراجعة حالة الملف الشخصي المحفوظة
مراجعة الملف الشخصي الصادر	مراجعة الملف الشخصي المعين ("تعيين الآن"). إذا كانت التسمية تظهر "(قديم)" خلف النص، فهذا يعني أنك قمت بحفظ ملف التعريف ولكنك لم تعيّنه بعد، لذا ستظل الأجهزة تحصل على الإصدار الأقدم.

نظرة عامة على الجهاز (على مستوى الجهاز فقط)

في حالة وجودك على أحد الأجهزة، ستتلقى ملخصاً عاماً للجهاز المحدد، ويتضمن ما يلي

اسم الجهاز	اسم الجهاز
آخر موقع معروف	آخر إحداثيات نظام تحديد المواقع العالمي (GPS) المعروفة
رقم الهاتف	رقم الهاتف
التطبيقات الإلزامية المعينة	عدد التطبيقات الإلزامية المخصصة
إصدار نظام التشغيل	إصدار نظام التشغيل الخاص بالجهاز
نظام التشغيل	نظام التشغيل (Android / iOS / Windows Phone)
الرقم التسلسلي	الرقم التسلسلي للجهاز
ملكية الجهاز	جهاز الشركة أو الجهاز الخاص
نوع الجهاز	الهاتف أو الجهاز اللوحي
متجذر	الحالة، التي تشير إلى ما إذا كان الجهاز قد تم تجذيره
متوافق	متوافق مع المبادئ التوجيهية
عنوان IP	عنوان IP
آخر ظهور	النقطة الزمنية، عندما كان الجهاز متصلاً بـ AppTec لآخر مرة
الدفعة الأخيرة	النقطة الزمنية، عندما يرسل الخادم دفعة إلى الجهاز
تعيين المستخدم	قائمة منسدلة لتعيين الجهاز لمستخدم آخر

مراجعة التكوين (على مستوى الجهاز فقط)

هنا ستتلقى نظرة عامة على ملف تعريف المجموعة المعين للجهاز.

إذا قمت بالنقر على الملف الشخصي للمجموعة، فستتمكن من الوصول إلى الملف الشخصي مباشرةً ويمكنك إجراء الإعدادات.

باستخدام الرمز، يمكنك إعادة التطبيقات المعينة إلى إعدادات ملف تعريف المجموعة.

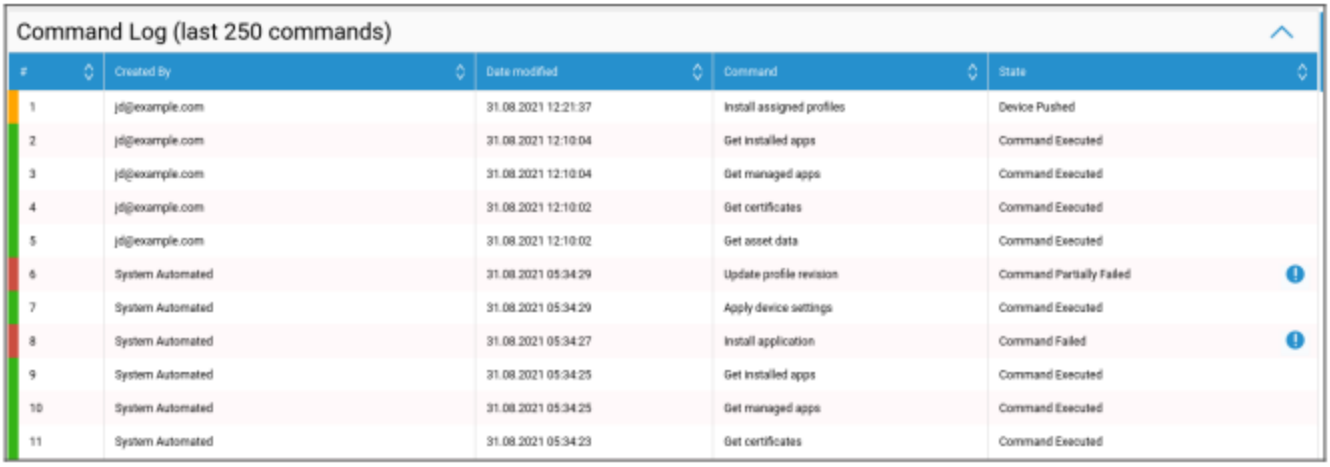
باستخدام الرمز، يمكنك إعادة ضبط ملف تعريف الجهاز بحيث لا يحتوي على أي إعدادات على الإطلاق.

تشير عبارة "تتوفر مراجعة أحدث" إلى أن ملف تعريف المجموعة قد تم تغييره وحفظه ولكن لم يتم تعيينه. يجب تعيين ملف تعريف المجموعة باستخدام "تعيين الآن" على مستوى المجموعة لتطبيق التغييرات على الأجهزة.

سجل الجهاز (على مستوى الجهاز فقط)

سجل الأوامر

هنا يمكنك معرفة الأوامر التي تم إصدارها للجهاز وما هي حالتها.



يتم إنشاء الأوامر التي تم إنشاؤها بواسطة "النظام الآلي" تلقائياً بواسطة النظام.

حالات الأوامر المحتملة

تم دفع الجهاز	تم إرسال طلب دفع إلى خدمة الدفع (مثل APNS) لإخبار الجهاز بالاتصال مرة أخرى بخادم EMM.
تم إنشاء الأمر	تم إنشاء الأمر في النظام.
تم إرسال الأمر	تم إرسال الأمر إلى الجهاز بعد اتصاله بالخادم.
تم تنفيذ الأمر	تم تنفيذ الأمر بنجاح.
فشل الأمر	فشل الأمر. *
فشل الأمر جزئياً	اعتمادًا على نظام تشغيل الجهاز قد يتم تجميع بعض الأوامر معًا. في هذا فشلت بعض أجزاء مجموعة الأوامر هذه. *
تم تنفيذ الأمر، وفشل الأمر في النهاية	تم تنفيذ الأمر ولكن ربما لم يتم تنفيذه.
إعادة دفع الأمر	تم إعادة دفع الأمر من قبل مستخدم.
مهملة	تم تجاهل الأمر. على سبيل المثال لأنه تم استبداله بأمر آخر أو تم إعادة تسجيل الجهاز وإزالة الأوامر القديمة

*إذا كانت هناك علامة تعجّب خلف الرسالة، يمكنك الحصول على مزيد من المعلومات من خلال تمرير مؤشر الماوس فوق الرمز.

إعدادات الجهاز

تهيئة العميل

هنا يمكنك إجراء التكوينات التالية على جهاز Android الخاص بك:

رسالة تحذير بعد تعطيل إدارة الأجهزة	إنشاء رسالة تحذير بعد تعطيل إدارة الأجهزة
وقت عدم الامتثال	الحد الزمني، وبعد ذلك سيتم تنفيذ "إجراء الإنفاذ بعد الامتثال"، إذا كان الجهاز غير متوافق. دقيقة واحدة 1 دقيقة كحد أقصى. 24 ساعة
إجراء الإنفاذ بعد انتهاء مهلة الامتثال	الإجراء الذي يجب اتخاذه، بمجرد أن يصبح الجهاز غير متوافق. • لا تفعل شيئًا = لا تفعل شيئًا • جهاز القفل = جهاز القفل = جهاز القفل • مسح الجهاز = ستتم استعادة الجهاز إلى إعدادات المصنع
تواتر جمع البيانات	التواتر الذي سيتم به جمع معلومات الجهاز/النظام العالمي لتحديد المواقع
تردد نبضات قلب الجهاز	الفاصل الزمني الذي يجب أن يتصل فيه الجهاز بخادم AppTec360 دقيقة واحدة 1 دقيقة كحد أقصى. 24 ساعة
تمكين تحديثات الموقع	إذا تم تنشيطه، يرسل الجهاز تحديثات الموقع إلى خادم AppTec360
وقت تحديث الموقع	يحدد الفترات الزمنية التي يرسل فيها الجهاز تحديثات الموقع إلى AppTec
استخدام دقة الموقع الجغرافي من Google لتحديث الموقع الجغرافي	إذا تم تفعيله، فسيتم استخدام دقة الموقع الجغرافي من Google (المعروف سابقًا باسم موقع الشبكة) لتحديثات الموقع الجغرافي (إذا تم إلغاء تنشيط هذا الإعداد ضمن "القيود"، فلن يؤثر هذا الإعداد على أي شيء)
استخدام موقع GPS لتحديث الموقع	في حالة تفعيله، سيتم استخدام GPS لتحديثات الموقع الجغرافي
السماح بالمواقع الوهمية (الوهمية)	السماح بتزوير معلومات الموقع الجغرافي عبر تطبيقات الطرف الثالث
إجراء فقدان الاتصال المفقود	يمكّنك من تعيين إجراء معين سيتم تنفيذه بعد فشل عدد معين من نبضات القلب
وضع إنفاذ السياسة	يحدد مدى قوة طلب عميل AppTec360 من المستخدم تنفيذ إجراءات معينة تتطلب إدخال المستخدم. الفاصل الزمني (افتراضي) = الطلب على فترات، بحيث يمكن للمستخدم وضع هذا في الخلفية لفترة من الوقت.

	لا يوجد تنبيه = لا توجد نافذة منبثقة لأي تفاعل مطلوب. يجب عليك فتح عميل AppTec360 يدويًا للتحقق مما إذا كان هناك إجراء مطلوب تنبيه مستمر = يمكن للمستخدم تنفيذ الإجراء المطلوب فقط. سيفرض عميل AppTec360 نفسه في المقدمة إذا حاول المستخدم تجنبه
قفل إصدار AppTec360	يتيح لك تحديد إصدار من عميل AppTec360 وهو الإصدار الأقصى الذي يقوم العميل بتحديث نفسه إليه.

ورق حائط

هنا يمكنك تحديد خلفية مخصصة.

يتيح لك "تحديد لون" تحديد لون بتنسيق سداسي عشري (على سبيل المثال #00000000). القيم السداسية فقط مسموح بها.

يتيح لك "تعيين صورة كخلفية" تحميل صورة. يرجى الانتباه إلى أن الأجهزة المختلفة ذات المشغلات وإصدارات نظام التشغيل المختلفة تعمل بشكل مختلف. لا يوجد خط إرشادي عام للحجم والنسبة، لأن ذلك يعتمد على الجهاز.

استخدم JPG (أو JPEG) أو PNG لتنسيق الملف.

إدارة الأصول (على مستوى الجهاز فقط)

إدارة الأصول

معلومات الجهاز

الطراز	تسمية طراز الجهاز
نظام التشغيل	نظام التشغيل
إصدار نظام التشغيل	إصدار نظام التشغيل
دعم AE	دعم Android Enterprise (الحاوية والمدارة بالكامل)
الرقم التسلسلي	الرقم التسلسلي
اسم الجهاز	اسم الجهاز
حالة البطارية	حالة البطارية
الذاكرة الحرة/إجمالي الذاكرة الحرة	الذاكرة الحرة/الإجمالية
Samsung KNOX	مستوى API KNOX KNOX من سامسونج
بطاقة SD متوفرة	بطاقة SD متوفرة
مضاهاة بطاقة SD	محاكاة بطاقة SD
بطاقة SD قابلة للإزالة	بطاقة SD قابلة للإزالة
ذاكرة SD الحرة/إجمالي الذاكرة الحرة	ذاكرة بطاقة SD الحرة/إجمالي ذاكرة بطاقة SD الحرة

الواي فاي

عنوان IP	عنوان IP للجهاز
واي فاي ماك	عنوان MAC الواي فاي

خلوي

الحالة	الحالة (بطاقة SIM مثبتة)
رقم الهاتف	رقم الهاتف
التجوال (الصوت/البيانات)	التجوال للصوت/البيانات
حالة التجوال	حالة التجوال الحالية
عنوان IP	عنوان IP
المشغل/الناقل	المشغل/الناقل
التكنولوجيا الخلوية	التكنولوجيا الخلوية
IMEI	رقم IMEI
ICCID	هذا هو المعرف الخاص ببطاقة SIM، وغالبًا ما تكون أيضًا بطاقة ذكية أو بطاقة دائرة متكاملة (ICC)
IMSI	توفر الهوية الدولية للمشتركين في الهاتف المحمول (IMSI) في شبكات GSM وUMTS للهواتف المحمولة تعريفاً محدداً لمستخدمي الشبكة يتكون IMSI من 15 رقماً كحد أقصى ويتم تكوينه بالطريقة التالية: • رمز البلد المتنقل (MCC)، 3 أرقام • رمز شبكة الهاتف المحمول (MNC)، 2 أو 3 أرقام • رقم تعريف مشترك الهاتف المحمول (MSIN)، من 1-10 أرقام
MCC/ MNC الحالية	انظر "SIM MCC/MNC"
SIM MCC/MNC	رمز البلد المتنقل هو مُعرِّف قطري محدد، وضعه الاتحاد الدولي للاتصالات وفقاً للمعيار E.212. يعمل هذا بالاقتران مع رمز شبكة الهاتف المحمول (MNC) لتحديد هوية شبكة الهاتف المحمول. يعني رمز البلد/رمز شبكة الهاتف المحمول الخاص ببطاقة SIM. إذا كنت تقوم بالتجوال في شبكة جوال أخرى، فمن المنطقي أن يكون "MCC/ MNC الحالي" و "MCC/ MNC لشريحة SIM"، مختلفين.

بلوتوث

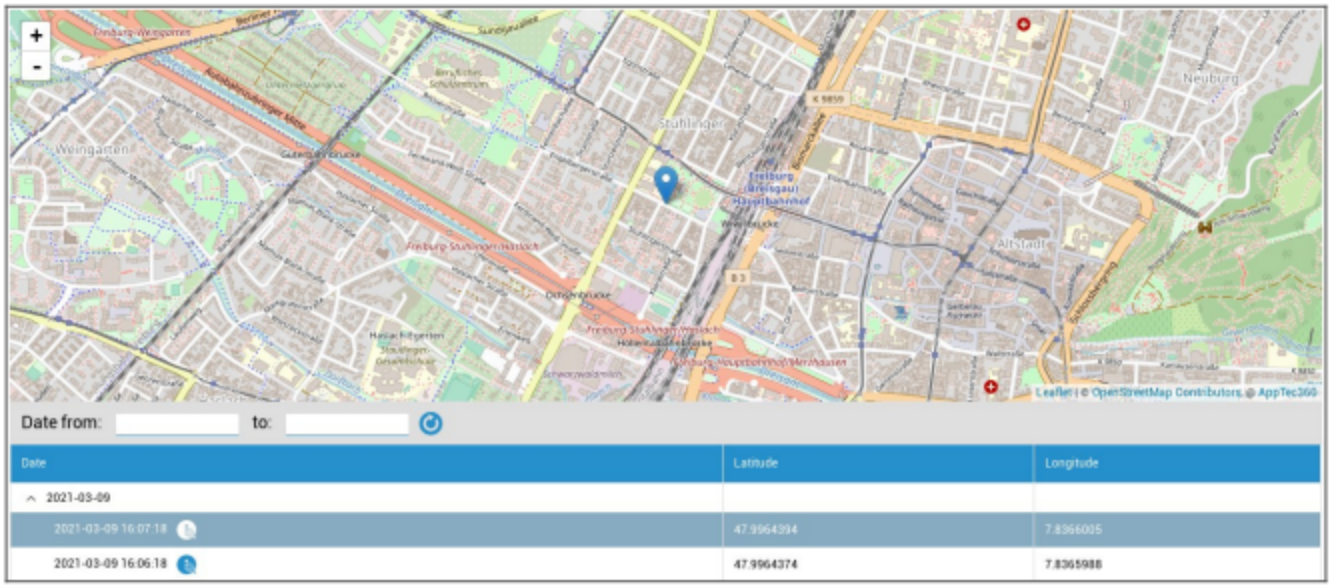
بلوتوث ماك	عنوان MAC للبلوتوث

إدارة الأمن

مكافحة السرقة (على مستوى الجهاز فقط)

معلومات GPS (على مستوى الجهاز فقط)

هنا يمكنك تحديد موقع الجهاز الحالي/الأخير. يمكن حماية تحديد الموقع باستخدام كلمة مرور واحدة أو حتى كلمتي مرور - انظر: الإعدادات العامة - الخصوصية - الوصول إلى نظام تحديد المواقع العالمي (GPS)



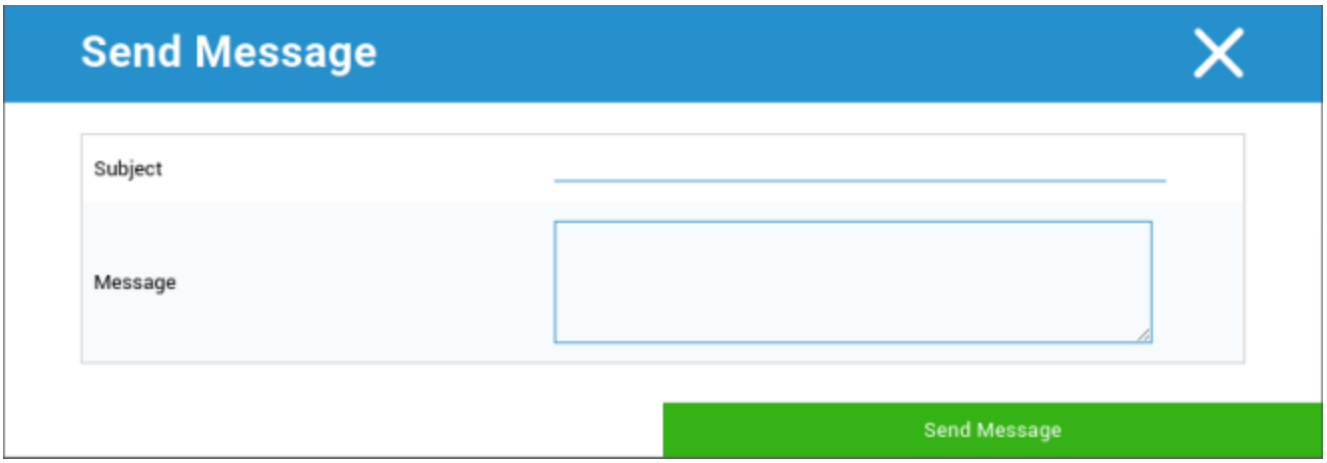
المسح والقفل (على مستوى الجهاز فقط)

ضمن "المسح والقفل"، يمكنك تنفيذ الإجراءات الثلاثة التالية:

مسح كامل	تتم استعادة الجهاز مرة أخرى إلى إعدادات المصنع (يتم حذف بيانات الشركة وكذلك البيانات الشخصية)
مسح المؤسسات	تتم إزالة بيانات الشركة فقط من جهاز المستخدم النهائي (جميع التطبيقات والبيانات وما إلى ذلك التي تم توفيرها بواسطة AppTec360)
قفل الشاشة	يتم تنشيط قفل الشاشة، ويكفي إلغاء قفل الجهاز باستخدام كلمة مرور الجهاز/رقم التعريف الشخصي

الرسالة (على مستوى الجهاز فقط)

يمكنك ملء الموضوع ورسالة وإرسالها إلى جهاز المستخدم النهائي. سيتم عرض هذه الرسالة في عميل AppTec360.



تهيئة الأمان

رمز المرور

تحت "رمز المرور" يمكنك تفويض كلمة مرور الجهاز، وتتوفر لك خيارات الإعداد التالية

الحد الأدنى لطول كلمة المرور	ينشئ، الحد الأدنى لعدد الرموز التي يجب أن تحتويها كلمة المرور
جودة كلمة المرور	قوة كلمة المرور غير محدد = غير محدد كل كلمة مرور مقبولة = كل كلمة مرور مقبولة أحرف رقمية على الأقل = يجب أن تحتوي على أحرف رقمية على الأقل أحرف معقدة على الأقل = يجب أن تحتوي على أحرف خاصة على الأقل أحرف أبجدية رقمية على الأقل = يجب أن تحتوي على أحرف أبجدية رقمية على الأقل أحرف أبجدية على الأقل = يجب أن تحتوي على أحرف أبجدية على الأقل
الحد الأقصى لقفل وقت عدم النشاط	المهلة القصوى للشاشة. يؤدي هذا فقط إلى تكوين القيمة القصوى التي يمكن للمستخدم تحديدها
الحد الأدنى من الأحرف الصغيرة المطلوبة في كلمة المرور	الحد الأدنى من الأحرف الصغيرة المطلوبة في كلمة المرور
الحد الأدنى من الأحرف الكبيرة المطلوبة في كلمة المرور	الحد الأدنى من الأحرف الكبيرة المطلوبة في كلمة المرور
الحد الأدنى من الأحرف غير الأحرف المطلوبة في كلمة المرور	الحد الأدنى من الأحرف غير الأحرف المطلوبة في كلمة المرور
الحد الأدنى من الأرقام العددية المطلوبة في كلمة المرور	الحد الأدنى من الأرقام العددية المطلوبة في كلمة المرور
الحد الأدنى من الرموز المطلوبة في كلمة المرور	الحد الأدنى من الرموز المطلوبة في كلمة المرور
مهلة انتهاء صلاحية كلمة المرور	ينشأ، وبعد هذه الفترة الزمنية تنتهي صلاحية كلمة المرور ويجب إصدار كلمة مرور جديدة
تقييد سجل كلمات المرور	عدد كلمات المرور المستخدمة سابقاً غير المسموح بها
الحد الأقصى لمحاولات كلمة المرور الفاشلة	يحدد، كم مرة يمكن إدخال كلمة مرور بشكل غير صحيح، قبل أن يتم إجراء مسح كامل للجهاز

التشفير

تحت هذه النقطة، يمكنك تشفير ذاكرة الجهاز الداخلية، وكذلك ذاكرة بطاقة SD.

تتطلب تشفير التخزين المطلوبة	إذا تم تنشيط هذا الإعداد، فسيتم تشفير ذاكرة الجهاز، طالما أن الجهاز يدعم هذه الوظيفة. بمجرد أن يتم تشفير ذاكرة الجهاز للمرة الأولى، لن يكون من الممكن إلغاء تشفيرها. وبالمثل، سيتم تبديل سياسة كلمة المرور تلقائياً إلى 6 رموز أبجدية رقمية
تتطلب تشفير بطاقة SD	ينطبق هذا الإعداد على أجهزة Samsung فقط! إذا تم تنشيط هذا الإعداد، يمكن تشفير بطاقة SD الخارجية ولا يمكن إلغاء تشفيرها يدوياً إلا على جهاز المستخدم النهائي. وبالمثل، سيتم تبديل سياسة كلمة المرور تلقائياً إلى 6 رموز أبجدية رقمية

مضاد الفيروسات

سيؤدي تمكين AntiVirus إلى تثبيت Ikarus على الأجهزة. يرجى الانتباه إلى أن هذا يتطلب ترخيصاً منفصلاً يمكن إدخاله في الإعدادات العامة ← إدارة التطبيقات ← تطبيقات الطرف الثالث.

المسح التلقائي	يحدد ما إذا كان Ikarus يقوم بالفحص التلقائي أم لا، وعدد مرات إجراء هذا الفحص سيؤدي تمكين "الفحص التلقائي الكامل" إلى إجراء فحص كامل. وإلا سيتم إجراء فحص سريع
التحديثات التلقائية	تمكين التحديثات التلقائية لقاعدة بيانات الفيروسات وتحديد عدد مرات حدوث ذلك
حماية التطبيق	تمكين فحص التطبيقات بالإضافة إلى الفحص العادي الذي يفحص الملفات فقط
حماية بطاقة SD	تمكين حماية بطاقة SD. وبدون ذلك، يقتصر الفحص على التخزين المحلي فقط
تحديث Wi-Fi فقط	حدود التحديث إلى Wi-Fi

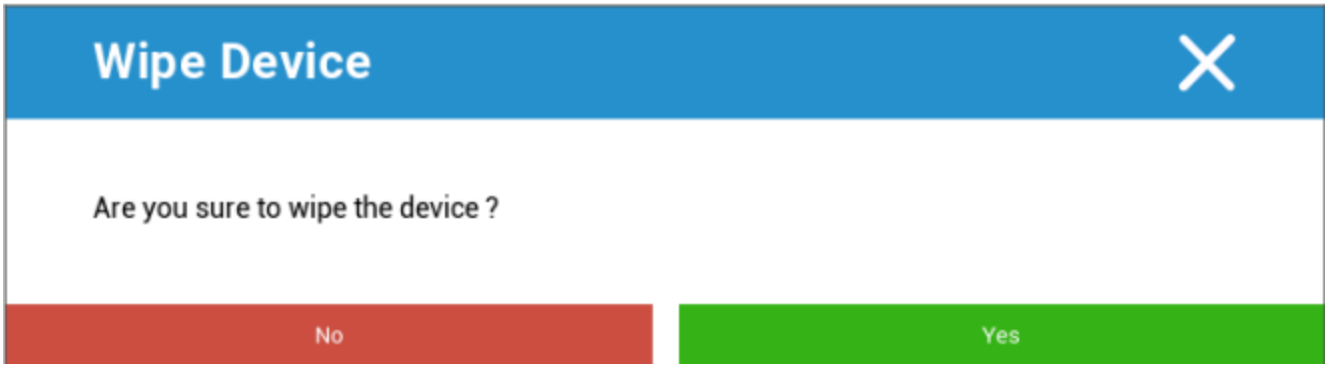
نهاية العمر الافتراضي (على مستوى الجهاز فقط)

المسح (على مستوى الجهاز فقط)

ضمن "مسح"، يمكنك استعادة الجهاز إلى إعدادات المصنع. هنا سيتم حذف بيانات الشركة وكذلك البيانات الخاصة على جهاز المستخدم النهائي.

بالنقر على "رمز الطرح" يجب أن تتلقى الرسالة التالية

مسح بطاقة SD أيضاً؟	سيتم أيضاً مسح ذاكرة بطاقة SD أيضاً



باستخدام "نعم" يمكنك إجراء المسح.

تحت عنوان "تقرير المسح" يمكن عرض العناصر التالية

ممسوح بواسطة	تاريخ من قام بالمسح
التاريخ	التاريخ
الحالة	الحالة (على سبيل المثال، إذا تم إجراء المسح بنجاح)

إعدادات التقييد

القيود

هنا، يمكن تقييد وحظر مجموعة متنوعة من الأشياء.

تمكين الكاميرا	السماح باستخدام الكاميرا
فرض المزامنة التلقائية	يتعلق بواجهة "المزامنة" تشغيل = المزامنة مفعلة بشكل دائم إيقاف التشغيل = المزامنة معطلة بشكل دائم اختيار المستخدم = محدد من قبل المستخدم
قوة البلوتوث	تشغيل = البلوتوث مفعل بشكل دائم إيقاف التشغيل = تم إلغاء تنشيط البلوتوث بشكل دائم اختيار المستخدم = محدد من قبل المستخدم
قوة نظام تحديد المواقع العالمي (GPS)	قيد التشغيل = نظام تحديد المواقع العالمي (GPS) مفعل بشكل دائم إيقاف التشغيل = نظام تحديد المواقع العالمي (GPS) معطل بشكل دائم اختيار المستخدم = محدد من قبل المستخدم
فرض دقة الموقع الجغرافي من Google	تشغيل = توطين دائم على الإنترنت إيقاف التشغيل = إلغاء التنشيط الدائم لتوطين الإنترنت اختيار المستخدم = محدد من قبل المستخدم

بالنسبة لأجهزة Samsung المزودة بواجهة KNOX 1.0 أو أعلى، تتوفر خيارات الإعدادات التالية.

السماح لبطاقة SD	السماح لبطاقة SD
السماح بالكتابة على بطاقة SD	السماح بـ "الكتابة" على بطاقة SD
السماح بالتقاط الشاشة	السماح بالتقاط الشاشة
السماح للحافظة	السماح بالحافظة
إعدادات النسخ الاحتياطي وبيانات التطبيق في Google Cloud	إيقاف التشغيل = إلغاء تنشيط النسخ الاحتياطي من Google تشغيل = تفعيل النسخ الاحتياطي من Google اختيار المستخدم = محدد من قبل المستخدم
السماح بتصحيح أخطاء USB	السماح بتصحيح أخطاء USB (يستخدم، على سبيل المثال، لإنشاء سجلات الجهاز (ADB))
السماح بتقرير أعطال Google	السماح بإرسال تقرير الأعطال من Google من التطبيقات
السماح بإعادة ضبط المصنع	يسمح للمستخدم باستعادة الجهاز إلى إعدادات المصنع الخاصة به
السماح بترقية OTA	السماح بالتحديثات "عبر الهواء"
السماح بتخزين USB المضيف	إذا تم تنشيطه، يمكن توصيل ذاكرة USB، في شكل HD أو قارئ بطاقة SD، في حالة تنشيطها
السماح بمشغل وسائط USB (MTP، PTP)	السماح بمشغل وسائط USB (MTP، PTP)
السماح بالميكروفون	تشغيل = السماح بالميكروفون لتطبيقات الطرف الثالث إيقاف التشغيل = حظر الميكروفون لتطبيقات الطرف الثالث اختيار المستخدم = يمكن للمستخدمين الاختيار، إذا كان تطبيق الطرف الثالث لديه إمكانية الوصول إلى الميكروفون
السماح بتقنية الاتصال قريب المدى (NFC)	السماح بتقنية الاتصال قريب المدى قريب المدى
السماح بمصادر غير معروفة (تحميل جانبي لملف APK)	في حالة التمكين، يُسمح بالتحميل الجانبي للتطبيقات (ملفات APK). بمجرد تعطيل هذا الإعداد، يتعين على المستخدم تمكينه يدويًا عند إعادة السماح بتثبيت ملفات APK من مصادر غير معروفة.
السماح بإنشاء المستخدم	السماح بإنشاء عدة مستخدمين

مالك جهاز AE

(يجب أن يكون الجهاز في وضع مالك جهاز Android Enterprise) يوصى بإنشاء الأجهزة كجهاز "Android Enterprise" وليس كجهاز "Android".

الأمن

عدم السماح بموقع المشاركة	يحدد ما إذا كان المستخدم غير مسموح له بتشغيل مشاركة الموقع.
تعطيل التمهيد الآمن	يحدد ما إذا كان المستخدم غير مسموح له بإعادة تشغيل الجهاز في وضع التمهيد الآمن.
عدم السماح بإعادة تعيين الشبكة	يحدد ما إذا كان المستخدم غير مسموح له بإعادة تعيين إعدادات الشبكة من الإعدادات.
عدم السماح بإعادة ضبط المصنع	يحدد ما إذا كان المستخدم غير مسموح له بإعادة ضبط الجهاز.
تمكين بنك التنمية الآسيوي	يسمح بالاتصال بجهاز كمبيوتر شخصي عبر ADB
تعطيل حماية المفاتيح	تعطيل برنامج حماية المفاتيح
معلومات شاشة قفل مالك الجهاز	يضبط معلومات مالك الجهاز لتظهر على شاشة القفل.
إنفاذ الامتثال	وضع مطالبة المستخدم - سيُطلب من المستخدم تنفيذ الإجراءات اللازمة. حاوية قفل الوضع - إخفاء جميع التطبيقات حتى يتم استيفاء جميع المتطلبات

إدارة التطبيقات	
السماح بالربط بين تطبيقات الملفات الشخصية	السماح للتطبيقات في ملف التعريف الأصلي بمعالجة روابط الويب من ملف التعريف المُدار.
عدم السماح بالتحكم في التطبيق	يحدد ما إذا كان المستخدم غير مسموح له بتعديل التطبيقات في الإعدادات أو المشغلات.
عدم السماح بتثبيت التطبيق	يحدد ما إذا كان المستخدم غير مسموح له بتثبيت التطبيقات.
تعطيل إلغاء تثبيت التطبيقات	يحدد ما إذا كان المستخدم غير مسموح له بإلغاء تثبيت التطبيقات.
سياسة إذن وقت التشغيل	يحدد كيفية التعامل مع طلبات الأذونات الجديدة من التطبيقات.
السماح بمصادر غير معروفة	في حالة التمكين، يمكن للمستخدمين تحميل التطبيقات بشكل جانبي عن طريق تثبيت ملف .apk.

الاتصال	
عدم السماح بتكوين شبكة الجوال	يحدد ما إذا كان المستخدم غير مسموح له بتكوين شبكات الهاتف المحمول.
عدم السماح بتكوين الربط	يُحدد ما إذا كان المستخدم غير مسموح له بتكوين نقاط الاتصال والنقاط الساخنة المحمولة.
عدم السماح بتكوين VPN	يحدد ما إذا كان المستخدم غير مسموح له بتكوين شبكة VPN.
عدم السماح بتكوين Wifi	يحدد ما إذا كان المستخدم غير مسموح له بتغيير نقاط وصول WiFi.
عدم السماح بشعاع NFC الصادر	يحدد ما إذا كان المستخدم غير مسموح له باستخدام NFC لإرسال البيانات من التطبيقات.
تكوين قفل الواي فاي القفل	يتحكم هذا الإعداد في ما إذا كان ينبغي تأمين تكوينات WiFi التي تم إنشاؤها بواسطة تطبيق مالك الجهاز (أي أن تكون قابلة للتحرير أو الإزالة فقط من قبل تطبيق مالك الجهاز، وليس حتى من قبل تطبيق الإعدادات).
تمكين تجوال البيانات	تنشيط تجوال البيانات

بلوتوث	
عدم السماح بالبلوتوث	يحدد ما إذا كان البلوتوث غير مسموح به على الجهاز. يتطلب أندرويد 8.0
عدم السماح بمشاركة البلوتوث	يحدد ما إذا كانت مشاركة البلوتوث الصادرة غير مسموح بها على الجهاز. يتطلب أندرويد 8.0
عدم السماح بتكوين البلوتوث	يحدد ما إذا كان المستخدم غير مسموح له بتكوين البلوتوث.

إدارة الحسابات	
عدم السماح بإضافة ملف تعريف مُدار	يحدد ما إذا كان المستخدم غير مسموح له بإضافة ملفات تعريف مُدارة. يتطلب أندرويد 8.0
عدم السماح بإضافة مستخدمين	يحدد ما إذا كان المستخدم غير مسموح له بإضافة مستخدمين جدد.
عدم السماح بإزالة ملف التعريف المُدار	يحدد ما إذا كان يمكن إزالة ملفات التعريف المدارة لهذا المستخدم، بخلاف مالك ملف التعريف الخاص به. يتطلب أندرويد 8.0
عدم السماح بتعديل الحساب	يحدد ما إذا كان المستخدم غير مسموح له بإضافة حسابات وإزالتها، ما لم تتم إضافتها برمجيًا بواسطة المصادقة.

الاتصالات الهاتفية	
عدم السماح بالمكالمات الصادرة	يحدد عدم السماح للمستخدم بإجراء مكالمات هاتفية صادرة.
عدم السماح بالرسائل النصية القصيرة	يحدد أن المستخدم غير مسموح له بإرسال أو استقبال الرسائل النصية القصيرة.

النظام	
عدم السماح بإنشاء النوافذ	يحدد أنه لا ينبغي إنشاء نوافذ غير نوافذ التطبيق.
عدم السماح بتعيين أيقونة المستخدم	يحدد ما إذا كان المستخدم غير مسموح له بتغيير الرمز الخاص به.
عدم السماح بتعيين الخلفية	تقييد المستخدم لعدم السماح بتعيين خلفية.
تعطيل شريط الحالة	يؤدي تعطيل شريط الحالة إلى حظر الإشعارات والإعدادات السريعة وتراكبات الشاشة الأخرى التي تسمح بالهروب من جهاز يستخدم مرة واحدة.
تمكين الوقت التلقائي	يضبط الوقت تلقائياً.
تمكين المنطقة الزمنية التلقائية	يضبط المنطقة الزمنية تلقائياً.
البقاء قيد التشغيل أثناء التوصيل بالكهرباء	سيبقى الجهاز نشطاً أثناء توصيله بمصدر طاقة.

التخزين	
تعطيل تعطيل التحقق من التطبيق	يحدد ما إذا كان المستخدم غير مسموح له بتعطيل التحقق من التطبيق.
عدم السماح بتركيب الوسائط المادية	يحدد ما إذا كان المستخدم غير مسموح له بتركيب وسائط خارجية فعلية.

تمكين خدمة النسخ الاحتياطي	تدير خدمة النسخ الاحتياطي جميع آليات النسخ الاحتياطي والاستعادة على الجهاز. سيؤدي تعيين هذا إلى خطأ إلى منع النسخ الاحتياطي للبيانات أو استعادتها. يتم إيقاف تشغيل خدمة النسخ الاحتياطي بشكل افتراضي. يتطلب أندرويد 8.0
تمكين وحدة تخزين USB للتخزين الشامل	تمكين استخدام وحدة التخزين الشامل USB.

لوحة المفاتيح	
عدم السماح بالملء التلقائي	يحدد ما إذا كان المستخدم غير مسموح له باستخدام خدمات الملء التلقائي. يتطلب أندرويد 8.0
عدم السماح بالنسخ واللصق بين الملفات الشخصية	يحدد ما إذا كان يمكن لصق ما تم نسخه في حافظة ملف التعريف هذا في ملفات التعريف ذات الصلة.

الصوت	
عدم السماح بتعديل الحجم	يحدد ما إذا كان المستخدم غير مسموح له بتعديل مستوى الصوت الرئيسي.
تعطيل إلغاء كتم صوت الميكروفون	يحدد ما إذا كان المستخدم غير مسموح له بضبط مستوى صوت الميكروفون.
جهاز كتم الصوت	جهاز كتم الصوت.

سياسة تحديث النظام	
التحكم في تحديثات نظام التشغيل	قم بتمكين هذا لتعيين سلوك التحديث إلى تلقائي أو مؤجل أو مؤجل.

حاوية BYOD

أندرويد إنتربرايز

أندرويد إنتربرايز

تمكين أندرويد إنتربرايز	تمكين Android Enterprise (AE). AE مدعوم منذ أندرويد 5.1 وما فوق.
إنفاذ الامتثال	وضع مطالبة المستخدم - سيُطلب من المستخدم تنفيذ الإجراءات اللازمة. حاوية قفل الوضع - إخفاء جميع التطبيقات حتى يتم استيفاء جميع المتطلبات
سياسة إذن وقت التشغيل	مطالبة المستخدم بطلبات الأذونات الجديدة منح طلبات الإذن الجديدة الجديدة دائماً رفض طلبات الإذن الجديدة دائمًا تحذير: تواجه بعض التطبيقات مشاكل في التعرف على الأذونات إذا تم تعيينها تلقائياً. إذا كنت تمنح الأذونات دائمًا وواجهت مشاكل مع التطبيقات التي تقول أن الأذونات مفقودة، فقم بتعيين هذا على "مطالبة المستخدم" وأعد تثبيت التطبيق
السماح بالحافظة الصادرة	يسمح بالنسخ واللصق من داخل الحاوية إلى خارجها
السماح بتحديد هوية المتصل	إظهار اسم المكالمة الواردة بناءً على جهات الاتصال في الحاوية
السماح بالبحث عن جهة الاتصال القرار	يسمح بالبحث عن الأسماء في جهات اتصال الحاوية عند إجراء المكالمات
السماح بمشاركة جهات اتصال Bluetooth	يسمح بالوصول إلى حاوية الاتصال في السيارة
عدم السماح بشعاع NFC الصادر	تعطيل NFC للحاوية
السماح بمصادر غير معروفة	في حالة التمكين، يمكن للمستخدمين تحميل التطبيقات بشكل جانبي عن طريق تثبيت ملف .apk.
السماح بتصحيح أخطاء USB	إذا تم تمكينه، يمكن للمستخدمين تمكين تصحيح أخطاء USB.
عدم السماح بتعديل الحساب	عدم السماح بإنشاء حسابات في الحاوية وحذفها وتعديلها في الحاوية ضع في اعتبارك أن بعض التطبيقات تحتاج إلى إنشاء حسابات أو تعديلها لتعمل كما هو متوقع

Gmail Exchange

يتيح لك تكوين Gmail في الحاوية. يرجى الانتباه إلى أن تمكين هذا التكوين لا يؤدي إلى تثبيت التطبيق تلقائيًا. لا يزال عليك إضافة هذا التطبيق كتطبيق إلزامي.

عنوان البريد الإلكتروني	عنوان البريد الإلكتروني
اسم مضيف الخادم	اسم مضيف الخادم
اسم تسجيل الدخول	اسم تسجيل الدخول
التوقيع	التوقيع
عدد الأيام السابقة للمزامنة	عدد الأيام السابقة للمزامنة.
معرّف الجهاز	معرّف EAS. اترك هذا فارغًا إذا كانت بيئتك لا تتطلب ذلك
استخدام طبقة مآخذ التوصيل الآمنة (SSL)	تمكين استخدام SSL. قد يؤدي تعطيل ذلك إلى تقليل الأمان
قبول جميع الشهادات	يقبل جميع الشهادات. قد يؤدي تمكين ذلك إلى تقليل الأمان
السماح بالحسابات غير المُدارة	السماح للمستخدم بإضافة حسابات إضافية
شهادة العميل	تحميل شهادة العميل إذا كان خادم Exchange الخاص بك يتطلب ذلك

تطبيقات نظام AE

هنا يمكنك تمكين تطبيقات النظام لحاوية Android Enterprise Container. يرجى الأخذ في الاعتبار أن التطبيق المحدد يجب أن يكون في مخزن النظام، وإلا فلن يحدث شيء.

رمز مرور الحاوية

فقط لنظام أندرويد 7.0 أو أعلى

يسمح لك بتعيين متطلبات كلمة مرور محددة للحاوية.

الحد الأدنى لطول كلمة المرور	ينشئ، الحد الأدنى لعدد الرموز التي يجب أن تحتويها كلمة المرور
جودة كلمة المرور	قوة كلمة المرور غير محدد = غير محدد كل كلمة مرور مقبولة = كل كلمة مرور مقبولة أحرف رقمية على الأقل = يجب أن تحتوي على أحرف رقمية على الأقل أحرف معقدة على الأقل = يجب أن تحتوي على أحرف خاصة على الأقل أحرف أبجدية رقمية على الأقل = يجب أن تحتوي على أحرف أبجدية رقمية على الأقل أحرف أبجدية على الأقل = يجب أن تحتوي على أحرف أبجدية على الأقل
الحد الأقصى لقفل وقت عدم النشاط	الحد الأقصى للوقت حتى يتم قفل الحاوية. يقوم هذا بتكوين القيمة القصوى فقط التي يمكن للمستخدم تحديدها
الحد الأدنى من الأحرف الصغيرة المطلوبة في كلمة المرور	الحد الأدنى من الأحرف الصغيرة المطلوبة في كلمة المرور
الحد الأدنى من الأحرف الكبيرة المطلوبة في كلمة المرور	الحد الأدنى من الأحرف الكبيرة المطلوبة في كلمة المرور
الحد الأدنى من الأحرف غير الأحرف المطلوبة في كلمة المرور	الحد الأدنى من الأحرف غير الأحرف المطلوبة في كلمة المرور
الحد الأدنى من الأرقام العددية المطلوبة في كلمة المرور	الحد الأدنى من الأرقام العددية المطلوبة في كلمة المرور
الحد الأدنى من الرموز المطلوبة في كلمة المرور	الحد الأدنى من الرموز المطلوبة في كلمة المرور
مهلة انتهاء صلاحية كلمة المرور	ينشأ، وبعد هذه الفترة الزمنية تنتهي صلاحية كلمة المرور ويجب إصدار كلمة مرور جديدة
تقييد سجل كلمات المرور	عدد كلمات المرور المستخدمة سابقاً غير المسموح بها
الحد الأقصى لمحاولات كلمة المرور الفاشلة	يحدد، عدد المرات التي يمكن فيها إدخال كلمة المرور بشكل غير صحيح، قبل أن يتم حذف الحاوية

Samsung KNOX

التفعيل

هنا يمكنك تمكين حاوية Samsung KNOX Container. يُرجى العلم أن هذا لم يعد مدعومًا من سامسونج على نظام Android 10 أو أعلى. استخدم حاوية Android Enterprise Container على Android 10 أو أعلى

رمز مرور نوكس

وضع المبادئ التوجيهية التي تتعلق بإعدادات كلمة مرور الجهاز

الحد الأدنى لطول كلمة المرور	يحدد، عدد الرموز التي يجب أن تحتويها كلمة المرور
جودة كلمة المرور	قوة كلمة المرور كل كلمة مرور على ما يرام = كل كلمة مرور على ما يرام يجب أن يكون الحد الأدنى من الأحرف الرقمية = يجب أن يكون الحد الأدنى من الأحرف الرقمية موجودًا يجب أن تكون الأحرف المعقدة على الأقل = يجب أن يكون هناك حد أدنى من الأحرف الخاصة يجب أن يكون الحد الأدنى من الأحرف الأبجدية الرقمية = يجب أن يكون الحد الأدنى من الأحرف الأبجدية الرقمية يجب أن تكون الأحرف الأبجدية على الأقل = يجب أن يكون الحد الأدنى من الأحرف الأبجدية موجودًا
الحد الأدنى من الأحرف المعقدة المطلوبة	يجب وجود الحد الأدنى من الأحرف المعقدة
الحد الأقصى لمهلة عدم النشاط	الحد الأقصى لمهلة عدم نشاط المستخدم، قبل قفل لوحة المفاتيح
السماح بمصادقة بصمة الإصبع	السماح بمصادقة بصمة الإصبع
السماح بمصادقة قزحية العين	السماح بمصادقة التعرف على قزحية العين
الحد الأقصى لعمر كلمة المرور	يحدد، بعد أي وقت تنتهي صلاحية كلمة المرور ويجب إصدار كلمة مرور جديدة
سجل كلمات المرور المخزنة	عدد كلمات المرور السابقة غير المسموح بها
الحد الأقصى لمحاولات كلمة المرور الفاشلة	يحدد، عدد المرات التي قد يتم فيها إرسال كلمة المرور بشكل غير صحيح، قبل أن يتم مسح الجهاز بالكامل

نوكس سيكيوريتي

الحد من وظائف الجهاز المحددة

تمكين الكاميرا	السماح باستخدام الكاميرا
السماح لمتجر Samsung KNOX App Store	السماح باستخدام متجر تطبيقات Samsung KNOX App Store
السماح لخدمات Google Play من Google Play	السماح لخدمات Google Play من Google Play
السماح للمتصفح	السماح باستخدام المتصفح الأصلي
السماح بلقطات الشاشة	السماح بإنشاء لقطات شاشة

السماح باستيراد جهات الاتصال	في حالة تفعيلها، يُسمح بالوصول إلى جهات اتصال الجهاز من حاوية KNOX
السماح بتصدير جهات الاتصال	في حالة تفعيله، يُسمح بالوصول إلى جهات اتصال KNOX من الجهاز
السماح باستيراد التقويم	في حالة تنشيطه، يُسمح بالوصول إلى تقويم الجهاز من حاوية KNOX
السماح بتصدير التقويم	في حالة تفعيله، يُسمح بالوصول إلى تقويم KNOX من الجهاز
السماح بلوحة مفاتيح غير آمنة	السماح باستخدام لوحة مفاتيح غير آمنة
تمكين استيراد الملفات	تمكين استيراد الملفات إلى حاوية KNOX
تمكين تصدير الملفات	تمكين تصدير الملف من حاوية KNOX

نوكس للصرافة

هنا يمكنك تكوين ملف تعريف التبادل لحاوية KNOX Container

عنوان البريد الإلكتروني	عنوان البريد الإلكتروني للمستخدم المقدم يرجى ملاحظة "العناصر النائبة"، التي يمكنك استخدامها للعمل مع بيانات الاعتماد ولا تقوم بإجراء تغييرات يدوياً على كل جهاز بنقرة على **إظهار العناصر النائبة** يمكنك عرضها بنفسك
اسم مضيف الخادم	عنوان الخادم الخاص بخوادم Exchange الخاصة بك
اسم تسجيل الدخول	اسم تسجيل الدخول لجهاز المستخدم النهائي المعني، يُرجى أيضًا ملاحظة "العناصر النائبة" هنا
المجال	عنوان المجال
كلمة المرور (على مستوى الجهاز فقط)	يمكن اختياريًا تزويد الجهاز الفردي بكلمة مرور، وفي حالة بقائها فارغة، سيُطلب من المستخدم إدخال كلمة مرور الصرف الخاصة به
عدد الأيام السابقة للمزامنة	عدد الأيام التي يتم فيها تحديد موعد مزامنة رسائل البريد الإلكتروني
التوقيع	يمكن إرفاق توقيع
الحساب الافتراضي	يثبت، أن حساب البريد الإلكتروني هذا هو الحساب القياسي
استخدام طبقة مآخذ التوصيل الآمنة (SSL)	استخدام اتصال SSL
استخدام أمان طبقة النقل (TLS)	استخدام اتصال TLS
قبول جميع الشهادات	جميع الشهادات مقبولة. الرجاء تحديد هذا الخيار، إذا كان خادم Exchange لديك يستخدم شهادة موقعة ذاتياً

بريد نوكس الإلكتروني

عنوان البريد الإلكتروني	عنوان البريد الإلكتروني للمستخدم المقدم يرجى ملاحظة "العناصر النائبة"، التي يمكنك استخدامها للعمل مع بيانات الاعتماد ولا تقوم بإجراء تغييرات يدوياً على كل جهاز بنقرة على **إظهار العناصر النائبة** يمكنك عرضها بنفسك
بروتوكول الخادم الوارد	بروتوكول الخادم الوارد IMAP أو POP
عنوان الخادم الوارد	عنوان الخادم الوارد
منفذ الخادم الوارد	منفذ الخادم الوارد
تسجيل الدخول إلى الخادم الوارد/اسم المستخدم	تسجيل الدخول إلى الخادم الوارد/اسم المستخدم
كلمة مرور الخادم الوارد	كلمة مرور الخادم الوارد
يستخدم الخادم الوارد SSL	يستخدم الخادم الوارد SSL
يستخدم الخادم الوارد TLS	يستخدم الخادم الوارد TLS
يقبل الخادم الوارد جميع الشهادات	الخادم الوارد يقبل جميع أنواع الشهادات
بروتوكول الخادم الصادر	بروتوكول الخادم الصادر SMTP
منفذ الخادم الصادر	منفذ الخادم الصادر
يستخدم الخادم الصادر بيانات اعتماد إضافية	بيانات اعتماد إضافية للخادم الصادر. إذا تم ضبط هذا على "إيقاف التشغيل"، فسيتم استخدام إعدادات الخادم الصادر
تسجيل الدخول إلى الخادم الصادر/اسم المستخدم	تسجيل الدخول إلى الخادم الصادر/اسم المستخدم
كلمة مرور الخادم الصادر	كلمة مرور الخادم الصادر
يستخدم الخادم الصادر SSL	يستخدم الخادم الصادر SSL
يستخدم الخادم الصادر TLS	يستخدم الخادم الصادر TLS
يقبل الخادم الصادر جميع الشهادات	يقبل الخادم الصادر جميع أنواع الشهادات الصادرة
التوقيع	هنا يمكن إرفاق توقيع
إعلام المستخدم عند تلقي بريد إلكتروني جديد	إعلام المستخدم عند تلقي بريد إلكتروني جديد

تطبيقات نوكس

أنشئ التطبيقات هنا التي تريد توزيعها على أجهزة المستخدم النهائي. ستكون هذه متاحة بعد ذلك في حاوية KNOX-Container. لإضافة تطبيق، يُرجى المتابعة كما تفعل في القائمة تطبيقات إلزامية

اسم التطبيق	اسم التطبيق
إلزامي منذ	النقطة الزمنية، عند إضافة التطبيق
المصدر	مصدر التطبيق (متجر بلاي ستور | في المنزل)

من خلال النقر على الرمز، يمكن إزالة التطبيق المعني مرة أخرى

إدارة الاتصال

الواي فاي

بالنسبة لهذا الإعداد، قم بإجراء التكوين المسبق لأجهزة المستخدم النهائي، للوصول إلى نقاط الوصول الداخلية

معرّف مجموعة الخدمات (SSID)	SSID للشبكة التي سيتم الاتصال بها
الشبكة الخفية	تنشيط، في حالة عدم قيام نقطة الوصول إلى نقطة الوصول ببث SSID
نوع الأمان	إنشاء نوع أمان نقطة الوصول

نوع الأمان

WEP

كلمة المرور	كلمة المرور الخاصة بـ AP

WPA/WPA2

كلمة المرور	كلمة المرور الخاصة بـ AP

802.1x EAP 802.1x

طريقة EAP-Method	

الأشخاص ذوو الإعاقة	الهوية	الهوية
	كلمة المرور	كلمة المرور

PEAP	بروتوكول المصادقة في المرحلة 2	لا شيء	لا يوجد بروتوكول إضافي
		MSCHAPV2	بروتوكول MSCHAPV2

		GTC	بروتوكول GTC
	شهادة المرجع المصدق (CA)	شهادة المرجع المصدق (CA)	
	الهوية	الهوية	
	هوية مجهولة	هوية مجهولة	
	كلمة المرور	كلمة المرور	

طريقة EAP-Method	

TTLS	بروتوكول المصادقة في المرحلة 2	لا شيء	لا يوجد بروتوكول إضافي
		برنامج مساعدة الشعب الفلسطيني	بروتوكول PAP
		MSCHAP	بروتوكول MSCHAP
		MSCHAPV2	بروتوكول MSCHAPV2
		GTC	بروتوكول GTC
	شهادة المرجع المصدق (CA)	شهادة المرجع المصدق (CA)	
	الهوية	الهوية	
	هوية مجهولة	هوية مجهولة	
	كلمة المرور	كلمة المرور	

TLS	شهادة المرجع المصدق (CA)	شهادة المرجع المصدق (CA)
	الهوية	الهوية
	كلمة المرور	كلمة المرور

VPN

نوع الاتصال	**إنشاء نوع اتصال VPN**

إذا قمت بتحديد "VPN لكل تطبيق" كنوع VPN، سيتغير عملاء VPN المتاحين. تقصر الشبكة الافتراضية الخاصة لكل تطبيق على تطبيقات معينة وتبدأ اتصال الشبكة الافتراضية الخاصة تلقائيًا إذا تم تشغيل تطبيق معين.

عميل AppTec360 VPN	يستخدم عميل AppTec360 VPN Client مع البوابة العالمية
اسم الاتصال	اسم اتصال VPN
تكوين البوابة	حدد تكوين VPN للبوابة العالمية

دائماً على VPN	يجبر الشبكة الافتراضية الخاصة على أن تكون نشطة دائمًا، بحيث تمر حركة المرور بأكملها عبر الشبكة الافتراضية الخاصة.
تمكين الإغلاق الأصلي	يحظر جميع الشبكات عندما يكون الجهاز غير متصل بشبكة VPN. استخدم هذا بعناية لأن هذا يمكن أن يتسبب في فقدان الاتصال بالكامل إذا لم يتم تكوينه بشكل صحيح. فقط لمؤسسات أندرويد على أندرويد 7 أو أعلى
تمكين تأمين AppTec360 AppTec360	حظر استخدام جميع التطبيقات حتى يتم تشغيل اتصال VPN

Cisco AnyConnect	
اسم الاتصال	اسم اتصال VPN
الخادم	عنوان الخادم
وضع الشهادة	معطل = معطل = معطل تلقائي = تلقائي

L2TP (KNOX فقط)	متوفر فقط على أجهزة سامسونج
اسم الاتصال	اسم الاتصال
الخادم	عنوان الخادم
تمكين L2TP سري L2TP	
نطاقات بحث DNS	نطاقات بحث DNS

نوع الاتصال	**إنشاء نوع اتصال VPN**

PPTP (KNOX فقط)	متوفر فقط على أجهزة سامسونج
اسم الاتصال	اسم اتصال VPN
الخادم	عنوان الخادم
تمكين التشفير	تمكين التشفير
نطاقات بحث DNS	نطاقات بحث DNS

L2TP / IPSec PSK (KNOX فقط)	متوفر فقط على أجهزة سامسونج
اسم الاتصال	اسم اتصال VPN
الخادم	عنوان الخادم
المفتاح المشترك المسبق IPSec	مفتاح مشترك مسبقاً للمصادقة
تمكين L2TP سري L2TP	
L2TP سري L2TP	
نطاقات بحث DNS	نطاقات بحث DNS

IPSec XAuth PSK (KNOX فقط)	متوفر فقط على أجهزة سامسونج
اسم الاتصال	اسم اتصال VPN
الخادم	عنوان الخادم
معرّف IPSec	اسم المستخدم للاتصال
المفتاح المشترك المسبق IPSec	كلمة المرور للاتصال
نطاقات بحث DNS	نطاقات بحث DNS

OpenVPN	
اسم الاتصال	اسم الاتصال

ملف تعريف OpenVPN	فيما يلي مكان نسخ محتوى الملف .ovpn
تطبيق OpenVPN	هناك تطبيقان مختلفان لاستخدام OpenVPN نوصي باستخدام تطبيق "OpenVPN لنظام Android". ولكن بدلاً من ذلك، يمكن استخدام تطبيق "OpenVPN Connect"

القيود

هنا يمكنك تعيين القيود، فيما يتعلق بإدارة الاتصال.

السماح بتجوال البيانات	السماح ببيانات الجوال أثناء التجوال
فرض تجوال البيانات	إذا تم تفعيله، يتم تفعيل التجوال لبيانات الهاتف المحمول بشكل دائم (غير مستحسن!) يحل هذا الإعداد محل إعداد "السماح بتجوال البيانات"!
الإعدادات التالية متوفرة فقط على Samsung KNOX 2.0 أو أعلى	
السماح بمكالمات الطوارئ فقط	السماح بمكالمات الطوارئ فقط
السماح بالواي فاي	السماح بالواي فاي
الحد الأدنى لمستوى أمان شبكة WiFi	الحد الأدنى لمستوى أمان شبكة WiFi مفتوح = يُسمح باستخدام جميع أنواع الواي فاي
منع المستخدم من إضافة شبكات WiFi	لا يجوز للمستخدم إضافة شبكة WiFi بنفسه هذا الإعداد ممكن فقط، إذا تم تعريف ملف تعريف WiFi ضمن "إدارة الاتصال"
السماح بالرسائل النصية القصيرة ورسائل الوسائط المتعددة	الكل = كل حركة مرور الرسائل النصية القصيرة ورسائل الوسائط المتعددة مسموح بها الرسائل النصية الواردة فقط = يُسمح فقط بالرسائل النصية الواردة فقط الرسائل القصيرة الصادرة فقط = يُسمح بالرسائل القصيرة الصادرة فقط لا يوجد = غير مسموح بنقل الرسائل النصية القصيرة/رسائل الوسائط المتعددة
السماح بالمزامنة أثناء التجوال	السماح بالمزامنة أثناء التجوال قيد التشغيل = مفعل مطفأة = معطلة = معطلة اختيار المستخدم = اختيار المستخدم
السماح بالتجوال الصوتي	السماح بالتجوال الصوتي قيد التشغيل = مفعل مطفأة = معطلة = معطلة اختيار المستخدم = اختيار المستخدم
استخدام النظام خادم وكيل http النظام البروكسي	يعتمد استخدام خادم وكيل HTTP، الذي توفره إعدادات النظام في الإعدادات، على الشبكة المتصلة (WiFi أو APN)

شبكة APN

الإعدادات التالية متاحة فقط على Samsung SAFE 2.0 أو أعلى!

اسم العرض APN	اسم العرض APN	
اسم نقطة الوصول	اسم الشخص المسؤول	
بروتوكول الخادم الصادر	غير محدد	
	لا يوجد	
	برنامج مساعدة الشعب الفلسطيني	بروتوكول PAP
	تشاب	بروتوكول CHAP
	PAP أو CHAP	إما بروتوكول PAP أو بروتوكول CHAP
MCC - رمز البلد المتنقل	يتم إدخال MCC هنا، اترك هذا الحقل فارغاً، إذا كان يجب استخدام MCC الخاص ببطاقة SIM المُدخلة	
MNC - كود شبكة الجوال	يتم إدخال مركز الاتصالات المتعددة الجنسيات هنا، اترك هذا الحقل فارغاً، إذا كان يجب استخدام مركز الاتصالات المتعددة الجنسيات الخاص ببطاقة SIM المُدخلة	
عنوان الخادم	عنوان الخادم	
رقم منفذ الخادم	رقم منفذ الخادم	
عنوان وكيل الخادم	عنوان وكيل الخادم	
عنوان خادم رسائل الوسائط المتعددة	عنوان خادم رسائل الوسائط المتعددة (MMS)، بالنسبة للقياسي يُرجى تركه فارغاً	
رقم منفذ رسائل الوسائط المتعددة	رقم منفذ رسائل الوسائط المتعددة	
عنوان وكيل رسائل الوسائط المتعددة	عنوان وكيل رسائل الوسائط المتعددة	
اسم المستخدم	اسم المستخدم	
كلمة المرور	كلمة المرور	
نوع نقطة الوصول	الأنواع المسموح بها هي: "افتراضي"، "supl"، "mms" إذا تُرك هذا الحقل فارغًا، فسيتم استخدام "افتراضي، mms، supl"	
شبكة APN المفضلة	يُفضل استخدام APN	

بلوتوث

هنا، يمكن إجراء مجموعة متنوعة من إعدادات البلوتوث.

الإعدادات التالية متاحة فقط على Samsung KNOX 1.0 أو أعلى!

السماح باكتشاف الجهاز عبر البلوتوث	السماح باكتشاف الجهاز عبر البلوتوث
السماح بإقران البلوتوث	السماح بالاقتران بالبلوتوث
السماح بأجهزة سماعات البلوتوث	السماح بأجهزة سماعات البلوتوث
السماح بأجهزة البلوتوث التي تعمل بدون استخدام اليدين	السماح للأجهزة التي تعمل بالبلوتوث بدون استخدام اليدين
السماح لأجهزة Bluetooth A2DP	السماح ببث الصوت عبر Bluetooth A2DP بين الأجهزة
السماح بالمكالمات الصادرة	السماح بإجراء مكالمات صادرة عبر الإنترنت
السماح بنقل البيانات عبر البلوتوث	السماح بنقل البيانات عبر البلوتوث
السماح بالربط عبر البلوتوث	يسمح باستخدام الجهاز كمودم (اتصال بلوتوث بالإنترنت)
السماح بالاتصال بالكمبيوتر عبر البلوتوث	السماح بالاتصال بالكمبيوتر عبر البلوتوث

إدارة PIM

المبادلات

متوفر فقط مع Samsung KNOX 1.0 أو أعلى!

عنوان البريد الإلكتروني	عنوان البريد الإلكتروني للمستخدم المقدم يرجى ملاحظة "العناصر النائبة"، التي يمكنك استخدامها للعمل مع بيانات الاعتماد ولا تقوم بإجراء تغييرات يدوياً على كل جهاز بنقرة على **إظهار العناصر النائبة** يمكنك عرضها بنفسك
اسم مضيف الخادم	عنوان الخادم الخاص بخوادم Exchange الخاصة بك
اسم تسجيل الدخول	اسم تسجيل الدخول لجهاز المستخدم النهائي المعني، يرجى أيضًا ملاحظة "العناصر النائبة هنا
المجال	عنوان المجال
كلمة المرور (على مستوى الجهاز فقط)	اختياريًا، يمكن تزويد الجهاز الفردي بكلمة مرور، وفي حالة بقائها فارغة، سيُطلب من المستخدم إدخال كلمة مرور Exchange الخاصة به
عدد الأيام السابقة للمزامنة	عدد الأيام التي يتم فيها تحديد موعد مزامنة رسائل البريد الإلكتروني
التوقيع	يمكن إرفاق توقيع (تلميح: تتطلب بعض الأجهزة تنسيق HTML للتوقيع)
الحساب الافتراضي	ينشئ، أن حساب البريد هذا هو الحساب القياسي
استخدام طبقة مآخذ التوصيل الآمنة (SSL)	استخدام اتصال SSL
استخدام أمان طبقة النقل (TLS)	استخدام اتصال TLS
قبول جميع الشهادات	جميع الشهادات مقبولة. الرجاء تحديد هذا الخيار، إذا كان خادم Exchange لديك يستخدم شهادة موقعة ذاتياً

البريد الإلكتروني

هنا، يمكنك توزيع حسابات IMAP و POP على أجهزة المستخدم النهائي المعنية.

الإعدادات التالية متاحة فقط على Samsung KNOX 1.0 أو أعلى!		
عنوان البريد الإلكتروني	عنوان البريد الإلكتروني للمستخدم المقدم يرجى ملاحظة "العناصر النائبة"، التي يمكنك استخدامها للعمل مع بيانات الاعتماد ولا تقوم بإجراء تغييرات يدوياً على كل جهاز بنقرة على **إظهار العناصر النائبة** يمكنك عرضها بنفسك	
بروتوكول الخادم الوارد	بروتوكول الخادم الوارد	IMAP oder POP
عنوان الخادم الوارد	عنوان الخادم الوارد	
منفذ الخادم الوارد	منفذ الخادم الوارد	
تسجيل الدخول إلى الخادم الوارد/ اسم المستخدم	تسجيل الدخول إلى الخادم الوارد/اسم المستخدم	
كلمة مرور الخادم الوارد (على مستوى الجهاز فقط)	كلمة مرور الخادم الوارد (على مستوى الجهاز فقط)	
يستخدم الخادم الوارد SSL	يستخدم الخادم الوارد SSL	
يستخدم الخادم الوارد TLS	يستخدم الخادم الوارد TLS	
يقبل الخادم الوارد جميع الشهادات	الخادم الوارد يقبل جميع أنواع الشهادات	
بروتوكول الخادم الصادر	بروتوكول الخادم الصادر	SMTP
منفذ الخادم الصادر	منفذ الخادم الصادر	
يستخدم الخادم الصادر بيانات اعتماد إضافية	بيانات اعتماد إضافية للخادم الصادر. إذا تم تعيين هذا على "إيقاف التشغيل"، فسيتم استخدام إعدادات الخادم الصادر	
تسجيل الدخول إلى الخادم الصادر/اسم المستخدم	تسجيل الدخول إلى الخادم الصادر/اسم المستخدم	
كلمة مرور الخادم الصادر (على مستوى الجهاز فقط)	كلمة مرور الخادم الصادر	
يستخدم الخادم الصادر SSL	يستخدم الخادم الصادر SSL	
يستخدم الخادم الصادر TLS	يستخدم الخادم الصادر TLS	
يقبل الخادم الصادر جميع الشهادات	الخادم الصادر يقبل جميع أنواع الشهادات	
التوقيع	يمكن إرفاق التوقيع هنا (تلميح: تتطلب بعض الأجهزة تنسيق HTML للتوقيع)	

إعلام المستخدم عند تلقي بريد إلكتروني جديد	إعلام المستخدم عند تلقي بريد إلكتروني جديد

AE Gmail Exchange

معلومات: سيتم تطبيق هذا التكوين على تطبيق Gmail. لذا عليك الموافقة على Gmail وتثبيته.

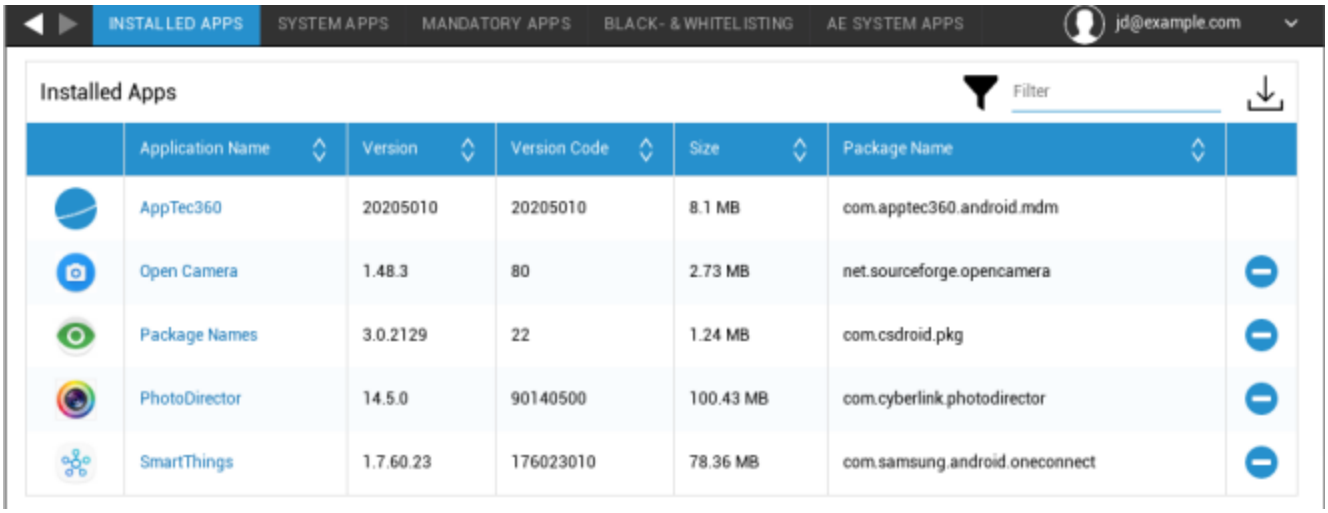
عنوان البريد الإلكتروني	عنوان البريد الإلكتروني للمستخدم المقدم يرجى ملاحظة "العناصر النائبة"، التي يمكنك استخدامها للعمل مع بيانات الاعتماد ولا تقوم بإجراء تغييرات يدوياً على كل جهاز بنقرة واحدة على إظهار العناصر النائبة يمكنك عرضها بنفسك
اسم مضيف الخادم	عنوان الخادم الخاص بخوادم Exchange الخاصة بك
اسم تسجيل الدخول	اسم تسجيل الدخول لجهاز المستخدم النهائي المعني، يرجى أيضًا ملاحظة "العناصر النائبة هنا
التوقيع	يمكن إرفاق توقيع (تلميح: تتطلب بعض الأجهزة تنسيق HTML للتوقيع)
عدد الأيام السابقة للمزامنة	عدد الأيام التي يتم فيها تحديد موعد مزامنة رسائل البريد الإلكتروني
معرّف الجهاز	معرّف EAS. اترك هذا فارغًا إذا كانت بيئتك لا تتطلب ذلك
استخدام طبقة مآخذ التوصيل الآمنة (SSL)	استخدام اتصال SSL
قبول جميع الشهادات	جميع الشهادات مقبولة. الرجاء تحديد هذا الخيار، إذا كان خادم Exchange لديك يستخدم شهادة موقعة ذاتياً
السماح بالحسابات غير المُدارة	السماح للمستخدم بإضافة حسابات إضافية
شهادة العميل	تحميل شهادة العميل إذا كان خادم Exchange الخاص بك يتطلب ذلك

إدارة التطبيقات

مدير تطبيقات المؤسسات

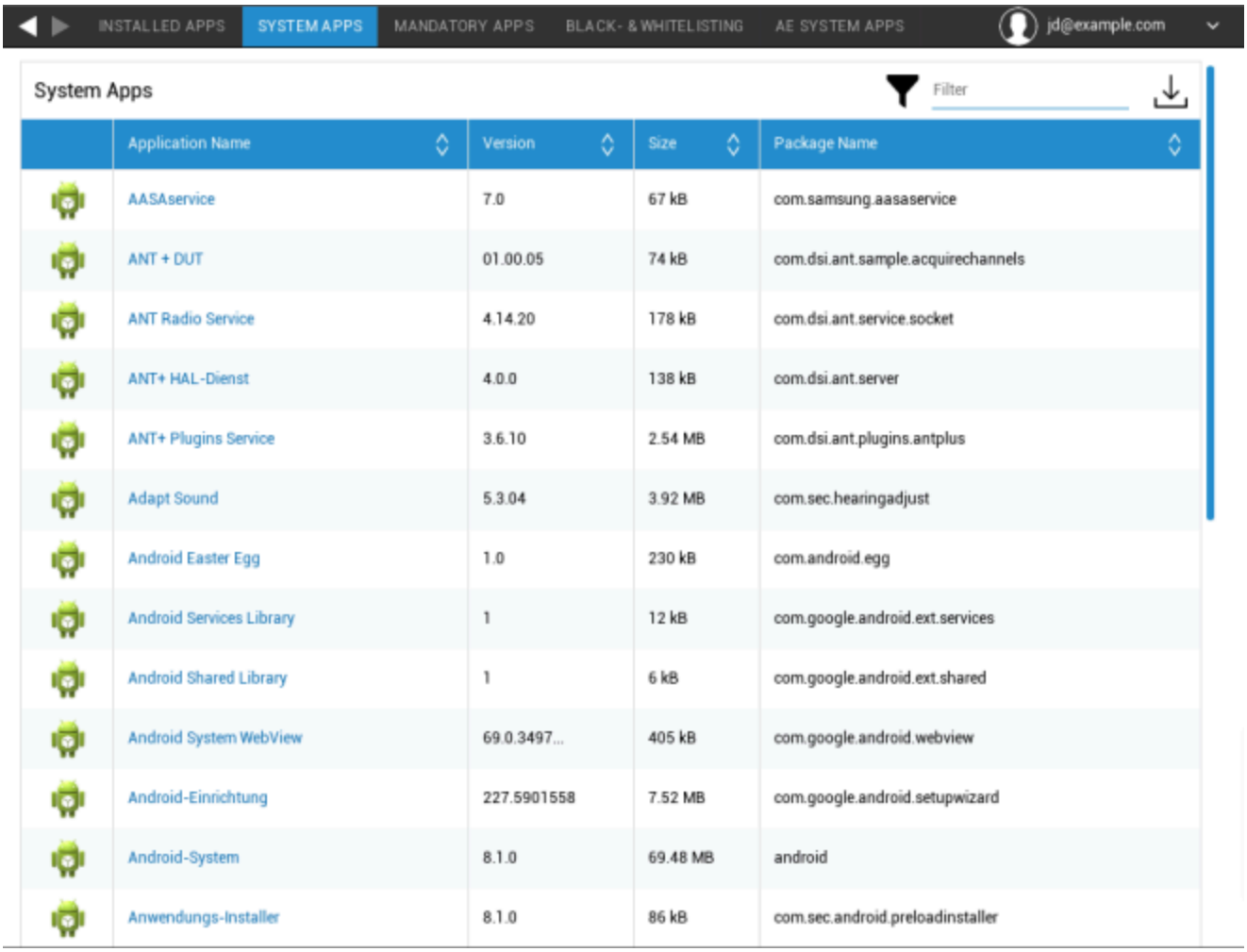
التطبيقات المثبتة (على مستوى الجهاز فقط)

هنا سيتم عرض جميع التطبيقات المثبتة حالياً على جهاز المستخدم النهائي.


INSTALLED APPS
SYSTEM APPS
MANDATORY APPS
BLACK- & WHITELISTING
AE SYSTEM APPS
jd@example.com
Installed Apps
Filter
Application Name
Version
Version Code
Size
Package Name
AppTec360
20205010
20205010
8.1 MB
com.apptec360.android.mdm
Open Camera
1.48.3
80
2.73 MB
net.sourceforge.opencamera
Package Names
3.0.2129
22
1.24 MB
com.csdroid.pkg
PhotoDirector
14.5.0
90140500
100.43 MB
com.cyberlink.photodirector
SmartThings
1.7.60.23
176023010
78.36 MB
com.samsung.android.oneconnect

تطبيقات النظام (على مستوى الجهاز فقط)

ضمن "تطبيقات النظام"، سيتم سرد جميع تطبيقات النظام المثبتة مسبقاً مع اسم الحزمة وإصدارها.



التطبيقات الإلزامية

في التطبيقات الإلزامية يمكنك تحديد التطبيقات التي يجب تثبيتها على الجهاز. اعتمادًا على التكوين والجهاز، سيتم تثبيت التطبيق تلقائيًا أو سيُطلب من المستخدم تثبيته.

يرجى العلم أنه يوصى باستخدام Android Enterprise لسهولة إدارة التطبيق.

السيناريوهات كما هو موضح أدناه:

تطبيقات متجر Play العادية

تحتاج عمليات تثبيت تطبيقات Playstore دائمًا إلى تفاعل المستخدم. بالإضافة إلى ذلك، يجب تهيئة حساب Google على الجهاز.

تثبيت التطبيق في المنزل

على أجهزة سامسونج سيتم تثبيت هذه التطبيقات بصمت. الاستثناء الوحيد هو الحاوية، حيث يتعين على المستخدم تأكيد التثبيت.

في أي سيناريو آخر، يتعين على المستخدم تأكيد تثبيت التطبيق.

تطبيقات متجر أندرويد بلاي ستور للمؤسسات

سيتم تثبيت هذه التطبيقات دائماً بصمت، دون تدخل المستخدم.

لإضافة تطبيق إلزامي، انقر على "+" وحدد التطبيق المطلوب من القائمة. يُرجى الانتباه إلى أنه لا يمكنك تثبيت التطبيقات من علامة التبويب "متجر Google Play"، إذا كان الجهاز مهيأً مع Android Enterprise إما على أنه مُدار بالكامل أو كحاوية.

في حالة استخدام Android Enterprise، حدد التطبيقات من قسم "متجر AE Play Store". لجعل التطبيقات متاحة هنا، قم بتأكيدها في متجر Google Enterprise Play من خلال الانتقال إلى الإعدادات العامة ← متجر AE Play Store ← تطبيقات متجر Play Store.

عند إزالة تطبيق إلزامي، سيتم أيضاً إلغاء تثبيته من الجهاز.

يمكنك النقر على اسم التطبيق في قائمة التطبيقات الإلزامية والانتقال إلى علامة التبويب "التكوين" لتهيئة التطبيق. يتطلب ذلك استخدام Android Enterprise ويجب أن يدعم التطبيق ذلك. لذلك تعتمد الخيارات المتاحة على التطبيق المحدد.

تطبيقات نظام AE

هنا يمكنك تمكين تطبيقات النظام لأجهزة Android Enterprise. يرجى الأخذ في الاعتبار أن التطبيق المحدد يجب أن يكون في مخزن النظام، وإلا فلن يحدث شيء. 296

القيود والإعدادات

القائمة السوداء والبيضاء

هنا يمكنك تحديد قائمة سوداء أو بيضاء. سيتم حظر جميع التطبيقات الموجودة في القائمة السوداء. سيتم حظر جميع التطبيقات غير الموجودة في القائمة البيضاء. القائمة السوداء الفارغة لا تحظر أي شيء، بينما القائمة البيضاء الفارغة تحظر كل شيء*

** سيتم إدراج جميع التطبيقات والتطبيقات الإلزامية من متجر تطبيقات المؤسسات في القائمة البيضاء تلقائيًا. لا تحتاج إلى إضافتها يدويًا*

عند النقر على "+" يمكنك إما البحث عن تطبيق تريد إضافته إلى القائمة السوداء أو البيضاء أو إدخال اسم الحزمة يدويًا.

قيود تطبيق النظام

ضمن "قيود تطبيقات Sys App Restrictions"، يمكنك حظر التطبيقات والخدمات المثبتة مسبقًا، من بين أمور أخرى، كما يحلو لك.

تعطيل المتصفح	تعطيل المتصفح القياسي
تعطيل التقويم	تعطيل التقويم الأصلي
تعطيل الآلة الحاسبة	تعطيل الآلة الحاسبة
تعطيل متصفح كروم	تعطيل متصفح كروم
تعطيل الساعة	تعطيل الساعة
تعطيل جهات الاتصال	تعطيل جهات الاتصال
تعطيل برنامج الاتصال المعطل	تعطيل برنامج الاتصال الأصلي
تعطيل البريد الإلكتروني	تعطيل البريد الإلكتروني
تعطيل الصرف	تعطيل حسابات الصرف
تعطيل فيسبوك	تعطيل تطبيق فيسبوك
تعطيل المعرض	تعطيل تطبيق المعرض الأصلي
تعطيل Gmail	تعطيل Gmail
تعطيل كتب Google	تعطيل كتب Google
تعطيل كشك Google Play Kiosk	تعطيل كشك Google Play Kiosk
تعطيل خرائط Google	تعطيل خرائط Google
تعطيل موسيقى Google	تعطيل موسيقى Google
تعطيل أفلام Google	تعطيل أفلام Google
تعطيل متجر جوجل بلاي ستور	تعطيل متجر Google Play Store (متجر التطبيقات العام)
تعطيل Google Plus	تعطيل Google Plus
تعطيل بحث Google	تعطيل بحث Google
تعطيل Google Talk / Google Hangouts	تعطيل Google Talk / Google Hangouts
تعطيل مشغل الموسيقى	تعطيل تطبيق مشغل الموسيقى الأصلي
تعطيل الإعدادات	تعطيل إعدادات الجهاز
تعطيل مجموعة أدوات Sim Toolkit	تعطيل خدمات مجموعة أدوات Sim Toolkit
تعطيل الرسائل النصية القصيرة/رسائل الوسائط المتعددة	تعطيل الرسائل النصية القصيرة/رسائل الوسائط المتعددة
تعطيل التجوّل الافتراضي	تعطيل خدمات التجوّل الافتراضي
تعطيل يوتيوب	تعطيل يوتيوب

تطبيقات سامسونج

ضمن "تطبيقات سامسونج"، يمكنك تحديد إعدادات و/أو قيود إضافية لأجهزة سامسونج.

تعطيل تشغيل AllShare Play / Samsung Link	تعطيل تشغيل AllShare Play / Samsung Link
تعطيل ChatON	تعطيل ChatON
تعطيل محور اللعبة	تعطيل محور اللعبة
تعطيل اللعب الجماعي	تعطيل اللعب الجماعي
تعطيل المساعدة	تعطيل مساعدة سامسونج
تعطيل KNOX	تعطيل حاوية Samsung KNOX Container
تعطيل المذكرة	تعطيل المذكرة الصوتية
تعطيل ملفاتي	تعطيل ملفاتي
تعطيل القارئ الضوئي	تعطيل القارئ الضوئي
تعطيل مكتب بولاريس بولاريس	تعطيل مكتب بولاريس بولاريس
تعطيل مركز القراءات المعطل / كتب سامسونج	تعطيل مركز القراءات المعطل / كتب سامسونج
تعطيل مذكرة S مذكرة	تعطيل تطبيق Samsung Memo Memo
تعطيل المترجم S مترجم S	تعطيل تطبيق مترجم سامسونج Samsung Translator
تعطيل صوت S صوتي	تعطيل المساعد الصوتي S المساعد الصوتي
تعطيل تطبيقات سامسونج	تعطيل متجر تطبيقات سامسونج
تعطيل Samsung Hub	تعطيل متاجر سامسونج الترفيهية
تعطيل مشغل الفيديو	تعطيل مشغل الفيديو
تعطيل مسجل الصوت	تعطيل مسجل الصوت
تعطيل WatchON	تعطيل WatchON (يحاكي جهاز التحكم عن بُعد)

تطبيقات هواوي

ضمن "تطبيقات Huawei"، يمكنك تحديد إعدادات و/أو قيود إضافية على جهاز Huawei.

تعطيل DLNA	تعطيل DLNA
تعطيل مثبت التطبيق	تعطيل مثبت التطبيق
تعطيل مدير الملفات	تعطيل مدير الملفات
تعطيل مدير النسخ الاحتياطي	تعطيل مدير النسخ الاحتياطي
تعطيل محدث النظام	تعطيل محدث النظام
تعطيل صندوق الأدوات	تعطيل صندوق الأدوات
تعطيل الطقس	تعطيل الطقس
تعطيل راديو FM	تعطيل راديو FM

إعدادات إدارة التطبيق

هنا يمكنك تحديد سلوك تحديث تطبيقات InHouse Apps.

يحدد تردد التحقق من التحديث عدد المرات التي يبحث فيها تطبيق AppTec360 عن تحديثات لتطبيقات InHouse. بمجرد اكتشاف إصدار جديد، سيتم تنزيله وتثبيته.

تحدد عتبة Wi-Fi ما إذا كان يجب أن يقتصر التنزيل على اتصالات Wi-Fi إذا كان التطبيق أكبر من العتبة التي قمت بتكوينها. إذا كان أصغر أو إذا لم تحدد عتبة، فسيتم تنزيل التطبيق في شبكة Wi-Fi وفي شبكة خلوية.

متجر تطبيقات المؤسسات

يُرجى العلم أن التطبيقات التي تتم إضافتها هنا (متجر تطبيقات المؤسسات) لن يتم تثبيتها تلقائيًا على الجهاز (الأجهزة). يجب على المستخدم فتح متجر تطبيقات المؤسسات على الجهاز وتثبيت التطبيق يدوياً.

إذا كنت ترغب في تثبيت التطبيقات تلقائيًا على الجهاز، يُرجى الانتقال إلى "إدارة التطبيقات" → "مدير تطبيقات المؤسسة" → "التطبيقات الإلزامية" وإضافة التطبيقات المطلوبة هناك.

تحت هذه النقطة، يمكنك توزيع تطبيقات اختيارية على المستخدمين.

بلاي ستور

انقر على "+" لإضافة تطبيق متجر Play إلى المتجر. إذا كنت تستخدم Android Enterprise، يُرجى الانتقال إلى "متجر تطبيقات إدارة التطبيقات Enterprise Play Store". اعلم أيضًا أنه يجب تكوين حساب Google على الجهاز لتثبيت التطبيقات المحددة هنا.

داخل الشركة

تحت نقطة "داخلياً"، يمكنك تحميل التطبيقات المطورة داخلياً وتوزيعها.

انقر على زر "+" لإضافة تطبيق InHouse إلى متجر تطبيقات المؤسسة والذي يمكن للمستخدم تثبيته بعد ذلك. في هذا الحوار يمكنك أيضاً تحميل تطبيق InHouse جديد.

متجر Play Play للمؤسسات

يرجى الانتباه إلى أن التطبيقات التي تتم إضافتها هنا (متجر Play للمؤسسات) لن يتم تثبيتها تلقائيًا على الجهاز (الأجهزة). يجب على المستخدم فتح متجر Play على الجهاز وتثبيت التطبيق يدويًا.

إذا كنت ترغب في تثبيت التطبيقات تلقائيًا على الجهاز، يُرجى الانتقال إلى "إدارة التطبيقات" → "مدير تطبيقات المؤسسة" → "التطبيقات الإلزامية" وإضافة التطبيقات المطلوبة هناك.

تحت هذه النقطة، يمكنك توزيع تطبيقات اختيارية على المستخدمين.

هنا يمكنك إضافة تطبيقات إلى متجر Playstore الخاص بمؤسسات Android. يُرجى ملاحظة أنه يجب عليك الموافقة على التطبيقات في الإعدادات العامة ← متجر Play للمؤسسات ← تطبيقات متجر Play. ستتم إضافة هذه التطبيقات إلى متجر Google Play Store العادي.

اعلم أيضًا أنه يجب عليك أولاً تحديد تخطيط مع التطبيقات في الإعدادات العامة ← إدارة التطبيقات ← إدارة التطبيقات ← تخطيط متجر AE Play ← تخطيط المتجر.

يجب أن تكون التطبيقات في تخطيط قبل أن تتمكن من إضافتها بنجاح إلى المتجر.

وضع الكشك والتشغيل

وضع الكشك

يسمح لك وضع الكشك بتحديد تطبيق أو عنوان URL مسبقاً. ثم سيكون من الممكن تشغيل/زيارة هذا التطبيق و/أو عنوان URL حصرياً.

وبالمثل، يمكن إلغاء تنشيط أزرار الأجهزة المختلفة في وضع الكشك المتنوع.

بدء التشغيل التلقائي	بدء تشغيل وضع الكشك تلقائياً، بمجرد وصول الملف الشخصي إلى جهاز المستخدم النهائي
وضع الكشك المجدول؟	يمكنك تخطيط وقت لوضع الكشك، وسيبدأ هذا بعد ذلك وينتهي تلقائيًا، في الوقت الذي تحدده أنت
وقت البدء	وقت البدء
الوقت بالدقائق	الوقت بالدقائق، وبعد ذلك يجب أن ينتهي وضع الكشك مرة أخرى

نوع التطبيق

تطبيق واحد	إذا كنت ترغب في بدء تشغيل التطبيق في وضع الكشك، حدد "حزمة" ضمن "نوع التطبيق"
تطبيق الكشك	انقر هنا، من أجل تحديد التطبيق الذي يجب تشغيله في وضع الكشك ستجد النظرة العامة المعتادة لإدارة التطبيقات يمكنك الاختيار بين "متجر جوجل بلاي" و"تطبيقات أندرويد الداخلية" و"اسم الحزمة"

نوع التطبيق	

عنوان URL	إذا كنت تريد تشغيل عنوان URL في وضع الكشك، حدد "عنوان URL" ضمن "نوع التطبيق" ثم حدد عنوان URL الذي تريده
مسح المتصفح بعد عدم النشاط	هنا يمكنك تحديد فاصل زمني بالدقائق، وبعد ذلك يجب إعادة تشغيل وضع الكشك
مسح ذاكرة التخزين المؤقت للويب وملفات تعريف الارتباط	إذا قمت بتفعيل هذه الوظيفة، فبعد إعادة تشغيل وضع الكشك، سيتم مسح ذاكرة التخزين المؤقت للويب (ملفات تعريف الارتباط والصور المخزنة مؤقتًا)
سياسة نفس المنشأ	في حالة تفعيل هذه الوظيفة، يمكن للمستخدم تصفح الصفحات الفرعية لعنوان URL المحدد فقط على سبيل المثال، قمت بتحديد عنوان URL التالي:www.mypage.com بعد ذلك، يمكن للمستخدم تصفح الرابط التالي: www.mypage.com/subpage
عناوين URL المدرجة في القائمة البيضاء	هنا يمكنك الاحتفاظ بقائمة بيضاء، كل عناوين URL هذه مسموح بها 1 عنوان URL كحد أقصى لكل سطر يجب أن يبدأ عنوان URL ب http:/ أو https://
عناوين URL المدرجة في القائمة السوداء	هنا يمكنك الاحتفاظ بقائمة سوداء، جميع عناوين URL هذه غير مسموح بها 1 عنوان URL كحد أقصى لكل سطر يجب أن يبدأ عنوان URL ب http:/ أو https://
اتجاه الشاشة	يتعلق هذا الإعداد بتعديلات الشاشة تلقائي = تلقائي عمودي = تنسيق عمودي أفقي = الوضع الأفقي

تطبيق متعدد	إذا قمت بتحديد وضع الكشك "متعدد التطبيقات"، فسيتم فرض استخدام مشغّل AppTec360.
التطبيقات	التطبيق: اختر تطبيق Playstore أو تطبيق داخلي كتطبيق كشك. من الممكن أيضاً إدخال اسم الحزمة. يجب تثبيت تطبيق الكشك المحدد على الجهاز. تذكر تعيين تطبيق الكشك على أنه إلزامي. اختصار على الشاشة الرئيسية: إذا تم الضبط على "تشغيل" سيتم إنشاء اختصار على الشاشة الرئيسية. إذا تم الضبط على "إيقاف التشغيل" سيظل التطبيق يظهر في قائمة التطبيقات.

تم تمكين كلمة مرور الخروج	إذا قمت بتفعيل هذه الوظيفة، فمن الممكن للمستخدم، إنهاء وضع الكشك، بكلمة مرور تم تحديدها مسبقًا من قبلك
كلمة مرور الخروج	هذه هي كلمة المرور، التي تم تحديدها مسبقاً من قبلك
طي شريط الحالة تلقائيًا	في حالة التمكين، سيتم عرض شريط الحالة تلقائيًا بشكل مطوي. باستخدام هذا الخيار يمكن للمستخدمين رؤية المعلومات في شريط الحالة، ولكن لا يمكنهم الوصول إلى وظائفه
تعطيل شريط الحالة	يحتوي شريط الحالة على إشعارات واختصارات ومعلومات. متاح فقط لأجهزة سامسونج المزودة بـ KNOX 1.0 أو أكبر.
تعطيل مفاتيح مستوى الصوت	تعطيل مفاتيح مستوى الصوت (متوفر فقط على أجهزة سامسونج المزودة بنظام KNOX 1.0 أو أعلى)
تعطيل مفتاح التشغيل/إيقاف التشغيل	تعطيل مفتاح التشغيل/إيقاف التشغيل (متوفر فقط على أجهزة سامسونج المزودة بنظام KNOX 1.0 أو أعلى)
تعطيل زر الصفحة الرئيسية	تعطيل زر الصفحة الرئيسية. إذا تم تنشيط هذه الوظيفة، فلا يمكن إنهاء وضع الكشك إلا في وحدة تحكم AppTec360 (متوفر فقط على أجهزة Samsung المزودة ب KNOX 1.0 أو أعلى)
تعطيل شريط التنقل	باستخدام هذا يمكنك تعطيل شريط التنقل (رجوع / قائمة) إذا تم تنشيط هذه الوظيفة، فلا يمكن إنهاء وضع الكشك إلا في وحدة تحكم AppTec360 (متوفر فقط على أجهزة Samsung المزودة ب KNOX 1.0 أو أعلى)

إعدادات تحديث التطبيق	
السماح بتحديثات التطبيق	سيُطلب من المستخدمين إجراء تحديثات للتطبيقات حتى عندما يكون وضع Kiosk نشطاً. على الأجهزة المزودة بـ Samsung KNOX، سيتم تحديث التطبيقات بصمت.
نافذة التحديث	قم بتعيين فاصل زمني يُطلب فيه من المستخدمين تثبيت تحديثات التطبيق.

برنامج TeamViewer	
تمكين الوصول غير المراقب	إذا تم تمكينه، يمكن للمسؤولين التحكم بالجهاز عن بُعد دون تدخل المستخدم. يجب تثبيت تطبيق TeamViewer Host على الجهاز.

مُشغِّل تطبيقات AppTec360

تمكين مشغل التطبيقات AppTec360	تشغيل: تمكين مشغّل AppTec360. يجب على المستخدم تعيينه كمشغل افتراضي مرة واحدة. ملاحظة: إذا تم تمكين وضع الكشك، وتم ضبط وضع الكشك على "تطبيق متعدد"، فسيتم فرض استخدام مشغل AppTec360.
أيقونات كبيرة	تشغيل: يعرض نسخة أكبر من أيقونات التطبيقات في المشغّل
إخفاء أيقونة تطبيق AppTec360	تشغيل: يخفي تطبيق AppTec360 بالكامل
إخفاء أيقونة متجر AppTec360	تشغيل: يخفي AppTec360 Enterprise AppStore بالكامل

إعدادات AppTec360

تمكين تطبيق إعدادات AppTec360 AppTec360	يوفر تطبيق إعدادات AppTec360 AppTec360 التحكم في اتصالات الواي فاي والبلوتوث
تمكين الإعدادات في التطبيق المتعدد وضع الكشك	في حالة التمكين، يمكن للمستخدمين الوصول إلى تطبيق إعدادات AppTec360 أثناء تنشيط وضع الكشك متعدد التطبيقات

جهاز التحكم عن بُعد

سبلاش توب

يعرض الحالة الحالية لإعداد Splashtop. هنا سترى الخطوات التي تحتاج إلى تنفيذها للوصول إلى الجهاز عن بُعد عبر Splashtop. هنا تحتاج أيضًا إلى إدخال رمز النشر الذي يمكنك الحصول عليه من موقع Splashtop الإلكتروني. رمز النشر مطلوب للاتصال بالجهاز.

برنامج Teamviewer

يعرض الحالة الحالية لإعداد برنامج Teamviewer. هنا سترى الخطوات التي تحتاج إلى تنفيذها للوصول إلى الجهاز عن بُعد عبر برنامج Teamviewer.

إدارة المحتوى

صندوق المحتوى

هنا يمكنك تمكين Contentbox لهذا الجهاز. بمجرد التفعيل، سيتم تثبيت تطبيق Contentbox على الجهاز.

متصفح آمن

هنا يمكنك تمكين المتصفح الآمن لهذا الجهاز. بمجرد التفعيل، سيتم تثبيت تطبيق المتصفح الآمن على الجهاز. يمكن تهيئة هذا المتصفح لتقديم متصفح ويب على الجهاز الذي يقتصر على احتياجاتك.

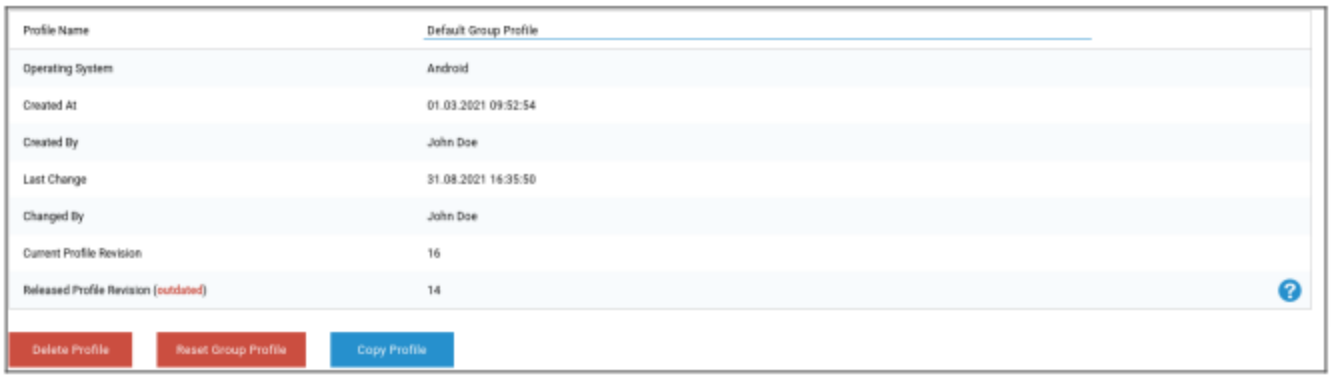
تتطلب كلمة مرور	مطالبة المستخدم بإعداد كلمة مرور واستخدامها للوصول إلى المتصفح.
تقييد التنزيلات / فتح في	حظر التنزيلات من المواقع الإلكترونية
تقييد التحميلات	تقييد عمليات التحميل إلى عناوين URL معينة. لا توفر عنوان URL لحظر التحميل بالكامل
السماح بالنسخ	السماح بنسخ النص أو قصه أو مشاركته داخل صفحات الويب.
السماح بالتقاط الشاشة	السماح بالتقاط لقطات الشاشة.
تواتر تنظيف البيانات	حدد التردد الذي يجب إزالة جميع بيانات المستخدم (السجل وذاكرة التخزين المؤقت وما إلى ذلك) تلقائيًا.
الإشارات المرجعية للشركة	ستظهر الإشارات المرجعية في مجلد "الإشارات المرجعية للشركة" في الإشارات المرجعية للمتصفحات. وهي غير قابلة للتحرير من قبل المستخدم.
إخفاء شريط العنوان	إخفاء شريط العناوين بحيث لا يرى المستخدم عنوان URL الذي يزوره
القائمة البيضاء داخل المتصفح (بدون البوابة العالمية)	تمكين القائمة البيضاء لعناوين URL من جانب العميل. - يتم إدراج الإشارات المرجعية للشركة دائمًا في القائمة البيضاء - مدعوم لـ 100 عنوان URL فقط - يرجى استخدام البوابة العالمية لقائمة سوداء وبيضاء غير محدودة
القائمة السوداء والقائمة البيضاء المستندة إلى البوابة	تتطلب القائمة السوداء المتطلبات التالية: - بوابة عالمية للتطبيق AppTec360 عاملة ("الإعدادات العامة" → "البوابة العالمية") - تكوين VPN عامل مع خادم DNS محدد ("الإعدادات العامة" → "البوابة العالمية" → "إعدادات VPN") - تكوين قائمة سوداء ("الإعدادات العامة" → "البوابة العالمية" → "القائمة السوداء للنطاق") - اتصال VPN صالح في الملف الشخصي ("إدارة الاتصال" → "VPN")

التكوين ويندوز 10 كمبيوتر شخصي

جنرال لواء

نظرة عامة على ملف تعريف المجموعة (على مستوى المجموعة فقط)

عند فتح الملف الشخصي للمجموعة، ستحصل على نظرة عامة سريعة على الملف الشخصي.



اسم الملف الشخصي	اسم الملف الشخصي (يمكن تغييره هنا)
نظام التشغيل	نظام التشغيل الذي تم إنشاء ملف التعريف له
تم إنشاؤها في	وقت الإنشاء
تم إنشاؤها بواسطة	منشئ الملف الشخصي
آخر تغيير	وقت آخر تغيير في الملف الشخصي
تم التغيير بواسطة	الحساب الذي أجرى التغييرات الأخيرة
مراجعة الملف الشخصي الحالي	مراجعة حالة الملف الشخصي المحفوظة
مراجعة الملف الشخصي الصادر	مراجعة الملف الشخصي المعين ("تعيين الآن"). إذا كانت التسمية تظهر "(قديم)" خلف النص، فهذا يعني أنك قمت بحفظ ملف التعريف ولكنك لم تعيّنه بعد، لذا ستظل الأجهزة تحصل على الإصدار الأقدم.

نظرة عامة على الجهاز (على مستوى الجهاز فقط)

نظرة عامة موجزة عن الجهاز، والتي تحتوي على ما يلي:

اسم الكمبيوتر الشخصي	اسم الكمبيوتر الشخصي
العميل	الأجهزة نوع ويندوز الأجهزة
آخر موقع معروف	خط العرض وخط الطول لآخر موقع معروف للأجهزة
التطبيقات الإلزامية المعينة	عدد التطبيقات الإلزامية المعينة للجهاز
معرف الكمبيوتر الشخصي	معرف الكمبيوتر الشخصي
إصدار نظام التشغيل	يعرض إصدار ويندوز الخاص بك
إصدار نظام التشغيل	إصدار Windows المثبت حالياً
بناء نظام التشغيل	بناء ويندوز الحالي
نظام التشغيل	نظام التشغيل المثبت حالياً
الرقم التسلسلي	الرقم التسلسلي للجهاز
ملكية الجهاز	نوع الملكية المكوَّن
نوع الجهاز	نوع الجهاز
متجذر	يظهر ما إذا كان الجهاز متجذرًا أم لا
متوافق	يظهر ما إذا كان الجهاز متوافقاً أم لا
آخر ظهور	التاريخ والوقت، عندما تم إجراء التغييرات على الملف الشخصي
تعيين المستخدم	يعرض المستخدم أو المجموعة التي تم تعيين هذا الجهاز لها حالياً. يمكنك نقل الجهاز عن طريق تحديد مستخدم أو مجموعة مختلفة من القائمة المنسدلة.

الإعدادات

السماح بالتحديث التلقائي	السماح بتحديثات نظام التشغيل التلقائية أو عدم السماح بها.

مراجعة التكوين (على مستوى الجهاز فقط)

هنا ستتلقى نظرة عامة على ملف تعريف المجموعة المعين للجهاز.

إذا قمت بالنقر على الملف الشخصي للمجموعة، فستتمكن من الوصول إلى الملف الشخصي مباشرةً ويمكنك إجراء الإعدادات.

باستخدام الرمز، يمكنك إعادة التطبيقات المعينة إلى إعدادات ملف تعريف المجموعة.

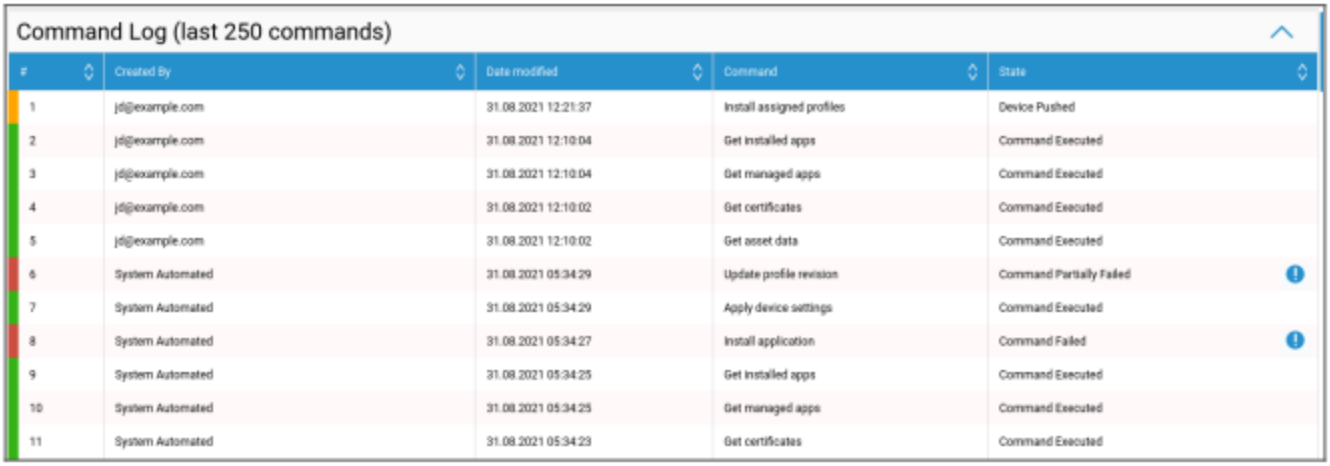
باستخدام الرمز، يمكنك إعادة ضبط ملف تعريف الجهاز بحيث لا يحتوي على أي إعدادات على الإطلاق.

تشير عبارة "تتوفر مراجعة أحدث" إلى أن ملف تعريف المجموعة قد تم تغييره وحفظه ولكن لم يتم تعيينه. يجب تعيين ملف تعريف المجموعة باستخدام "تعيين الآن" على مستوى المجموعة لتطبيق التغييرات على الأجهزة.

سجل الجهاز (على مستوى الجهاز فقط)

سجل الأوامر

هنا يمكنك معرفة الأوامر التي تم إصدارها للجهاز وما هي حالتها.



يتم إنشاء الأوامر التي تم إنشاؤها بواسطة "النظام الآلي" تلقائياً بواسطة النظام.

حالات الأوامر المحتملة

تم دفع الجهاز	تم إرسال طلب دفع إلى خدمة الدفع (مثل APNS) لإخبار الجهاز بالاتصال مرة أخرى بخادم EMM.
تم إنشاء الأمر	تم إنشاء الأمر في النظام.
تم إرسال الأمر	تم إرسال الأمر إلى الجهاز بعد اتصاله بالخادم.
تم تنفيذ الأمر	تم تنفيذ الأمر بنجاح.
فشل الأمر	فشل الأمر. *
فشل الأمر جزئياً	اعتمادًا على نظام تشغيل الجهاز قد يتم تجميع بعض الأوامر معًا. في هذا فشلت بعض أجزاء مجموعة الأوامر هذه. *
تم تنفيذ الأمر، وفشل الأمر في النهاية	تم تنفيذ الأمر ولكن ربما لم يتم تنفيذه.
إعادة دفع الأمر	تم إعادة دفع الأمر من قبل مستخدم.
مهملة	تم تجاهل الأمر. على سبيل المثال لأنه تم استبداله بأمر آخر أو تم إعادة تسجيل الجهاز وإزالة الأوامر القديمة

*إذا كانت هناك علامة تعجّب خلف الرسالة، يمكنك الحصول على مزيد من المعلومات من خلال تمرير مؤشر الماوس فوق الرمز.

إدارة الأصول (على مستوى الجهاز فقط)

معلومات الجهاز

الشركة المصنعة	الشركة المصنعة للجهاز
الطراز	طراز الجهاز
رقم الموديل	رقم الموديل
نظام التشغيل	نظام التشغيل
إصدار نظام التشغيل	إصدار نظام التشغيل
الرقم التسلسلي	الرقم التسلسلي
معرف الصرف	معرف الصرف
إجمالي ذاكرة الوصول العشوائي (RAM)	إجمالي ذاكرة الوصول العشوائي (RAM)
دقة العرض	دقة العرض
لغة الهاتف	لغة الجهاز
إصدار البرنامج الثابت	إصدار البرنامج الثابت
إصدار عميل DM	إصدار عميل إدارة الأجهزة
إصدار الأجهزة	إصدار الجهاز
بنية وحدة المعالجة المركزية	بنية وحدة المعالجة المركزية (نوع المعالج)

خلوي

شبكة ناقل الشريحة SIM	شبكة الناقل
رقم الهاتف	رقم الهاتف
حالة التجوال	حالة التجوال
IMEI	IMEI
IMSI	IMSI
البرنامج الثابت للمودم	البرنامج الثابت للمودم

معلومات المزامنة

اتصال DM الفوري	يجب أن يقوم الجهاز على الفور بإنشاء اتصال بـ AppTec
وقت إعادة المحاولة الأولي	وقت إعادة المحاولة الأولية لهذا الاتصال الأول
إعادة محاولة الاتصال	عدد محاولات إعادة الاتصال الجديدة، بعد قطع الاتصال من "إدارة الاتصال" أو خطأ على مستوى WinInet
الحد الأقصى لوقت النوم	الحد الأقصى لوقت السكون بعد خطأ في إرسال الحزمة
إعادة محاولة المزامنة الأولى	وقت المرحلة الأولى بعد التسجيل
فترة إعادة المحاولة الأولى	وقت المرحلة الأولى بعد التسجيل
إعادة محاولة المزامنة الثانية	وقت المرحلة الثانية بعد التسجيل
الفاصل الزمني لإعادة المحاولة الثانية	وقت المرحلة الثانية بعد التسجيل
إعادة محاولة المزامنة المنتظمة	وقت المراحل الإضافية بعد التسجيل
الفاصل الزمني لإعادة المحاولة المنتظمة	وقت المراحل الإضافية بعد التسجيل

إدارة الأمن

مكافحة السرقة (على مستوى الجهاز فقط)

معلومات GPS (على مستوى الجهاز فقط)

هنا يمكنك تحديد موقع الجهاز الحالي/الأخير. يمكن حماية تحديد الموقع باستخدام كلمة مرور واحدة أو حتى كلمتي مرور - انظر: "الإعدادات العامة"> "الخصوصية"> "الوصول إلى نظام تحديد المواقع العالمي"

إعدادات نظام تحديد المواقع العالمي (GPS)

تمكين تتبع نظام تحديد المواقع العالمي (GPS)	تمكين المزامنة المنتظمة لمعلومات GPS.
فترة التتبع	قم بتعيين الفاصل الزمني لمزامنة معلومات GPS.

تهيئة الأمان

رمز المرور

الحد الأدنى لطول كلمة المرور	الحد الأدنى لطول كلمة المرور	
تكوين كلمة المرور	يحدد عدد الأحرف المحددة التي يجب أن تحتويها كلمة المرور وهي تتألف من حروف كبيرة وحروف صغيرة وأرقام ورموز خاصة	
جودة كلمة المرور	هنا يمكنك ضبط جودة كلمة المرور	
	أبجدي رقمي	الأرقام والحروف فقط
	رقمي	الأرقام فقط
	رقمي أو أبجدي رقمي	أرقام أو أرقام وحروف
قفل الحد الأقصى لوقت عدم النشاط	عدد دقائق عدم نشاط المستخدم على الجهاز، وبعد ذلك سيتم قفل الجهاز. يجب على المستخدم إلغاء قفل الجهاز بعد هذا الوقت، عن طريق إدخال كلمة مرور الجهاز.	
انتهاء صلاحية كلمة المرور	تعيين الوقت حتى يجب تعيين كلمة مرور جديدة	
تقييد سجل كلمات المرور	عدد كلمات المرور المستخدمة سابقاً، غير مسموح بها	
الحد الأقصى لمحاولات كلمة المرور الفاشلة	عدد المرات التي يمكن فيها إدخال كلمة المرور بشكل غير صحيح، قبل إجراء مسح كامل للجهاز	

مضاد الفيروسات

إعدادات مكافحة الفيروسات - ضبط إعدادات الفحص	
نوع الفحص	تحديد ما إذا كنت تريد إجراء فحص سريع أو فحص كامل
تعيين بدء المسح الضوئي	يحدد الوقت من اليوم الذي سيبدأ فيه Windows Defender عملية الفحص
تردد المسح الضوئي	تحديد اليوم الذي يجب تشغيل فحص Windows Defender فيه
تكرار تحديث التوقيع	تحديد الفاصل الزمني بالساعات الذي سيتم استخدامه للتحقق من وجود توقيعات

تكوين نوع الملفات للمسح الضوئي	
السماح بالمسح الضوئي لملفات الأرشيف	السماح أو عدم السماح بمسح الأرشيفات (مثل .zip) عند الوصول إليها.
السماح بمسح البرامج النصية	السماح بوظيفة فحص البرامج النصية لـ Windows Defender أو عدم السماح بها.
السماح بمسح رسائل البريد الإلكتروني	السماح بالمسح الضوئي لرسائل البريد الإلكتروني أو عدم السماح به.
السماح بمسح ملفات الشبكة	السماح بمسح ملفات الشبكة أو عدم السماح بمسح ملفات الشبكة.
السماح بإجراء مسح كامل لمحركات أقراص الشبكة المعينة	السماح بالمسح الضوئي لمحركات أقراص الشبكة المعينة أو عدم السماح به (يتم تمكينه فقط عند تمكين الفحص الكامل).
التحكم في المسح الضوئي ثنائي الاتجاه	يتحكم في مجموعات الملفات التي يجب مراقبتها.
السماح بالمسح الكامل لمحركات الأقراص القابلة للإزالة	السماح بالمسح الكامل لمحركات الأقراص القابلة للإزالة أو عدم السماح به. فقط أثناء بدء الفحص الكامل.

نوع الملفات المراد استبعادها من الفحص	
تجاهل أنواع الملفات للمسح الضوئي	تحديد مجموعة من أنواع امتدادات الملفات. كل امتداد ملف لكل حقل.
تجاهل مسارات الدليل	تحديد مجموعة من مسارات الدليل من أجل عدم مسحها ضوئياً. مسار واحد لكل حقل. أمثلة: "C:\ مثال" أو "C:\Windows" أو "C:\ Users".
استبعاد العمليات من الفحص	استبعاد الملفات التي تم فتحها بواسطة عمليات محددة من فحوصات برنامج Microsoft Defender لمكافحة الفيروسات. . مسار واحد لكل حقل. أمثلة: "C:\ myFile.exe"، "C:\myScript.bat"، "C:\Windows\myProcess.exe"

إعدادات إضافية	
السماح بالمراقبة في الوقت الحقيقي	السماح بوظيفة المراقبة الفورية لنظام Windows Defender أو عدم السماح بها
السماح بمراقبة السلوك	السماح بوظيفة مراقبة سلوك Windows أو عدم السماح بها
السماح بالحماية السحابية	السماح أو عدم السماح لـ Windows Defender بإرسال معلومات إلى Microsoft حول أي مشكلة يعثر عليها. ستقوم Microsoft بتحليل تلك المعلومات، ومعرفة المزيد عن المشكلة التي تؤثر على الجهاز، وتقديم حلول محسّنة
	سلوك إرسال العينات
السماح بحماية Windows Defender IOAV	السماح بحماية Windows Defender IOAV أو عدم السماح بها
السماح بالوصول إلى واجهة مستخدم "الحماية عند الوصول" الخاصة بالمدافعين	
متوسط عامل تحميل وحدة المعالجة المركزية	يمثل متوسط عامل تحميل وحدة المعالجة المركزية لفحص Windows Defender (بالنسبة المئوية)

التعامل مع البرامج الضارة	
منخفضة الشدة	يمكنك تحديد كيفية تعامل الجهاز مع البرامج الضارة لكل مستوى خطورة. الخيارات المتاحة هي: • نظيفة • الحجر الصحي • إزالة • السماح • تعريف المستخدم • المربع
متوسطة الشدة	
عالية الخطورة	
الشدة الشديدة	
أيام الاحتفاظ بالبرامج الضارة التي تم تنظيفها	الفترة الزمنية بالأيام التي سيتم فيها تخزين ملفات/عناصر العزل على النظام. القيمة الافتراضية هي 0، والتي تحتفظ بالعناصر في العزل، ولا تقوم بإزالتها تلقائياً. القيمة القصوى هي 90.

مركز الأمن

مركز أمان Windows - إعدادات أمان Windows		
تعطيل واجهة مستخدم الحماية من الفيروسات والتهديدات		
إخفاء واجهة مستخدم استعادة بيانات برامج الفدية الخبيثة		
تعطيل واجهة مستخدم حماية الحساب		
تعطيل جدار الحماية وواجهة مستخدم حماية الشبكة		
تعطيل واجهة المستخدم للتحكم في التطبيق والمتصفح		
عدم السماح بإجراء تغييرات على الحماية من الاستغلال	عدم السماح للمستخدم بإجراء تغييرات على إعدادات الحماية من الاستغلال	
تعطيل واجهة مستخدم أمان الجهاز		
إخفاء استكشاف أخطاء TPM وإصلاحها	إخفاء إعدادات استكشاف الأخطاء وإصلاحها TPM	
تعطيل زر مسح زر مسح TPM		
تعطيل أداء الجهاز وواجهة المستخدم الصحية		
تعطيل واجهة مستخدم خيارات العائلة المعطلة		

تخصيص الخبز المحمص	
تمكين معلومات الدعم المخصص	تمكين عرض معلومات الاتصال بالدعم المخصص لشركتك في أسفل يمين تطبيق مركز الأمان.
عنوان البريد الإلكتروني	تعيين عنوان البريد الإلكتروني للشركة
اسم الشركة	تعيين اسم الشركة
هاتف الشركة	تعيين هاتف الشركة
عنوان URL للمساعدة	تعيين عنوان URL للمساعدة الخاص بالشركة

إعدادات إضافية	
تعطيل الإشعارات	تعطيل عرض إعلامات مركز أمان Windows Defender Security Center.
إخفاء توصيات تحديث البرنامج الثابت TPM	إخفاء التوصية بتحديث البرنامج الثابت لـ TPM عند اكتشاف برنامج ثابت ضعيف.
عرض اسم الشركة وخيارات الاتصال	اعرض اسم شركتك وخيارات الاتصال الخاصة بك في بطاقة جهة اتصال تطير في مركز أمان Windows Defender.
إخفاء التمهيد الآمن	إخفاء منطقة التمهيد الأمني.
إخفاء التحكم في منطقة إعلام الأمان	إخفاء عنصر التحكم في منطقة إعلامات أمان Windows.

تكوين جدار الحماية

تكوين جدار الحماية - الإعدادات العامة	
تجاهل مجموعة المصادقة	تجاهل مجموعة المصادقة بأكملها إذا كانت لا تدعم جميع مجموعات المصادقة المحددة في المجموعة
نوع قائمة انتظار الحزمة	يحدد كيفية تمكين توسيع نطاق البرنامج على جانب الاستقبال لكل من الاستقبال المشفر ومسح المسار الأمامي لسيناريو بوابة نفق IPsec.
تعطيل إجراء تصفية FTP للحالة	إذا تم تعطيله، فلن يقوم بإجراء تصفية بروتوكول نقل الملفات (FTP) للسماح بالاتصالات الثانوية
وقت خمول الارتباط الأمني	يقوم هذا الحقل بتكوين وقت خمول اقتران الأمان، بالثواني. يتم حذف اقترانات الأمان بعد عدم رؤية نقل بيانات الشبكة لهذه الفترة الزمنية المحددة.
ترميز المفتاح المشترك مسبقاً	تعيين ترميز المفتاح المشترك مسبقاً
استثناءات IPSec	تكوين استثناءات بروتوكول الإنترنت
التحقق من قائمة إبطال الشهادات	

ملفات تعريف جدار الحماية (ملف تعريف المجال / ملف تعريف خاص / ملف تعريف عام)	
تمكين جدار الحماية لهذا الملف الشخصي	
تعطيل الإشعارات	تعطيل عرض إشعار للمستخدم عند حظر أحد التطبيقات من الاستماع على أحد المنافذ.
حظر استجابات البث الأحادي لعمليات البث المتعدد	
فرض قواعد جدار حماية التطبيقات المصرح بها	إذا لم يتم تطبيقه، يتم تجاهل قواعد جدار حماية التطبيق المصرح به في المخزن المحلي ولا يتم تطبيقه
فرض قواعد جدار حماية المنفذ العام	إذا لم يتم تطبيقه، يتم تجاهل قواعد جدار حماية المنفذ العام في المخزن المحلي ولا يتم تطبيقها. لا يكون للإعداد معنى إلا إذا تم تعيينه أو تعداده في مخزن نهج المجموعة أو إذا تم تعداده من GroupPolicyRSoPStore
تطبيق قواعد جدار الحماية	إذا لم يتم تطبيقه، يتم تجاهل قواعد جدار الحماية من المخزن المحلي ولا يتم تطبيقها
فرض قواعد أمان الاتصال	لا يتم تطبيقه، يتم تجاهل قواعد أمان الاتصال من المتجر المحلي ولا يتم تطبيقها
الإجراء الصادر الافتراضي	الإجراء الذي يقوم به جدار الحماية بشكل افتراضي على الاتصالات الصادرة
الإجراء الوارد الافتراضي	الإجراء الذي يقوم به جدار الحماية بشكل افتراضي على الاتصالات الواردة
تعطيل وضع التخفي	وضع التخفي هو آلية في جدار حماية Windows تساعد على منع المستخدمين الضارين من اكتشاف معلومات حول أجهزة كمبيوتر الشبكة والخدمات التي تقوم بتشغيلها.
تعطيل منع الاستجابة لحركة المرور غير المرغوب فيها	في حالة التعطيل، يجب ألا تمنع قواعد وضع التخفي لجدار الحماية الكمبيوتر المضيف من الاستجابة لمرور الشبكة غير المرغوب فيه إذا كان هذا المرور مؤمناً بواسطة IPsec

قواعد جدار الحماية

قواعد جدار الحماية	
الاسم	اسم القاعدة
الوصف	وصف القاعدة
الإجراء	حدد ما إذا كانت هذه القاعدة ستحظر حركة المرور أو تسمح بها. يُرجى مراعاة أن خيار الحظر قد يحظر أيضًا نقل البيانات (بناءً على بقية التكوين) بين خادم MDM والجهاز
الاتجاه	
تمكين اجتياز الحافة (متاح فقط عند ضبط **الاتجاه** على **حركة المرور الواردة**)	يشير إلى أن حركة المرور الواردة المحددة مسموح لها بالنفق عبر NAT والأجهزة الطرفية الأخرى باستخدام تقنية Teredo Tunneling.

البرامج والخدمات	
تحديد التطبيقات، كل ما عدا ذلك	إذا لم يتم تمكينه، فسيتم النظر في جميع التطبيقات
اسم عائلة الحزمة	اسم عائلة الحزمة التي ستطبق عليها القاعدة.
مسار ملف التطبيق	التطبيق الكامل مثل C:\Windows\System\Notepad.exe الذي ستطبق عليه القاعدة
الاسم الثنائي المؤهل بالكامل	الاسم الثنائي المؤهل بالكامل الذي ستطبق عليه القاعدة. الاسم الثنائي المؤهل بالكامل هو سلسلة على الشكل التالي: {ناشر/منتج/اسم المنتج، الإصدار}
اسم الخدمة	أدخل اسم الخدمة (مثل "EventLog"). يمكنك الحصول على قائمة بأسماء الخدمات على Powershell عن طريق تشغيل الأمر "Get-Service".

البروتوكولات والمنافذ				
البروتوكول	البروتوكول الذي تستخدمه القاعدة.			
	القيم المتاحة: - أي - مخصص - هوبورت - ICMPv4 - IGMP - TCP - UDP - IPv6 - مسار - IPv6-روت - IPv6-فراغ IPv6 - GRE - ICMPv6 - IPv6- NoNxt - IPv6-Opts - VRRP - PGM - L2TP	عند الضبط على مخصص	إدراج رقم البروتوكول بين 0 و255	رقم البروتوكول
		عند ضبطه على TCP أو UDP	تحديد منافذ محلية، سيتم استخدامها جميعًا وإلا سيتم استخدامها جميعًا	المنافذ المحلية التي ستستخدمها القاعدة، يُسمح أيضًا بمنافذ النطاق
			الميناء المحلي	منفذ واحد أو مجموعة من المنافذ. على سبيل المثال 100-300،200،120-320.
			تحديد المنافذ البعيدة، سيتم استخدامها جميعًا وإلا سيتم استخدامها جميعًا	المنافذ البعيدة التي ستستخدمها القاعدة، يُسمح أيضًا بمنافذ النطاق
			المنفذ البعيد	منفذ واحد أو مجموعة من المنافذ. على سبيل المثال 100-300،200،120-320.

النطاق	
تحديد عناوين IP محلية، أي IP خلاف ذلك	مجموعة من عناوين IP المحلية، ويمكن أن تكون أيضًا مجموعة من عناوين IP مفصولة بـ -
عنوان IP المحلي	مجموعة من عناوين IP مفردة أو مجموعة من عناوين IP مفصولة بـ -
تحديد عناوين IP عن بُعد، أي عنوان IP عن بُعد خلاف ذلك	حدد مجموعة من عناوين IP البعيدة، ويمكن أن تكون أيضًا نطاقًا من عناوين IP مفصولة بـ "-".
عنوان IP البعيد	تحديد عناوين IP مفردة أو نطاق من عناوين IP
التوكنات	الرموز التي يمكن تعيينها مع العناوين البعيدة. الرموز الرمزية Intranet و RmtIntranet و Ply2Renders مدعومة في نظام التشغيل Windows 10، الإصدار 1809 والإصدارات الأحدث.

الإعدادات المتقدمة	
تحديد ملفات التعريف، سيتم استخدامها جميعًا وإلا	إذا تم تعطيلها سيتم استخدام جميع الملفات الشخصية
المجال	الملف الشخصي للمجال
خاص	الملف الشخصي الخاص
عام	الملف الشخصي العام
تحديد الواجهات، سيتم استخدام جميع الواجهات، وإلا فسيتم استخدامها كلها	في حالة تعطيلها سيتم استخدام جميع الواجهات
شبكة المنطقة المحلية	واجهة الشبكة المحلية
الوصول عن بُعد	واجهة الوصول عن بُعد
لاسلكي	واجهة لاسلكية

المدراء المحليون	
إضافة مستخدمين محليين معتمدين	السماح بإضافة قائمة بالمستخدمين المحليين الذين سيستخدمون هذه القاعدة
المستخدمون المصرح لهم	قائمة المستخدمين المحليين المصرح لهم لهذه القاعدة. يجب أن يكون المستخدم بصيغة لغة تعريف وصف الأمان (SDDL)، على سبيل المثال PC_NAME\USERNAME. يجب عدم ملء هذا الحقل إذا تم تعيين اسم خدمة لاستخدام هذه القاعدة

إعدادات التقييد

وظائف الجهاز

السماح لبطاقة SD	السماح باستخدام بطاقة SD
السماح للكاميرا	السماح باستخدام الكاميرا
السماح بخدمة الموقع	السماح بخدمة تحديد موقع الجهاز
السماح بالتحميل الجانبي للتطبيق	السماح بتثبيت التطبيقات من مصادر غير معروفة
السماح بوضع المطور	السماح بوضع المطور
السماح بتجوال البيانات الخلوية	السماح بتجوال البيانات الخلوية
السماح ل Cortana	السماح للمساعد الصوتي Cortana
السماح للبحث باستخدام الموقع	السماح للبحث باستخدام الموقع
السماح بإضافة حساب بريد إلكتروني غير تابع لمايكروسوفت	حدد ما إذا كان مسموحاً للمستخدم بإضافة حسابات بريد إلكتروني غير تابعة ل MSA.
السماح باتصال حساب مايكروسوفت	تحديد ما إذا كان يسمح باستخدام حساب MSA للمصادقة على الاتصال غير المرتبط بالبريد الإلكتروني والخدمات.
السماح بمزامنة إعداداتي	السماح بمزامنة الإعدادات عبر الجهاز بأكمله
أسماء النطاقات المحمية للمؤسسات	يحدد أسماء نطاقات المؤسسة مفصولة بـ ";".
السماح للمستخدم بتعطيل استعادة النظام	يسمح للمستخدم بتعطيل استعادة النظام. **تحذير!** يجب استخدام هذه الميزة فقط على الأجهزة التي تملكها أو توفرها شركة أو مؤسسة المؤسسة أو على جهاز مملوك للمستخدم، حيث يسمح المستخدم بأن تتم إدارة الجهاز بالكامل من قبل شركة المؤسسة. إذا قمت بتعطيل إعداد النهج هذا، يتم إيقاف تشغيل "استعادة النظام"، ويتعذر الوصول إلى "معالج استعادة النظام". يتم أيضاً تعطيل خيار تكوين استعادة النظام أو إنشاء نقطة استعادة من خلال حماية النظام.
السماح بإلغاء تسجيل المستخدم	يسمح للمستخدم بإزالة جزء الشركة من الجهاز وبالتالي قطع الاتصال بخوادم AppTec360. في حالة حدوث ذلك، لن يكون من الممكن إدارة الجهاز بعد ذلك **تحذير!** يجب استخدام هذه الميزة فقط على الأجهزة التي تملكها أو توفرها شركة أو مؤسسة المؤسسة أو على جهاز مملوك للمستخدم، حيث يسمح المستخدم بأن تتم إدارة الجهاز

	بالكامل من قبل شركة المؤسسة. إذا قمت بتعطيل إعداد النهج هذا، فلن يتمكن المستخدمون من إزالة تسجيلات MDM. حدد ما إذا كان يُسمح للمستخدم بحذف حساب مكان العمل عبر لوحة تحكم مكان العمل. يمكن لخادم MDM دائماً حذف الحساب عن بُعد.

BitLocker

تكوين BitLocker

الإعدادات العامة	
طلب تشفير الجهاز	مطالبة المستخدمين بتمكين تشفير الجهاز.قد يُطلب من المستخدمين تمكين تشفير الجهاز، وذلك حسب إصدار Windows وتكوين النظام: - للتأكد من عدم تمكين التشفير من موفر آخر. - لإيقاف تشغيل تشفير BitLocker Drive Encryption ثم إعادة تشغيل BitLocker.
طرق التشفير	
طريقة التشفير لمحركات أقراص نظام التشغيل	
طريقة التشفير لمحركات أقراص البيانات الثابتة	
طريقة التشفير لمحركات أقراص البيانات القابلة للإزالة	
تعطيل التحذير بشأن تشفير القرص من طرف ثالث	قم بتعطيل مطالبة التحذير بشأن خدمة تشفير الأقراص الخارجية المستخدمة على الجهاز. بدءاً من Windows 10، الإصدار 1803، يتم دعم هذا الإعداد فقط للأجهزة المرتبطة ب Azure Active Directory.
السماح بتشغيل التشفير أثناء تسجيل دخول مستخدم غير مسؤول	مدعوم فقط للأجهزة المرتبطة ب Azure Active Directory المنضمة

امتدادات AppTec360	
التشفير الصامت	في حالة تحديدها مع "طلب تشفير الجهاز"، ستقوم خدمة إدارة AppTec360 بتشغيل التشفير التلقائي الصامت لمحركات أقراص الجهاز.
إنشاء بيانات اعتماد المستخدم تلقائياً	سيكون محرك أقراص نظام التشغيل المشفر محميًا ببيانات اعتماد المستخدم التي يتم إنشاؤها تلقائيًا. إما رقم تعريف شخصي TPM، عند توفر TPM أو كلمة مرور نصية مكونة من 6 أرقام. يتم إرسال بيانات الاعتماد التي تم إنشاؤها إلى عنوان البريد الإلكتروني المسجل لجهاز معين. إذا تم إيقاف تشغيل هذا الخيار، فإن الحماية الوحيدة الممكنة للتشفير الصامت هي استخدام TPM. في هذه الحالة، بالنسبة للأجهزة التي لا تحتوي على TPM، سيفشل التشفير الصامت.
تشفير محركات الأقراص الثابتة	كما سيتم تشفير أي محركات أقراص بيانات ثابتة متوفرة وحمايتها باستخدام "إلغاء القفل التلقائي" باستخدام مفتاح مخزّن على محرك أقراص نظام التشغيل.

إعدادات محرك أقراص نظام التشغيل	
طلب مصادقة إضافية عند بدء التشغيل	يسمح لك هذا الإعداد بتهيئة ما إذا كان BitLocker يتطلب مصادقة في كل مرة يتم فيها بدء تشغيل الكمبيوتر. يتم تطبيق هذا الإعداد أثناء إعداد BitLocker. إذا قمت بتمكين هذا الإعداد، يمكن للمستخدمين تكوين خيارات بدء التشغيل المتقدمة في معالج إعداد BitLocker.
حظر BitLocker بدون TPM متوافق	
TPM فقط	
TPM و PIN	
TPM والمفتاح	
TPM والمفتاح ورقم التعريف الشخصي	إذا كنت ترغب في طلب استخدام رقم تعريف شخصي ومحرك أقراص USB محمول (مفتاح)، يجب على المستخدم إعداد BitLocker باستخدام أداة سطر الأوامر "manage-bde" بدلاً من معالج إعداد تشفير محرك BitLocker Drive Encryption.

طلب الحد الأدنى لطول رقم التعريف الشخصي	
	الحد الأدنى من الأحرف

تكوين رسالة استرداد ما قبل التشغيل وعنوان URL	قم بتكوين رسالة الاسترداد بأكملها أو استبدل عنوان URL الحالي الذي يتم عرضه على شاشة استرداد مفتاح ما قبل التشغيل عند قفل محرك أقراص نظام التشغيل.

	ملاحظة: ليست كل الأحرف واللغات مدعومة في مرحلة ما قبل التمهيد. يوصى بشدة أن تختبر ظهور الأحرف التي تستخدمها بشكل صحيح على شاشة استرداد ما قبل التمهيد.
	خيار رسالة الاسترداد قبل التمهيد
	رسالة استرداد مخصصة
	عنوان URL مخصص للاسترداد

خيارات استرداد محرك أقراص نظام التشغيل	يسمح لك هذا الإعداد بالتحكم في كيفية استرداد محركات أقراص نظام التشغيل المحمي بواسطة BitLocker في حال عدم وجود بيانات الاعتماد المطلوبة. يتم تطبيق هذا الإعداد أثناء إعداد BitLocker. يُسمح بشكل افتراضي بعامل استرداد البيانات المستند إلى الشهادة بشكل افتراضي، ويمكن تحديد خيارات الاسترداد من قبل المستخدم بما في ذلك كلمة مرور الاسترداد ومفتاح الاسترداد ولا يتم نسخ معلومات الاسترداد احتياطيًا إلى AD DS.
عامل استرداد البيانات المستند إلى شهادة الكتلة	حدد ما إذا كان يمكن استخدام عامل استرداد البيانات مع محركات أقراص نظام التشغيل المحمي بواسطة BitLocker. قبل أن يمكن استخدام عامل استرداد البيانات يجب إضافته من عنصر نُهج المفاتيح العامة في وحدة تحكم إدارة نهج المجموعة أو محرر نهج المجموعة المحلي. راجع دليل نشر تشفير محرك الأقراص BitLocker Drive Encryption على Microsoft TechNet للحصول على مزيد من المعلومات حول إضافة وكلاء استرداد البيانات.
إعدادات كلمة مرور استرداد BitLocker	
إعدادات مفتاح استرداد BitLocker	
حفظ معلومات استرداد BitLocker في "خدمات مجال الدليل النشط	
تكوين وحدة تخزين استرداد الاسترداد AD DS BitLocker	يدعم تخزين حزمة المفاتيح استعادة البيانات من محرك الأقراص الذي تعرض للتلف المادي.
طلب تخزين بيانات الاسترداد في AD DS	منع المستخدمين من تمكين BitLocker ما لم يكن الكمبيوتر متصلاً بالمجال و

إعدادات محرك الأقراص الثابتة	
خيارات استعادة محركات الأقراص الثابتة	يسمح لك هذا الإعداد بالتحكم في كيفية استرداد محركات الأقراص الثابتة المحمية بواسطة BitLocker في حالة عدم وجود بيانات الاعتماد المطلوبة. يتم تطبيق هذا الإعداد أثناء إعداد BitLocker. يُسمح بشكل افتراضي بعامل استرداد البيانات المستند إلى الشهادة بشكل افتراضي، ويمكن تحديد خيارات الاسترداد من قبل المستخدم بما في ذلك كلمة مرور الاسترداد ومفتاح الاسترداد ولا يتم نسخ معلومات الاسترداد احتياطيًا إلى AD DS.
عامل استرداد البيانات المستند إلى شهادة الكتلة	
إعدادات كلمة مرور استرداد BitLocker	
إعدادات مفتاح استرداد BitLocker	
حفظ معلومات استرداد BitLocker في "خدمات مجال الدليل النشط	
تكوين وحدة تخزين استرداد الاسترداد AD DS BitLocker	يدعم تخزين حزمة المفاتيح استعادة البيانات من محرك الأقراص الذي تعرض للتلف المادي.
طلب تخزين بيانات الاسترداد في AD DS	منع المستخدمين من تمكين BitLocker ما لم يكن الكمبيوتر متصلاً بالمجال ونجاح النسخ الاحتياطي لمعلومات استرداد BitLocker إلى AD DS. ملاحظة: يتم إنشاء كلمة مرور الاسترداد تلقائياً.
رفض وصول الكتابة إلى محركات الأقراص الثابتة غير المحمية	

إعدادات محرك الأقراص القابل للإزالة	
رفض وصول الكتابة إلى محركات الأقراص القابلة للإزالة غير المحمية	رفض الوصول للكتابة إلى محركات أقراص البيانات القابلة للإزالة غير المحمية بواسطة Bitlocker. ملاحظة: إذا تم تمكين "الأقراص القابلة للإزالة: رفض الوصول للكتابة" في نهج المجموعة، فسيتم تجاهل إعداد النهج هذا.
رفض الوصول إلى الكتابة إلى الأجهزة التي تم تكوينها في مؤسسة أخرى	لن يتم منح حق الوصول للكتابة إلا لمحركات الأقراص التي تحتوي على حقول تعريف مطابقة لحقول تعريف الكمبيوتر. يتم تعريف هذه الحقول من خلال إعداد نهج المجموعة "توفير معرّفات فريدة لمؤسستك".

حالة BitLocker

هنا يمكنك الاطلاع على الحالة الحالية لمحركات أقراص BitLocker المشفرة

C [OS Drive]
حالة التشفير
مشفر (%)
حالة الحماية
طريقة التشفير
واقيات المفاتيح
كلمة مرور الاسترداد

بنقرة على زر "تدوير كلمة مرور الاسترداد" يمكنك تدوير كلمة مرور استرداد BitLocker.

إدارة الشهادات

قائمة الشهادات

فيما يلي قائمة بالشهادات المثبتة على الجهاز الذي يتم عرضه.

تكوين الشهادة

هنا يمكنك تكوين الشهادات وكيفية تثبيتها على الجهاز.

شهادة موثوق بها	
الوصف	وصف الشهادة
النطاق	نطاق نشر الشهادة: المستخدم الحالي مقابل الجهاز
متجر الشهادات	"الشهادات غير الموثوق بها" متوفرة فقط بدءاً من Windows 10، الإصدار 1803
ملف الشهادة	تحميل ملف PKCS#1

شهادة الهوية			
الوصف	وصف الشهادة		
النطاق	نطاق نشر الشهادة: المستخدم الحالي مقابل الجهاز		
الموقع الرئيسي	موفر تخزين المفاتيح لتثبيت المفتاح الخاص عليه.		
	TPM. فشل في حالة عدم وجود TPM		
	TPM. في حالة عدم وجود TPM، يتم الرجوع إلى برنامج KSP		
	موفر تخزين مفاتيح البرامج	وضع علامة على المفتاح الخاص على أنه قابل للتصدير	
	ويندوز هالو للأعمال	اسم الحاوية	تحديد اسم حاوية Windows Hello for Business (المعروفة سابقاً باسم Microsoft Passport for Work).
		نص مطالبة رقم التعريف الشخصي	تحديد النص المخصص لإظهاره في مطالبة Windows Hello for Business PIN أثناء تسجيل الشهادة.
أوراق الاعتماد	تحميل ملف PKCS#12		

SCEP

الوصف	وصف خادم SCEP			
نطاق النشر	نطاق نشر الشهادة: الجهاز الحالي مقابل المستخدم			
عناوين URL لخوادم SCEP	خادم واحد أو أكثر يقوم بإصدار الشهادات من خلال SCEP			
الموضوع	تمثيل اسم X.500. على سبيل المثال "C= الولايات المتحدة الأمريكية، O= شركة مايكروسوفت، CN=foo، 1.2.5.3.3= بار"			
الأسماء البديلة للموضوع	النوع	عنوان البريد الإلكتروني		
		نظام أسماء النطاقات		
		URI		
		اسم المستخدم الرئيسي (UPN)		
بصمة الإصبع CA	بصمة SHA1 لشهادة المرجع المصدق. E.g. 31:8F:1E:78:5C:D5:12:9F:7E:3B:AD:F3:1C:C0:19:03:96:43:A9:E5			
وحدات فترة الصلاحية	أيام أو شهور أو سنوات			
فترة الصلاحية				
التحدي	يُستخدم كسر مشترك مسبقاً للتسجيل التلقائي			
إعادة المحاولة	عدد المرات التي يجب أن يعيد فيها الجهاز المحاولة إذا أرسل الخادم استجابة PENDING. القيمة الافتراضية هي 5. القيمة القصوى هي 30.			
تأخير إعادة المحاولة	عدد الدقائق المطلوب انتظارها قبل إعادة المحاولة. القيمة الافتراضية هي 5. القيمة الدنيا هي 1.			
حجم المفتاح	حجم المفتاح بالبت			
خوارزمية التجزئة	عائلة خوارزمية التجزئة			
الاستخدام الرئيسي	يحدد ملحق استخدام المفتاح الغرض (على سبيل المثال، التشفير والتوقيع) من المفتاح الموجود في الشهادة. يجب تحديد واحد على الأقل من "التوقيع الرقمي" أو "تشفير المفتاح".			
استخدام المفتاح الموسع	تحديد استخدامات المفاتيح الموسعة.تخضع لتكوين خادم SCEP. تحديد قائمة معرفات OIDs المقابلة، على سبيل المثال 1.3.6.1.5.5.5.7.3.2 (مصادقة العميل)			
الموقع الرئيسي	موفر تخزين المفاتيح لتثبيت المفتاح الخاص عليه.			
		TPM. فشل في حالة عدم وجود TPM		

			TPM. في حالة عدم وجود TPM، يتم الرجوع إلى برنامج KSP
			موفر تخزين مفاتيح البرامج
	ويندوز هالو للأعمال	اسم الحاوية	تحديد اسم حاوية Windows Hello for Business (المعروفة سابقاً باسم Microsoft Passport for Work).
		نص مطالبة رقم التعريف الشخصي	تحديد النص المخصص لإظهاره في مطالبة Windows Hello for Business PIN أثناء تسجيل الشهادة.

إدارة الاتصال

الواي فاي

عند هذا الإعداد، قم بإجراء التهيئة المسبقة لأجهزة المستخدم النهائي للوصول إلى نقاط الوصول الداخلية

معرّف مجموعة الخدمة (SSID)	SSID للشبكة، التي سيتم إنشاء الاتصال بها
الانضمام التلقائي	تنشيط الانضمام التلقائي إلى الشبكة
الشبكة الخفية	تنشيط، في حالة عدم قيام نقطة الوصول إلى نقطة الوصول ببث SSID

نوع الأمان

إنشاء نوع أمان نقطة الوصول إلى التطبيق

نظام WEP المفتوح	
كلمة المرور	كلمة المرور الخاصة بـ AP

WPA PSK	
كلمة المرور	كلمة المرور الخاصة بـ AP

WPA EAP	
نوع المصادقة	نوع المصادقة، ممكن فقط مع "PEAP-MSCAHPv2"
إعادة الاتصال السريع	يمكن للأجهزة التبديل بين نقاط الوصول، دون الحاجة إلى مصادقة نفسها مرة أخرى
دخول الضيف	لا يمتلك المستخدم حساباً وبالتالي يجب عليه التسجيل كضيف
فحوصات الحجر الصحي	يجب على العميل إجراء فحوصات NAP (حماية الوصول إلى الشبكة) ومشاركة النتائج مع النظام، الذي يقرر بعد ذلك ما إذا كان بإمكان العميل الاتصال
طلب ربط التشفير	المصادقة ممكنة فقط من خلال ربط التشفير
التحقق من صحة الخادم	يتحقق العميل مما إذا كانت شهادة الخادم صالحة. إذا كانت هذه هي الحالة، سيتم إنشاء اتصال
المطالبة بالشهادات	السماح للمستخدم بقبول شهادات غير موثوق بها
أسماء الخوادم	يوفر خيار عرض اسم خادم RADIUS-Server، الذي يوفر مصادقة الشبكة وتخويلها

WPA2-PSK	
كلمة المرور	كلمة مرور AP

WPA2 EAP	
نوع المصادقة	نوع المصادقة، ممكن فقط مع "PEAP-MSCAHPv2"
إعادة الاتصال السريع	
دخول الضيف	
فحوصات الحجر الصحي	تنشيط حماية الوصول إلى الشبكة NAP
طلب ربط التشفير	المصادقة ممكنة فقط من خلال ربط التشفير
التحقق من صحة الخادم	
المطالبة بالشهادات	يطالب بشهادة خادم تم التحقق من صحتها أو اسم أو مصادقة شهادة جذرية (CA)
أسماء الخوادم	قائمة بالخوادم التي يجب أن تثق بها الأجهزة
لا يوجد	لا يوجد أمن ثابت
استخدام الخادم الوكيل	استخدام خادم وكيل
عنوان الخادم	عنوان الخادم الوكيل
منفذ الخادم	منفذ خادم الخادم الوكيل

استخدام الخادم الوكيل

تمكين استخدام الخادم الوكيل.

عنوان الخادم	عنوان الخادم الوكيل الذي تستخدمه هذه الشبكة.
منفذ الخادم	منفذ الخادم الوكيل الذي تستخدمه هذه الشبكة.

قيود الواي فاي

هنا يمكنك تحديد قيود Wifi المختلفة.

السماح بالواي فاي	السماح/رفض الواي فاي
السماح بمشاركة الإنترنت	السماح باستخدام نقطة اتصال
السماح بالاتصال التلقائي بنقاط اتصال WiFi Sense الساخنة	السماح بالاتصال التلقائي بنقاط اتصال WiFi Sense الساخنة
السماح بتهيئة WiFi يدوياً	السماح للمستخدم بالاتصال بشبكات WiFi التي لم يتم تعريفها بواسطة AppTec
تردد المسح الضوئي لشبكة WLAN اللاسلكية	يحدد الفاصل الزمني لشبكة WLAN-Scan. هنا، تزيد القيمة الأعلى من القدرة على التعرف على شبكات WIFI.

VPN

قم بإجراء الإعدادات المناسبة هنا، من أجل تكوين اتصالات VPN

اسم الاتصال	اسم الاتصال المشار إليه		
نوع VPN	يتم استخدام اتصال VPN لكل تطبيق لتأمين حركة مرور تطبيقات معينة.		
	VPN	دائماً في وضع التشغيل	سيؤدي هذا إلى توصيل الشبكة الافتراضية الخاصة تلقائيًا عند تسجيل الدخول وسيظل متصلاً حتى يقوم المستخدم بقطع الاتصال يدويًا.
	لكل تطبيق VPN	تطبيقات VPN	تحديد التطبيقات التي تستخدم اتصال VPN هذا
		الإغلاق لكل تطبيق	يؤدي الإغلاق لكل تطبيق إلى جعل التطبيقات المحددة متصلة فقط من خلال اتصال VPN هذا. تعتمد هذه الميزة على جدار حماية Windows Defender.
	ملف تعريف WIP	مجال WIP لهذا الاتصال	معرّف المؤسسة، وهو مطلوب لربط ملف تعريف VPN هذا بنهج حماية معلومات Windows (WIP)

نوع الاتصال

AppTec360 VPN	
بالنسبة لشبكة "AppTec360 VPN"، يلزم السماح بالتحميل الجانبي للتطبيق. يُرجى تمكين "السماح بالتحميل الجانبي للتطبيق" في "إدارة الأمان" → "إعدادات التقييد" → "وظائف الجهاز".	
تكوين البوابة	لتكوين اتصال VPN مع القائمة السوداء، يرجى تحديد تكوين VPN مع خادم DNS محدد. يمكنك إعداد تكوين VPN في "الإعدادات العامة" → "البوابة العامة" → "إعدادات VPN".

IKEv2		
الخوادم	قائمة خوادم VPN	
نفق الجهاز	تمكين الاتصال قبل تسجيل دخول المستخدم.	
طريقة التوثيق	برنامج EAP	EAP XML
	شهادات الماكينات	
خوارزمية التشفير		
خوارزمية التحقق من النزاهة		
مجموعة ديفي-هيلمان		
خوارزمية تحويل الشفرات		
خوارزمية تحويل المصادقة		
مجموعة السرية التامة إلى الأمام (PFS)		

PPTP		
الخوادم	قائمة خوادم VPN	
طريقة التوثيق	برنامج EAP	EAP XML

L2TP		
الخوادم	قائمة خوادم VPN	
طريقة التوثيق	برنامج EAP	EAP XML
خوارزمية التشفير		
خوارزمية التحقق من النزاهة		
مجموعة ديفي-هيلمان		
خوارزمية تحويل الشفرات		
خوارزمية تحويل المصادقة		
مجموعة السرية التامة إلى الأمام (PFS)		

أوتوماتيكي		
الخوادم	قائمة خوادم VPN	
طريقة التوثيق	برنامج EAP	EAP XML

تكوينات الشبكة الافتراضية الخاصة الافتراضية العامة

تذكر بيانات الاعتماد عند كل تسجيل دخول	
تسجيل عناوين IP مع DNS داخلي	
قواعد تصفية حركة مرور الشبكة	قصر اتصال VPN على مجموعة القواعد المحددة.
قائمة البحث عن لاحقة DNS	لاحقات DNS لإضافتها إلى قائمة بحث DNS لتوجيه الأسماء المختصرة.
قواعد جدول سياسة حل الأسماء (NRPT)	تحدد قواعد جدول نهج حل الأسماء (NRPT) كيفية حل نظام أسماء DNS للأسماء عند الاتصال بشبكة VPN.
كشف الشبكة الموثوق بها	قائمة لاحقات DNS لتحديد الشبكة الموثوق بها.
الانقسام النفقي	يعني الانقسام النفقي أن حركة المرور يمكن أن تنتقل عبر أي واجهة حسب ما تحدده مكدس الشبكات.
تقسيم الطرق النفقية	قائمة المسارات المراد إضافتها إلى جدول التوجيه لواجهة VPN.
إعداد الوكيل	تكوين البروكسي المستخدم مع هذه الشبكة
عنوان الوكيل	عنوان الخادم الوكيل كاسم مضيف مؤهل بالكامل أو عنوان IP.
الميناء	منفذ الخادم الوكيل.
عنوان URL التكوين التلقائي للوكيل	URL لاسترداد إعدادات الوكيل تلقائيًا.

قيود VPN

هنا يمكنك تحديد العديد من قيود VPN المختلفة.

السماح بإعدادات VPN	يسمح هذا الدليل الإرشادي للمستخدم/يمنع المستخدم من إلغاء تنشيط إعدادات VPN وتغييرها
السماح بشبكة VPN عبر الهاتف المحمول	يسمح/يمنع الجهاز من إنشاء اتصال VPN، إذا كان الجهاز يستخدم بيانات الهاتف المحمول
السماح بتجوال VPN عبر الهاتف الخلوي	يسمح/يمنع الجهاز من إنشاء اتصال VPN، إذا كان الجهاز متجولاً

بلوتوث

هنا يمكنك تحديد ما إذا كان يجب السماح/حظر البلوتوث.

السماح بالبلوتوث	تنشيط/إلغاء تنشيط البلوتوث

إدارة PIM

المزامنة النشطة للتبادل

إعداد حساب ActiveSync على جهاز المستخدم النهائي

اسم الحساب	اسم حساب البريد الإلكتروني
اسم مضيف الخادم	عنوان الخادم/شبكة QDN
اسم النطاق	مجال الخادم
عنوان البريد الإلكتروني	عنوان البريد الإلكتروني
اسم المستخدم	اسم المستخدم
كلمة مرور المستخدم	بشكل اختياري، يمكنك بالفعل إرفاق كلمة مرور للمستخدم هنا
استخدام SSL	استخدام اتصال SSL
الفاصل الزمني للمزامنة	هنا يمكن إنشاء فاصل التزامن هنا مزامنة يدوية = يجب على المستخدم تنزيل رسائل البريد الإلكتروني الخاصة به وإجراء مزامنة يدوية
مرشح عمر البريد	مقدار الوقت، حتى تتم مزامنة رسائل البريد الإلكتروني لا يوجد فلتر = غير محدود
مستوى السجل	إنشاء مستويات التسجيل لحركة مرور بيانات ActiveSync.
مزامنة البريد الإلكتروني	مفعل = تتم مزامنة رسائل البريد الإلكتروني
مزامنة جهات الاتصال	مفعل = تتم مزامنة جهات الاتصال
مزامنة التقويم	مفعل = تمت مزامنة التقويم
مهام المزامنة	مفعل = تتم مزامنة المهام

البريد الإلكتروني

إنشاء حسابات POP3/IMAP4 على جهاز المستخدم النهائي.

وصف الحساب	اسم حساب البريد الإلكتروني
اسم المرسل	اسم المرسل المعروض
اسم النطاق	اسم المجال لحساب البريد الإلكتروني
عنوان البريد الإلكتروني	عنوان البريد الإلكتروني للمستخدم
اسم المستخدم	اسم المستخدم
كلمة مرور المستخدم	بشكل اختياري، يمكنك بالفعل إرفاق كلمة مرور للمستخدم هنا
بيانات اعتماد الخادم الصادر البديلة	هنا يمكن تعريفه، إذا كانت بيانات الاعتماد الأخرى مطلوبة للخادم الصادر
اسم النطاق الصادر	اسم النطاق الصادر
اسم مستخدم الخادم الصادر	اسم مستخدم الخادم الصادر
كلمة مرور الخادم الصادر	كلمة مرور الخادم الصادر
بروتوكول البريد الإلكتروني	يمكن استخدام بروتوكول POP3 أو IMAP4 كبروتوكول
اسم مضيف خادم البريد الوارد	اسم مضيف خادم البريد الوارد
استخدام SSL للرسائل الواردة	استخدام SSL لرسائل البريد الإلكتروني الواردة
اسم مضيف خادم البريد الصادر	اسم مضيف خادم البريد الصادر
استخدام SSL للرسائل الصادرة	استخدام SSL لرسائل البريد الإلكتروني الصادرة
مصادقة الخادم الصادر	مطلوب مصادقة الخادم الصادر
الفاصل الزمني للمزامنة	هنا يمكن إنشاء فاصل التزامن هنا مزامنة يدوية = يجب على المستخدم تنزيل رسائل البريد الإلكتروني الخاصة به وإجراء مزامنة يدوية
مرشح عمر البريد	مقدار الوقت، حتى تتم مزامنة رسائل البريد الإلكتروني لا يوجد فلتر = غير محدود

إدارة التطبيقات

مدير تطبيقات المؤسسات

التطبيقات المثبتة

فيما يلي قائمة بالتطبيقات المثبتة حاليًا على الجهاز الذي يتم عرضه.

التطبيقات الإلزامية

هنا يمكنك تكوين قائمة بالتطبيقات الإلزامية على الجهاز.

سيتم التحقق من هذه القائمة في كل مرة يتصل فيها الجهاز بـ MDM وتثبيت جميع التطبيقات الموجودة في هذه القائمة التي تصادف أنها غير مثبتة على الجهاز، بغض النظر عما إذا كان التطبيق قد تم إلغاء تثبيته أو لم يتم تثبيته من قبل.

يمكنك تحميل تطبيقات Windows 10 الداخلية ثم إضافتها إلى هذه القائمة أو يمكنك إضافة تكوينات Microsoft Office التي تحتاج إلى تهيئتها مسبقًا في "الإعدادات العامة"> "إدارة التطبيقات"> "Microsoft Office".

قيود تطبيق النظام

تطبيقات صندوق الوارد
السماح بالمنبهات والساعة
السماح بالحاسبة
السماح للكاميرا
السماح بدعم الاتصال
السماح ل Cortana
السماح لمستكشف الملفات
السماح بالبدء
السماح بموسيقى الأخدود
السماح بالخرائط
السماح بالمراسلة
السماح ل Microsoft Edge
السماح بالأفلام والتلفزيون
السماح بالمال
السماح بالأخبار
السماح بـ OneDrive
السماح ل OneNote
السماح بتقويم Outlook والبريد
السماح للأشخاص
السماح بالهاتف
السماح بالصور
السماح بباوربوينت
السماح بالإعدادات
السماح ل Skype
السماح للرياضة
السماح بالمتجر
السماح بالمسجل الصوتي
السماح بالمحفظة
السماح بالطقس

السماح لمركز ملاحظات Windows Feedback Hub
السماح بكلمة
السماح ل Xbox

إعداد الصفحات
السماح للحسابات مكان العمل
السماح بالمعلومات المتقدمة
ركن السماح بالتطبيقات
السماح بالحظر والتصفية
السماح بملف تعريف اللون
السماح بوضع القيادة
السماح بالبريد الإلكتروني والحسابات
السماح بالمعادل
السماح للوحة المفاتيح
السماح لشريط التنقل
السماح بوضع الطائرة على الشبكة
السماح بمشاركة الإنترنت عبر الشبكة
السماح بخدمات الشبكة
السماح لشبكة Wi-Fi الشبكة
السماح ببلوتوث نظام الكمبيوتر الشخصي
السماح بتقييم جهازك
السماح باستعادة التحديث
السماح بالمشاركة
السماح بالبدء
لغة الوقت المسموح به
المنطقة الزمنية المسموح بها
السماح لشاشة قفل Windows الافتراضية
السماح بحساب العمل أو المدرسة

القائمة السوداء والبيضاء

ضمن "القائمة السوداء والقائمة البيضاء"، يمكنك الاختيار بين وضع "القائمة البيضاء" ووضع "القائمة السوداء".

القائمة البيضاء	يمكن فقط تثبيت التطبيقات والخدمات التي تمت إضافتها إلى القائمة على جهاز المستخدم النهائي. إذا كانت مثبتة مسبقاً على جهاز المستخدم النهائي، فسيتم تفعيلها وتعيينها، بحيث يمكن للمستخدم تشغيلها.
	جميع التطبيقات الأخرى التي لم تتم إضافتها إلى القائمة لا يمكن تثبيتها على جهاز المستخدم النهائي. إذا كانت هذه التطبيقات مثبتة مسبقاً على جهاز المستخدم النهائي فسيتم إلغاء تنشيطها وتعيينها، بحيث لا يمكن للمستخدم تشغيلها.
القائمة السوداء	لا يمكن تثبيت التطبيقات والخدمات التي تمت إضافتها إلى القائمة على جهاز المستخدم النهائي. إذا كانت مثبتة مسبقاً على جهاز المستخدم النهائي فسيتم إلغاء تنشيطها وتعيينها، بحيث لا يمكن للمستخدم تشغيلها.
	يمكن تثبيت جميع التطبيقات الأخرى التي لم تتم إضافتها إلى القائمة على جهاز المستخدم النهائي. إذا كانت هذه التطبيقات مثبتة مسبقاً على جهاز المستخدم النهائي، فسيتم تفعيلها وتعيينها، بحيث يمكن للمستخدم تشغيلها.

من خلال، يمكنك إضافة تطبيقات أو خدمات إضافية إلى القائمة المستخدمة حاليًا.

من خلال، يمكنك إضافة تطبيقات أو خدمات إضافية إلى القائمة غير النشطة حاليًا.

يمكنك إما إضافة تطبيق من "متجر تطبيقات ويندوز" أو إدخال "معرّف التطبيق" مباشرةً لإضافته إلى القائمة السوداء أو البيضاء.

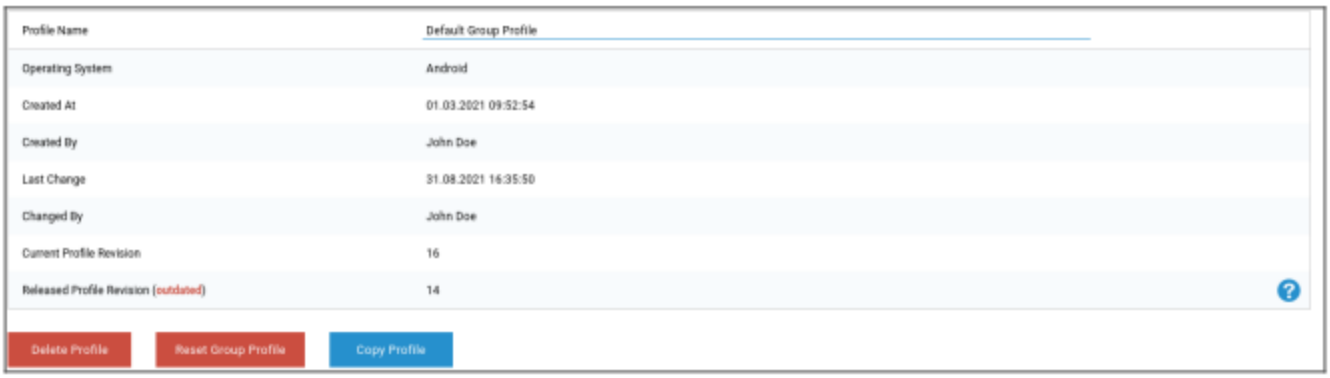
تهيئة نظام التشغيل MacOS

اعتماداً على ما إذا كنت قد حددت ملفاً شخصياً أو جهازاً، فإن العرض ونقاطه الفرعية يختلفان - يرجى الانتباه جيداً لهذا الأمر!

جنرال لواء

نظرة عامة على ملف تعريف المجموعة (على مستوى المجموعة فقط)

عند فتح الملف الشخصي للمجموعة، ستحصل على نظرة عامة سريعة على الملف الشخصي.



اسم الملف الشخصي	اسم الملف الشخصي (يمكن تغييره هنا)
نظام التشغيل	نظام التشغيل الذي تم إنشاء ملف التعريف له
تم إنشاؤها في	وقت الإنشاء
تم إنشاؤها بواسطة	منشئ الملف الشخصي
آخر تغيير	وقت آخر تغيير في الملف الشخصي
تم التغيير بواسطة	الحساب الذي أجرى التغييرات الأخيرة
مراجعة الملف الشخصي الحالي	مراجعة حالة الملف الشخصي المحفوظة
مراجعة الملف الشخصي الصادر	مراجعة الملف الشخصي المعين ("تعيين الآن"). إذا كانت التسمية تظهر "(قديم)" خلف النص، فهذا يعني أنك قمت بحفظ ملف التعريف ولكنك لم تعيّنه بعد، لذا ستظل الأجهزة تحصل على الإصدار الأقدم.

نظرة عامة على الجهاز (على مستوى الجهاز فقط)

نبذة موجزة عن الجهاز

اسم الجهاز	اسم الجهاز
الطراز	الطراز
نظام التشغيل	نظام التشغيل
الرقم التسلسلي	الرقم التسلسلي للجهاز
ملكية الجهاز	نوع الملكية المكوَّن
نوع الجهاز	نوع الجهاز
متوافق	يظهر ما إذا كان الجهاز متوافقاً أم لا
عنوان IP	عنوان IP الذي يتصل الجهاز بالخادم منه
آخر ظهور	وقت آخر اتصال من الجهاز
الدفعة الأخيرة	وقت آخر دفعة تم إرسالها إلى الجهاز
التعيين	هنا يمكنك نقل الجهاز إلى مستخدم آخر أو مجموعة أخرى

مراجعة التكوين (على مستوى الجهاز فقط)

هنا ستتلقى نظرة عامة على ملف تعريف المجموعة المعين للجهاز.

إذا قمت بالنقر على الملف الشخصي للمجموعة، فستتمكن من الوصول إلى الملف الشخصي مباشرةً ويمكنك إجراء الإعدادات.

باستخدام الرمز، يمكنك إعادة التطبيقات المعينة إلى إعدادات ملف تعريف المجموعة.

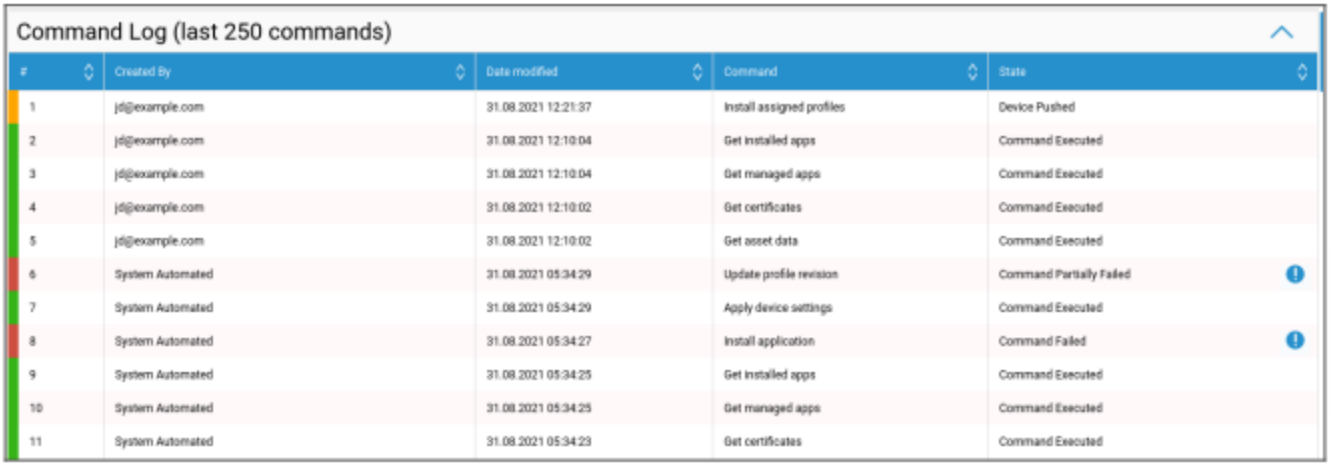
باستخدام الرمز، يمكنك إعادة ضبط ملف تعريف الجهاز بحيث لا يحتوي على أي إعدادات على الإطلاق.

تشير عبارة "تتوفر مراجعة أحدث" إلى أن ملف تعريف المجموعة قد تم تغييره وحفظه ولكن لم يتم تعيينه. يجب تعيين ملف تعريف المجموعة باستخدام "تعيين الآن" على مستوى المجموعة لتطبيق التغييرات على الأجهزة.

سجل الجهاز (على مستوى الجهاز فقط)

سجل الأوامر

هنا يمكنك معرفة الأوامر التي تم إصدارها للجهاز وما هي حالتها.



يتم إنشاء الأوامر التي تم إنشاؤها بواسطة "النظام الآلي" تلقائياً بواسطة النظام.

حالات الأوامر المحتملة

تم دفع الجهاز	تم إرسال طلب دفع إلى خدمة الدفع (مثل APNS) لإخبار الجهاز بالاتصال مرة أخرى بخادم EMM.
تم إنشاء الأمر	تم إنشاء الأمر في النظام.
تم إرسال الأمر	تم إرسال الأمر إلى الجهاز بعد اتصاله بالخادم.
تم تنفيذ الأمر	تم تنفيذ الأمر بنجاح.
فشل الأمر	فشل الأمر. *
فشل الأمر جزئياً	اعتمادًا على نظام تشغيل الجهاز قد يتم تجميع بعض الأوامر معًا. في هذا فشلت بعض أجزاء مجموعة الأوامر هذه. *
تم تنفيذ الأمر، وفشل الأمر في النهاية	تم تنفيذ الأمر ولكن ربما لم يتم تنفيذه.
إعادة دفع الأمر	تم إعادة دفع الأمر من قبل مستخدم.
مهملة	تم تجاهل الأمر. على سبيل المثال لأنه تم استبداله بأمر آخر أو تم إعادة تسجيل الجهاز وإزالة الأوامر القديمة

*إذا كانت هناك علامة تعجّب خلف الرسالة، يمكنك الحصول على مزيد من المعلومات من خلال تمرير مؤشر الماوس فوق الرمز.

إدارة الأصول (على مستوى الجهاز فقط)

معلومات الجهاز

رقم الموديل	رقم الموديل
اسم المضيف	اسم المضيف
اسم المضيف المحلي	اسم المضيف المحلي
نظام التشغيل	نظام التشغيل
إصدار نظام التشغيل	إصدار نظام التشغيل
UDID	UDID
الذاكرة الحرة/إجمالي الذاكرة الحرة	الذاكرة الحرة/إجمالي الذاكرة الحرة

الواي فاي

عنوان IP	عنوان IP
واي فاي ماك	واي فاي ماك

خلوي

رقم الهاتف	رقم الهاتف
حالة التجوال	حالة التجوال
التجوال (الصوت/البيانات)	التجوال (الصوت/البيانات)
عنوان IP	عنوان IP
المشغل/الناقل	المشغل/الناقل
شبكة ناقل الشريحة SIM	شبكة الناقل
إصدار الناقل	إصدار الناقل
ICCID	ICCID
MCC/ MNC الحالية	MCC/ MNC الحالية
SIM MCC/MNC	SIM MCC/MNC

بلوتوث

بلوتوث ماك	بلوتوث ماك

إدارة التحديث (على مستوى الجهاز فقط)

معلومات التحديث

تعرض علامة التبويب هذه معلومات حول إعدادات تحديث النظام على الجهاز.

تم تمكين الفحص التلقائي	إذا كان النظام يتحقق من التحديث تلقائياً.
تم تمكين التحديث التلقائي للتطبيق	إذا كان النظام سيقوم بتثبيت تحديثات التطبيق تلقائياً.
تم تمكين التحديثات التلقائية لنظام التشغيل	إذا كان النظام سيقوم بتثبيت تحديثات نظام التشغيل تلقائياً.
تمكين تحديثات الأمان التلقائية - التحديثات التلقائية	إذا كان النظام سيقوم بتثبيت تحديثات الأمان تلقائياً.
تم تمكين تنزيل خلفية تحديث التطبيق-التنزيل في الخلفية	إذا كان النظام سيقوم بتنزيل تحديثات التطبيق في الخلفية.
رابط الكتالوج	عنوان URL لكتالوج تحديث البرامج الذي يستخدمه العميل.
هو الكتالوج الافتراضي	إذا كانت "نعم"، يكون الكتالوج هو الكتالوج الافتراضي.
إجراء الفحص الدوري	إذا كانت "نعم"، ابدأ عملية فحص جديدة.
تاريخ الفحص السابق	تاريخ آخر فحص لتحديث البرنامج.
نتيجة الفحص السابق	رمز نتيجة آخر فحص لتحديث البرنامج.

إدارة الأمن

مكافحة السرقة

المسح والقفل

مسح كامل	إرسال أمر لإعادة ضبط إعدادات المصنع للجهاز
مسح المؤسسات	قم بإزالة جهاز MDM من الجهاز وإزالة جميع بيانات MDM (مثل الحسابات والتطبيقات)
قفل الشاشة	جعل الجهاز يعود إلى شاشة القفل

تهيئة الأمان

رمز المرور

يسمح بتعطيل الرمز المسموح به	يحدد ما إذا كان المستخدم مجبر على تعيين رقم تعريف شخصي. إن مجرد تعيين هذه القيمة (وليس غيرها) يجبر المستخدم على إدخال رمز مرور، دون فرض طول أو جودة.
السماح بقيمة بسيطة	السماح للمستخدم باستخدام نفس سلاسل الأرقام المتشابهة والمتصاعدة والمختزلة (على سبيل المثال 1234، 1111)
تتطلب قيمة أبجدية رقمية	يجب أن تحتوي كلمات المرور على حرف واحد على الأقل
الحد الأدنى لطول رمز المرور	الحد الأدنى لطول كلمة المرور
الحد الأدنى لعدد الأحرف المعقدة	الحد الأدنى لعدد الرموز الأبجدية الرقمية في كلمة المرور
الحد الأقصى لعمر رمز المرور	عدد الأيام التي يجب تغيير كلمة المرور بعدها
القفل التلقائي الأقصى	الحد الأقصى للوقت الذي يتم بعده قفل الجهاز
فترة السماح القصوى لقفل الجهاز	مقدار الوقت الذي يمكن فيه قفل الجهاز دون المطالبة برمز المرور عند فتح القفل
الحد الأقصى لعمر رمز المرور (1-730 يوماً، أو لا شيء)	الأيام التي يجب تغيير رمز المرور بعدها
سجل رمز المرور (1-50 رمز مرور، أو لا شيء)	عدد رموز المرور الفريدة قبل إعادة الاستخدام

الشهادة

PKCS#1	
الوصف	أدخل وصفاً للشهادة
أوراق الاعتماد	تحميل ملف pkcs1

PKCS#12	
الوصف	أدخل وصفاً للشهادة
أوراق الاعتماد	تحميل ملف pkcs12

إعدادات التقييد

وظائف الجهاز

السماح للكاميرا	السماح باستخدام الكاميرا
السماح لمركز الألعاب	عند الخطأ، يتم تعطيل Game Center وإزالة أيقونته من الشاشة الرئيسية.
السماح بالألعاب متعددة اللاعبين	عند الخطأ، يحظر الألعاب متعددة اللاعبين.
السماح بإضافة أصدقاء مركز اللعب Game Center	عند الخطأ، يحظر إضافة الأصدقاء إلى Game Center.
السماح لمكتبة صور iCloud	إذا تم التعيين على خطأ، فسيؤدي ذلك إلى تعطيل مكتبة صور iCloud. ستتم إزالة أي صور لم يتم تنزيلها بالكامل من مكتبة صور iCloud إلى الجهاز من التخزين المحلي.
السماح بمعرف اللمس	إذا كان خطأ، يمنع معرف اللمس من إلغاء قفل الجهاز.

آي كلاود

حظر وظائف معينة أثناء الاقتران على iCloud

السماح بمزامنة المستندات	السماح بمزامنة المستندات
السماح بمزامنة سلسلة المفاتيح على iCloud	السماح بمزامنة سلسلة المفاتيح على iCloud
السماح بملاحظات iCloud	عندما يكون خطأ، لا يسمح بخدمات MacOS iCloud Notes
السماح بـ iCloud BTMM	في حالة الخطأ، تعطيل خدمة MacOS Back to My Mac iCloud.
السماح بـ iCloud FMM	في حالة الخطأ، يؤدي ذلك إلى تعطيل خدمة MacOS Find My Mac iCloud.
السماح بالإشارات المرجعية على iCloud	في حالة الخطأ، لا يسمح بمزامنة إشارات MacOS iCloud المرجعية.
السماح لبريد iCloud	في حالة الخطأ، لا يسمح بخدمات iCloud لبريد MacOS Mail.
السماح بتقويم iCloud	في حالة الخطأ، يؤدي ذلك إلى عدم السماح بخدمات MacOS Cloud iCloud.
السماح بتذكيرات iCloud	في حالة الخطأ، عدم السماح بخدمات تذكير iCloud.
السماح بدفتر عناوين iCloud	في حالة الخطأ، يؤدي ذلك إلى تعطيل خدمات دفتر عناوين MacOS iCloud.

إدارة وسائل الإعلام

الإخراج عند تسجيل الخروج	إخراج جميع الوسائط القابلة للإزالة عند تسجيل الخروج
السماح للشبكة	السماح بالوصول لوسائط الشبكة
السماح بالقرص الداخلي	السماح بالوصول للقرص الداخلي.
طلب المصادقة	طلب المصادقة لاستخدام هذه الوسائط
للقراءة فقط	المستخدم قادر فقط على قراءة البيانات من الوسائط
السماح بالقرص الخارجي	السماح بالوصول للقرص الخارجي.
طلب المصادقة	طلب المصادقة لاستخدام هذه الوسائط
للقراءة فقط	المستخدم قادر فقط على قراءة البيانات من الوسائط
السماح باستخدام صور القرص	السماح بالوصول للصور.
طلب المصادقة	طلب المصادقة لاستخدام هذه الوسائط
للقراءة فقط	المستخدم قادر فقط على قراءة البيانات من الوسائط
السماح باستخدام أقراص DVD-RAM	السماح بالوصول إلى قرص DVD-RAM.
طلب المصادقة	طلب المصادقة لاستخدام هذه الوسائط
للقراءة فقط	المستخدم قادر فقط على قراءة البيانات من الوسائط
السماح باستخدام أقراص DVD	السماح بالوصول إلى قرص DVD.
طلب المصادقة	طلب المصادقة لاستخدام هذه الوسائط
السماح باستخدام الأقراص المدمجة	السماح بالوصول إلى قرص CD.
طلب المصادقة	طلب المصادقة لاستخدام هذه الوسائط

إدارة الاتصال

الواي فاي

هنا يمكنك إضافة اتصالات Wi-Fi وتهيئتها

معرّف مجموعة الخدمة (SSID)	SSID للشبكة، التي سيتم إنشاء الاتصال بها
الانضمام التلقائي	تمكين الانضمام التلقائي للشبكة
الشبكة الخفية	تم التمكين، في حالة عدم بث نقطة الوصول الآلي لمعرّف SSID
إعداد الوكيل	تكوين وكيل لكل نقطة وصول لكل نقطة وصول
لا يوجد	لا تستخدم خادم وكيل
يدوي	إنشاء وكيل يدوي
عنوان URL الخادم الوكيل	عنوان الوصول إلى إعدادات الوكيل
الميناء	إنشاء المنفذ الخاص بالوكيل
المصادقة	اسم المستخدم الخاص بالمصادقة على البروكسي
كلمة المرور	كلمة المرور الخاصة بالمصادقة على الوكيل
أوتوماتيكي	إنشاء وكيل تلقائياً
عنوان URL الخادم الوكيل	عنوان URL لملف إعدادات الوكيل
نوع الأمان	إنشاء نوع الأمان لبروتوكول الوصول الآمن
WEP	
كلمة المرور	كلمة المرور الخاصة بـ AP
WPA/WPA2	
كلمة المرور	كلمة المرور الخاصة بـ AP
WEP Enterprise - / WPA WPA2 للمؤسسات / أي مؤسسة	انظر خطأ في الجدول: المصدر المرجعي غير موجود أدناه
لا يوجد	عدم إنشاء أي أمان
تعطيل التوزيع العشوائي لعنوان MAC	تعطيل التخصيص العشوائي لعناوين MAC لشبكة Wi-Fi تلك أثناء اقترانها بالشبكة. يُظهر هذا أيضًا تحذيرًا للخصوصية في الإعدادات يشير إلى أن الشبكة قد قللت من حماية الخصوصية.

تهيئة شبكة Wi-Fi للمؤسسات

ملاحظة: متوفر فقط عندما يتم تعيين "نوع الأمان" على "نوع المؤسسة".

البروتوكولات	بروتوكول المصادقة المدعوم على الشبكة المستهدفة
TLS	تمكين/تعطيل الاستخدام
TTLS	تمكين/تعطيل الاستخدام
المصادقات الداخلية	بروتوكول المصادقة الذي يجب استخدامه: PAP، CHAP، MSCHAP، MSCHAPv2
برنامج LEAP	تمكين/تعطيل الاستخدام
PEAP	تمكين/تعطيل الاستخدام
EAP-FAST	تمكين/تعطيل الاستخدام
EAP-SIM	تمكين/تعطيل الاستخدام
استخدام PAC	استخدام PAC (التحكم في الوصول المحمي)
توفير PAC	تكوين توفير PAC
توفير PAC بشكل مجهول	التوفير المجهول لـ PAC
المصادقة	
اسم المستخدم	اسم مستخدم المصادقة
لا تستخدم لكل اتصال كلمة المرور	عدم استخدام كلمة المرور لكل اتصال
كلمة المرور	كلمة المرور التي يجب استخدامها
شهادة الهوية	تحميل/تحديد شهادة المصادقة
الهوية الخارجية	الهوية التي يمكن رؤيتها خارجيًا
الثقة	
الشهادة الموثوقة 1	تحميل أول شهادة موثوق بها
الشهادة الموثوقة 2	تحميل شهادة ثانية موثوق بها
الشهادة الموثوقة 3	تحميل شهادة ثالثة موثوق بها
الخادم الموثوق به أسماء الشهادات	أسماء شهادات الخادم المتوقعة (في قائمة مفصولة بفاصلة)

VPN

اعتماداً على نوع الاتصال المحدد، قد تظهر حقول مختلفة.

اسم الاتصال	اسم ملف تعريف VPN-ملف تعريف VPN
نوع VPN	
VPN	سيتم توجيه كل حركة مرور شبكة الجهاز عبر اتصال VPN.
نوع الاتصال	إنشاء نوع اتصال VPN
IPsec (سيسكو)	بروتوكول IPsec من سيسكو
L2TP	بروتوكول L2TP
SSL مخصص	الاتصال عبر SSL مخصص SSL
IKEv2	بروتوكول IKEv2
إعداد الوكيل	تكوين وكيل للاتصال بشبكة VPN
لا يوجد	عدم إنشاء أي وكيل
يدوي	إنشاء وكيل يدوياً
عنوان URL الخادم الوكيل	عنوان الوصول إلى إعدادات الوكيل
الميناء	إنشاء المنفذ الخاص بالوكيل
المصادقة	اسم المستخدم للمصادقة في الوكيل
كلمة المرور	كلمة المرور للمصادقة في الوكيل
أوتوماتيكي	إنشاء وكيل تلقائياً
عنوان URL الخادم الوكيل	عنوان URL للوصول إلى إعدادات الوكيل

وكيل HTTP

نوع الوكيل	
يدوي	إنشاء وكيل يدوياً
عنوان URL الخادم الوكيل	عنوان الوصول إلى إعدادات الوكيل
الميناء	إنشاء منفذ الوكيل
المصادقة	اسم المستخدم للمصادقة في الوكيل
كلمة المرور	كلمة المرور للمصادقة في الوكيل
أوتوماتيكي	إنشاء وكيل تلقائياً
عنوان URL لـ PAC الوكيل	عنوان URL لـ PAC الوكيل
السماح بالاتصال المباشر في حالة تعذر الوصول إلى PAC	السماح بالاتصال المباشر (بدون VPN)، إذا تعذر الوصول إلى PAC
السماح بتجاوز البروكسي للوصول إلى الشبكات الأسيرة	السماح بتجاوز البروكسي للوصول إلى الشبكات الداخلية الأسيرة

AirPrint

عنوان IP	عنوان IP للطابعة
مسار الموارد	مسار محدد إلى جهاز AirPrint

AirPlay

اسم الجهاز	اسم الجهاز
كلمة المرور	كلمة مرور الاقتران
القائمة البيضاء	تحديد قائمة بالأجهزة التي يمكن للجهاز الاقتران بها حصريًا

إدارة PIM

المزامنة النشطة للتبادل

اسم الحساب	اسم الحساب
عنوان البريد الإلكتروني	عنوان الحساب (على سبيل المثال max@company.com)
اسم مضيف الخادم	اسم المضيف الداخلي
اسم تسجيل الدخول	يجب أن يكون "المجال" و"اسم تسجيل الدخول" فارغين حتى يطلب الجهاز من المستخدم.
المجال	يجب أن يكون "المجال" و"اسم تسجيل الدخول" فارغين حتى يطلب الجهاز من المستخدم. إذا تم تمكين تكوين بوابة ACL ولم يكن حقل المجال فارغًا، فستقوم بوابة AppTec360 العالمية بمصادقة الجهاز بالاسم التالي "اسم المجال/اسم تسجيل الدخول"
كلمة المرور	كلمة المرور الخاصة بالحساب (مثل secretUserPassword)
الأيام الماضية من البريد للمزامنة	عدد الأيام الماضية للبريد المراد مزامنته
استخدام SSL	استخدام SSL لمضيف التبادل الداخلي
خيار متقدم	إظهار الخيارات المتقدمة
منفذ الخادم	المنفذ الداخلي
مسار الخادم	المسار الداخلي
اسم المضيف الخارجي	مضيف خارجي
منفذ خارجي	منفذ خارجي
المسار الخارجي	المسار الخارجي
استخدام SSL للخارجي مضيف التبادل	استخدام SSL لمضيف التبادل الخارجي

البريد الإلكتروني

إعداد حسابات POP3/ IMAP على جهاز المستخدم النهائي

وصف الحساب	اسم حساب البريد الإلكتروني
نوع الحساب	
IMAP	
بادئة المسار	بادئة المسار للمجلدات الخاصة
الملوثات العضوية الثابتة	
اسم عرض المستخدم	اسم عرض المستخدم
عنوان البريد الإلكتروني	عنوان البريد الإلكتروني للمستخدم

البريد الوارد	إعدادات الخادم الوارد
عنوان خادم البريد	عنوان خادم البريد
منفذ خادم البريد	منفذ خادم البريد
اسم المستخدم	اسم المستخدم المعني
نوع المصادقة	نوع المصادقة
لا يوجد	لا يوجد نوع مصادقة
كلمة المرور (على مستوى الجهاز فقط)	مطالبة كلمة المرور
الاستجابة لتحديات إدارة الألفية الجديدة	
NTLM	مصادقة NTLM-المصادقة
HTTP MD5 Digest	
استخدام SSL	استخدم SSL، إذا لزم الأمر

البريد الصادر	إعدادات الخادم الصادر
عنوان خادم البريد	عنوان خادم البريد
منفذ خادم البريد	منفذ خادم البريد
اسم المستخدم	اسم المستخدم المعني
نوع المصادقة	
لا يوجد	لا توجد طريقة مصادقة
كلمة المرور (على مستوى الجهاز فقط)	مطالبة كلمة المرور
الاستجابة لتحديات إدارة الألفية الجديدة	
NTLM	مصادقة NTLM-المصادقة
HTTP MD5 Digest	
استخدام SSL	استخدم SSL، إذا لزم الأمر
كلمة المرور الصادرة نفس كلمة المرور الواردة	كلمة المرور الصادرة نفس كلمة المرور الواردة
الاستخدام في البريد فقط	تنشيط، إذا كانت جميع رسائل البريد الإلكتروني الصادرة سيتم إرسالها عبر تطبيق البريد الإلكتروني

كالداف

تكوين إعداد حساب CalDav وتوزيع حساب CalDav

وصف الحساب	اسم العرض للحساب
اسم المضيف	اسم المضيف و/أو عنوان IP
الميناء	منفذ حساب CalDav
عنوان URL الرئيسي	عنوان URL الرئيسي للحساب
اسم المستخدم	اسم المستخدم الخاص ب CalDav
كلمة المرور (على مستوى الجهاز فقط)	كلمة مرور CalDav المحتملة
استخدام SSL	استخدم SSL، إذا لزم الأمر

كارد داف

تكوين إعداد حساب CardDav وتوزيع حساب CardDav

وصف الحساب	اسم العرض للحساب
اسم المضيف	اسم المضيف و/أو عنوان IP
الميناء	منفذ حساب CardDav
عنوان URL الرئيسي	عنوان URL الرئيسي للحساب
اسم المستخدم	اسم المستخدم الخاص ب CardDav
كلمة المرور (على مستوى الجهاز فقط)	كلمة المرور الخاصة بـ CardDav
استخدام SSL	استخدم SSL، إذا لزم الأمر

LDAP

في هذا المجال، قم بإعداد اتصال LDAP، من أجل السماح بتبادل ديناميكي للشهادات، بين جهاز المستخدم النهائي والدليل النشط.

يرجى ملاحظة أن المستخدم المحدد يتطلب إذن القراءة المعني.

وصف الحساب	وصف الحساب
اسم مستخدم الحساب	مستخدم للدخول إلى LDAP
كلمة مرور الحساب	كلمة المرور للدخول إلى LDAP
اسم مضيف الحساب	اسم مضيف خادم LDAP/عنوان IP
استخدام SSL	استخدم SSL، إذا لزم الأمر

في الجزء الثاني، يمكنك تحديد عوامل تصفية فردية للبحث في سجل LDAP.

الوصف	النطاق	قاعدة البحث
وصف المرشح	مستوى البحث في سجل LDAP	تحديد المرشح الفردي

لوحة المعلومات والتقارير

إعدادات لوحة التحكم

هنا يمكنك معرفة لوحات المعلومات الموجودة أو تعديلها أو إنشاء لوحات جديدة. تحتوي كل لوحة معلومات على مجموعة البيانات الخاصة بها لإظهارها وتكوين الرسم البياني.

التحكم في إعدادات لوحة التحكم

عام	تعيين لوحة التحكم عامة، بحيث يمكن للمستخدمين الآخرين رؤية لوحة التحكم. يجب أن يكون المستخدمون بالطبع قادرين على تسجيل الدخول وعرض لوحات المعلومات. إذا لم يتم تفعيل "عام"، يمكن للمنشئ فقط رؤيتها.
افتراضي	تعيين لوحة التحكم كافتراضية بحيث تفتح تلقائيًا في المرة التالية التي تصل فيها إلى طريقة عرض لوحة التحكم.
	إظهار لوحة التحكم والرسوم البيانية الخاصة بها
	حذف لوحة التحكم
	تحرير اسم لوحة التحكم والإعدادات
	قم بعمل نسخة من لوحة التحكم
	إضافة لوحة تحكم جديدة بالكامل

عرض لوحة المعلومات

يعرض هذا البيانات والرسوم البيانية للوحة المعلومات المحددة ويتيح لك أيضًا تغييرها.

التحكم في لوحة التحكم

يتيح لك تحديد البيانات التي يتم عرضها في لوحة التحكم، وكمية البيانات التي سيتم عرضها وحجمها لإظهار هذه البيانات
يعيدك إلى نظرة عامة على لوحة التحكم
إعادة تعيين لوحة التحكم المفتوحة حاليًا إلى الوضع الافتراضي لها
يحفظ جميع التغييرات التي أجريتها على لوحة التحكم المفتوحة حاليًا (على سبيل المثال البيانات التي يجب إظهارها)
تغيير نوع المخطط إلى مخطط عمودي
تغيير نوع المخطط إلى مخطط دائري
تغيير نوع المخطط إلى مخطط دائري مجوف
تغيير نوع المخطط البياني إلى مخطط مساحي قطبي
تغيير ترتيب الفرز

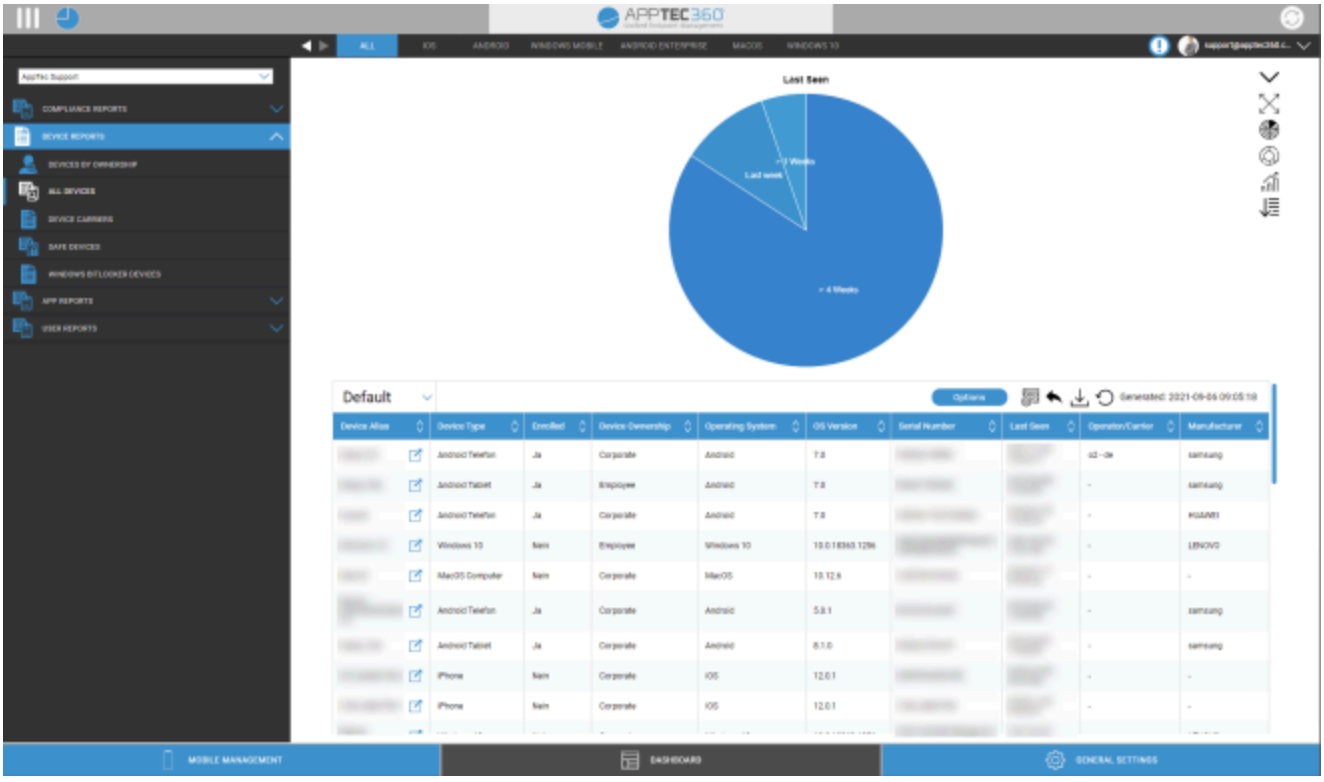
التقارير الموسعة

تقدم "التقارير الموسعة" لمحات عامة ورسوم بيانية مفصلة حول معلومات الجهاز والمستخدم.

هناك عدد قليل من التقارير الافتراضية ولكن يمكن تغييرها جميعًا يدويًا لإضافة أو إزالة البيانات لإظهارها.

يرجى ملاحظة أنه يمكنك فقط تغيير البيانات التي يتم عرضها يدويًا. تحدد فئة التقرير المحددة البيانات التي يستند إليها ذلك. على سبيل المثال، لن تتمكن أبدًا من رؤية أجهزة Android في تقرير iOS في تقارير الأجهزة جميع الأجهزة iOS

في أعلى اليسار، يمكنك قصر بيانات التقارير على مجموعة معينة (وجميع مجموعاتها الفرعية). يتم تعيين ذلك افتراضيًا على العقدة الجذرية، بحيث تأخذ جميع الأجهزة والمستخدمين في الاعتبار.



التحكم في التقارير الموسعة

في كل نظرة عامة يمكنك استخدام الوظائف التالية لتغيير التقرير بأي طريقة تريدها:

إخفاء المخطط (في حالة عرض المخطط)
إظهار المخطط (إذا كان المخطط مخفيًا)
توسيع المخطط (إذا كان المخطط مطويًا)
طي المخطط (إذا كان المخطط موسعًا)
تغيير نوع المخطط إلى مخطط عمودي
تغيير نوع المخطط إلى مخطط دائري
تغيير نوع المخطط إلى مخطط دائري مجوف
تغيير نوع المخطط البياني إلى مخطط مساحي قطبي
تغيير ترتيب الفرز
قم بتعديل الأجزاء التالية حول النظرة العامة المعروضة: • إضافة/إزالة أعمدة • تحديد الترتيب الذي يتم به عرض الأعمدة • إظهار/إخفاء الرسم البياني أعلى الجدول • حدد العمود المستخدم في الرسم البياني • تصفية بيانات الجدول الخاص بك
افتح مدير الإعداد لحفظ التقارير المختلفة وتحميلها
إعادة تعيين التقرير المفتوح حالياً إلى الوضع الافتراضي
تصدير التقرير الحالي كملف .csv
إعادة إنشاء البيانات وإعادة تحميل التقرير الحالي

يمكنك العثور على قائمة بجميع التقارير الافتراضية في الصفحات التالية.

تقارير الامتثال

الأجهزة المتجذرة

نظرة عامة على الأجهزة التي تم عمل روت لها/كسر حمايتها.

الأعمدة الافتراضية لهذا التقرير:

الاسم المستعار للجهاز
مالك الجهاز
البريد الإلكتروني
نظام التشغيل
رقم الهاتف
آخر ظهور
الشركة المصنعة

أجهزة التجوال

نظرة عامة على جميع الأجهزة التي تقوم بالتجوال

الأعمدة الافتراضية لهذا التقرير:

الاسم المستعار للجهاز
مالك الجهاز
البريد الإلكتروني
نوع الجهاز
نظام التشغيل
رقم الهاتف
آخر ظهور

الأجهزة الممكّنة للتجوال

نظرة عامة على جميع الأجهزة التي قامت بتفعيل التجوال ولكن ليس بالضرورة أن تكون قيد التجوال حالياً.

الأعمدة الافتراضية لهذا التقرير:

الاسم المستعار للجهاز
مالك الجهاز
البريد الإلكتروني
نوع الجهاز
نظام التشغيل
رقم الهاتف
آخر ظهور

الأجهزة الخاضعة للإشراف

نظرة عامة على جميع الأجهزة الخاضعة للإشراف في الوضع الخاضع للإشراف (iOS فقط)

الأعمدة الافتراضية لهذا التقرير:

الاسم المستعار للجهاز
مالك الجهاز
البريد الإلكتروني
نوع الجهاز
آخر ظهور

الأجهزة غير النشطة

نظرة عامة على جميع الأجهزة التي لم تتصل بالخادم خلال آخر 7 أيام

الأعمدة الافتراضية لهذا التقرير:

الاسم المستعار للجهاز
مالك الجهاز
البريد الإلكتروني
نوع الجهاز
نظام التشغيل
آخر ظهور

تقارير الجهاز

الأجهزة حسب الملكية

يمكنك هنا معرفة عدد الأجهزة التي تم نشرها حالياً كأجهزة مؤسسية (أجهزة الشركات) وأجهزة الموظفين (أجهزة خاصة).

الأعمدة الافتراضية لهذا التقرير:

الاسم المستعار للجهاز
مالك الجهاز
نوع الجهاز
ملكية الجهاز
نظام التشغيل

جميع الأجهزة

هنا يمكنك الاطلاع على نظرة عامة على جميع الأجهزة مع أهم المعلومات.

الأعمدة الافتراضية لهذا التقرير:

الاسم المستعار للجهاز
نوع الجهاز
مسجل
ملكية الجهاز
نظام التشغيل
إصدار نظام التشغيل
الرقم التسلسلي
آخر ظهور
المشغل/الناقل
الشركة المصنعة

حاملات الأجهزة

هنا يمكنك الاطلاع على نظرة عامة بخصوص الناقل (مزود الخدمة الخلوية).

الأعمدة الافتراضية لهذا التقرير:

الاسم المستعار للجهاز
مالك الجهاز
البريد الإلكتروني
نظام التشغيل
إصدار نظام التشغيل
المشغل/الناقل

الأجهزة الآمنة

هنا يمكنك الاطلاع على نظرة عامة على الأجهزة التي تستخدم الإصدار الآمن (SAFE).

نظرًا لأن النظرة العامة و/أو SAFE متاحة فقط لأجهزة سامسونج، فلن ترى علامات التبويب المعتادة تحت هذه النقطة.

الأعمدة الافتراضية لهذا التقرير:

الاسم المستعار للجهاز
مالك الجهاز
البريد الإلكتروني
نوع الجهاز
آخر ظهور
الإصدار الآمن

أجهزة ويندوز BitLocker Windows BitLocker

هنا يمكنك الاطلاع على نظرة عامة على أجهزة ويندوز التي تستخدم BitLocker.

الأعمدة الافتراضية لهذا التقرير:

الاسم المستعار للجهاز
مالك الجهاز
البريد الإلكتروني

حالة BitLocker

تقارير التطبيق

هنا يمكنك الحصول على مجموعة متنوعة من اللمحات العامة فيما يتعلق بالتطبيقات. في كل هذه التقارير، يمكنك النقر على إدخال ما لمعرفة المزيد من الإصدارات المثبتة على الأجهزة وعدد مرات التثبيت. في هذا العرض يمكنك النقر على إصدار معين مرة أخرى لمعرفة الأجهزة التي تم تثبيت هذا الإصدار المحدد عليها.

ملاحظة: قد يستغرق الأمر بعض الوقت حتى يحصل النظام على معلومات محدثة من الجهاز. بالإضافة إلى ذلك لا يتم تحديث التقارير كل دقيقة. قد تحتاج إلى التحلي بالصبر لرؤية الحالة الحالية إذا كنت قد قمت للتو بتعيين تطبيق أو إصدار جديد. ستؤدي إعادة تحميل التقرير يدويًا إلى إجبار التقرير على إظهار أحدث البيانات المتاحة

التطبيقات المثبتة

هنا يمكنك الحصول على نظرة عامة على جميع التطبيقات المثبتة.

الأعمدة الافتراضية لهذا التقرير:

الاسم	اسم التطبيق و/أو الخدمة المعنية
المعرف	معرف التطبيق/معرف الخدمة المحدد
العدد الإجمالي	عدد مرات تثبيت هذا التطبيق/الخدمة على أجهزة المستخدم النهائي

التطبيقات الأكثر تثبيتاً

هنا يمكنك الحصول على نظرة عامة على التطبيقات التي تم تثبيتها أكثر من غيرها.

الأعمدة الافتراضية لهذا التقرير:

الاسم	اسم التطبيق و/أو الخدمة المعنية
المعرف	معرف التطبيق/معرف الخدمة المحدد
العدد الإجمالي	عدد مرات تثبيت هذا التطبيق/الخدمة على أجهزة المستخدم النهائي

التطبيقات الإلزامية

هنا يمكنك الحصول على نظرة عامة على التطبيقات الإلزامية (الإلزامية المطلوبة).

الأعمدة الافتراضية لهذا التقرير:

الاسم	اسم التطبيق و/أو الخدمة المعنية
المعرف	معرف التطبيق/معرف الخدمة المحدد
مصدر التطبيق	أي متجر التطبيقات المعني AppStore: • جوجل بلاي ستور (أندرويد) • متجر تطبيقات iTunes AppStore (iOS)
نظام التشغيل	نظام التشغيل

التطبيقات المدرجة في القائمة السوداء

هنا يمكنك الحصول على نظرة عامة على جميع التطبيقات المحددة المدرجة في القائمة السوداء.

الأعمدة الافتراضية لهذا التقرير:

الاسم	اسم التطبيق و/أو الخدمة المعنية
المعرف	معرف التطبيق/معرف الخدمة المحدد
مصدر التطبيق	أي متجر التطبيقات المعني AppStore: • جوجل بلاي ستور (أندرويد) • متجر تطبيقات iTunes AppStore (iOS)
نظام التشغيل	نظام التشغيل

تقارير المستخدمين

التعريفة

هنا يمكنك الحصول على نظرة عامة على تعريفات هواتف المستخدمين وبطاقات SIM.

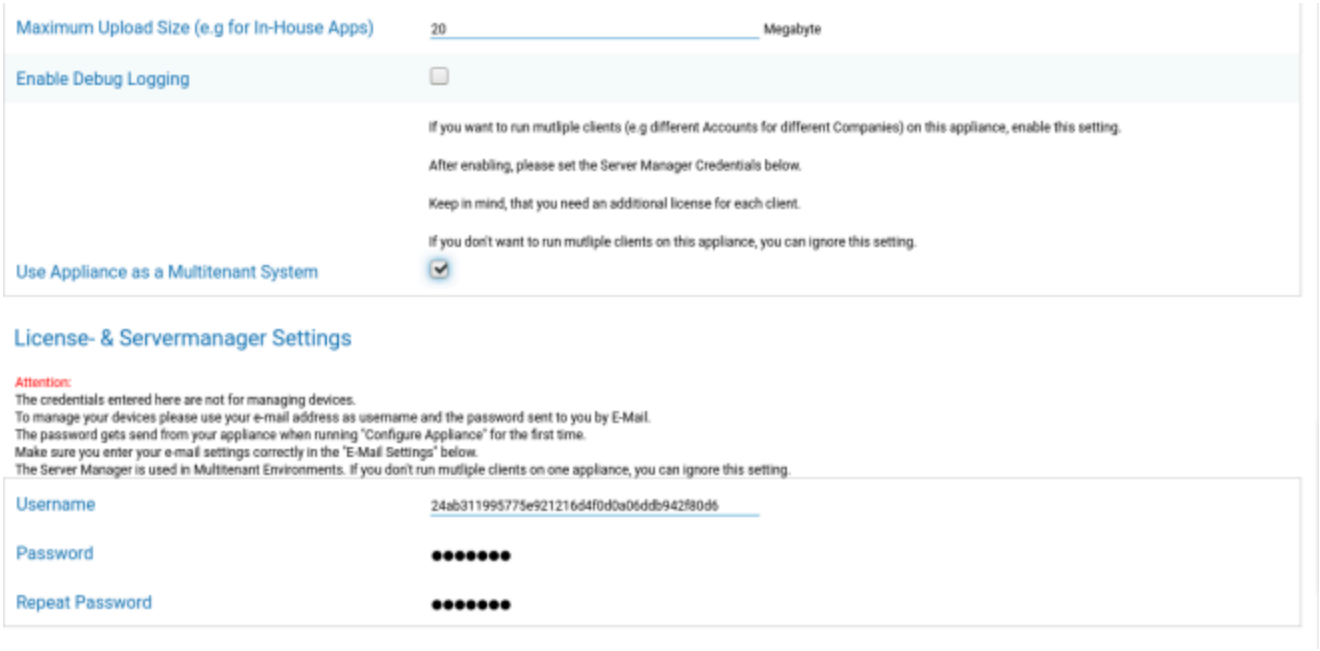
الأعمدة الافتراضية لهذا التقرير:

البريد الإلكتروني
الاسم
رقم الهاتف
الناقل
التعريفة الجمركية
الخيار
السعر
تم إلغاء العقد
بدء العقد
أثناء الوقت
الجوال والبيانات
حجم البيانات
شريحة SIM المتعددة
النوع
simCardSerial1
simCardSerial2
simCardSerial3
دبوس1
دبوس2
بوك1
بوك2
ملاحظة

إدارة تعدد المستأجرين

إن AppTec360 EMM قادر على استضافة العديد من المستأجرين المنفصلين، لكل منهم مستخدميه ومجموعاته وأذوناته وإعداداته العامة.

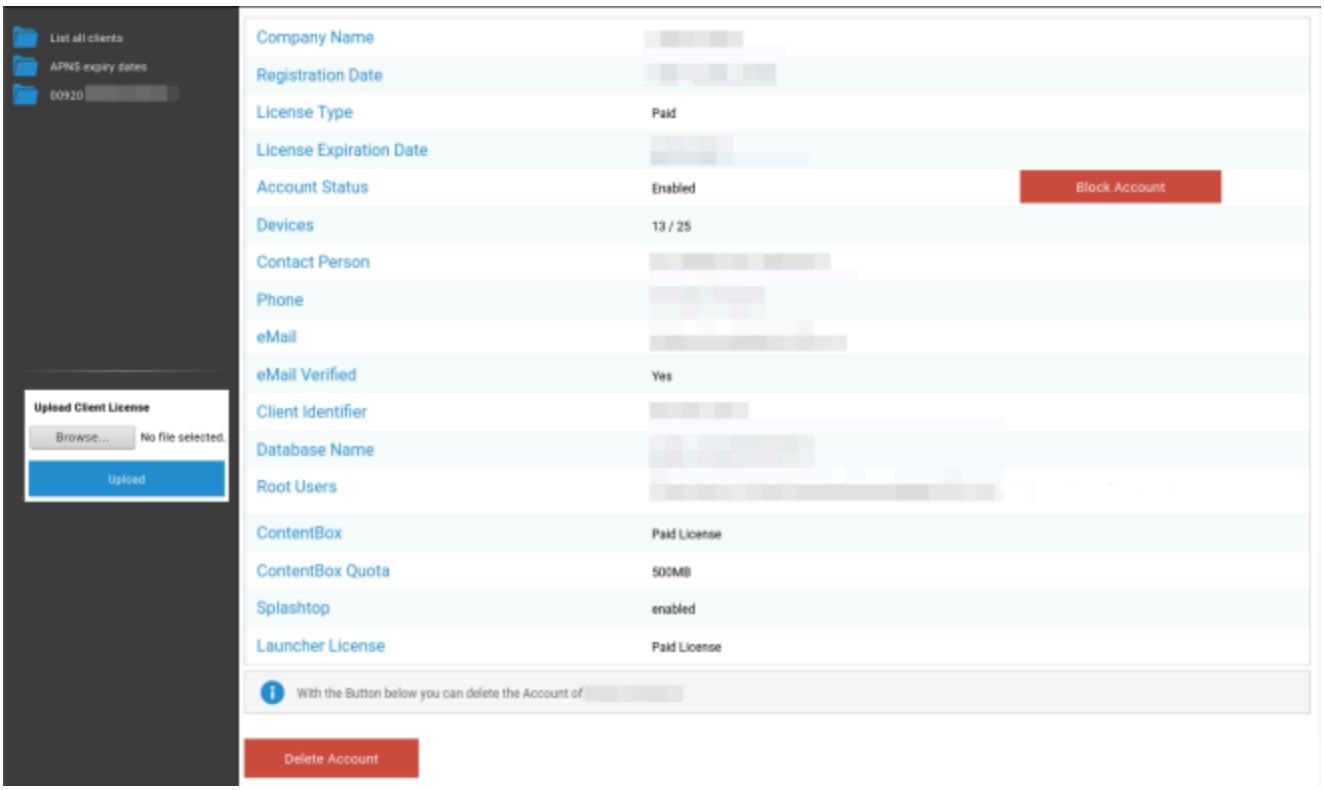
لتمكين إمكانيات تعدد المستأجرين، عليك تمكينها في واجهة تكوين الجهاز في "الخطوة الثالثة - إعدادات الخادم".



في القائمة الجديدة قم بتعيين اسم مستخدم وكلمة مرور لمدير الخادم. احفظ الإعدادات وقم بتشغيل "تكوين الجهاز" في "الخطوة الخامسة - اتفاقية الترخيص" لتطبيق الإعداد.

عند الانتهاء من التهيئة، يمكنك الآن تسجيل الدخول ببيانات الاعتماد المحددة من خلال واجهة إدارة الأجهزة المحمولة العادية.

بعد تسجيل الدخول يمكنك مشاهدة العرض التالي.



على اليسار يمكنك رؤية جميع المستأجرين (في هذه الحالة واحد فقط مع المعرف 920) وعلى اليمين المعلومات المتعلقة بهذا العميل. لديك أيضًا خيار حظر الوصول إلى الحساب وكذلك حذف العميل (تنبيه: سيؤدي ذلك إلى إزالة جميع البيانات المتعلقة بهذا العميل).

على اليسار، يمكنك تحميل ترخيص عميل جديد، والذي يمكن أن يكون إما تحديث ترخيص لعميل حالي أو ترخيص جديد ينشئ تلقائياً عميلاً جديداً. عندما يتم إنشاء عميل جديد يتم إرسال بريد إلكتروني يحتوي على كلمة مرور تسجيل الدخول تلقائياً إلى عنوان البريد الإلكتروني الذي تم إصدار الترخيص له.

للحصول على ترخيص عميل جديد أو محدث (على سبيل المثال عند الحاجة إلى المزيد من تراخيص الأجهزة) اتصل بمندوب المبيعات الخاص بك.

مشاهدات إضافية

قائمة بجميع العملاء

يعرض نظرة عامة حول جميع العملاء في النظام.

هوية العميل	هوية العميل
المعرف	معرّف العميل
قاعدة البيانات	قاعدة البيانات
اسم الشركة	اسم الشركة
البريد الإلكتروني	البريد الإلكتروني للشخص الذي يمكن الاتصال به
تم التحقق	سواء تم التحقق من البريد الإلكتروني لجهة الاتصال أم لا
البلد	البلد
الأجهزة	عدد الأجهزة المسجلة
تاريخ التسجيل	النقطة الزمنية لتخصيص الترخيص
آخر تسجيل دخول	آخر تسجيل دخول لحساب المسؤول
الترخيص	عرض نوع الترخيص (مجاني |مدفوع)
ترخيص CB	نوع ترخيص ContentBox (مجاني |مدفوع)
الحالة	حالة عميل AppTec الحالية
منتهية الصلاحية	يعرض، إذا انتهت صلاحية الترخيص
iOS	عدد أجهزة iOS
أندرويد	عدد أجهزة أندرويد
ويندوز موبايل	عدد أجهزة ويندوز موبايل
نظام التشغيل MacOS	عدد أجهزة MacOS
ويندوز 10	عدد أجهزة ويندوز 10
أندرويد إنتربرايز	عدد أجهزة Android المؤسسية
نظام التشغيل IOS BYOD (تسجيل المستخدم)	عدد أجهزة IOS BYOD (تسجيل المستخدم)
إنترنت الأشياء	عدد أجهزة إنترنت الأشياء

تواريخ انتهاء صلاحية APNS

يعرض نظرة عامة على جميع تواريخ انتهاء صلاحية شهادات APNS لجميع العملاء.

هوية العميل	هوية العميل
اسم الشركة	اسم الشركة
تاريخ انتهاء الصلاحية	تاريخ انتهاء صلاحية شهادة Apple APNS-شهادة Apple APNS
المعلومات	معلومات حول انتهاء الصلاحية

اتصل بنا

أسئلة إضافية؟ ما عليك سوى الاتصال بنا تحت

للأسئلة الفنية العامة

support@apptec360.com

+41 61 511 3210

للأسئلة المتعلقة بتثبيت جهاز افتراضي

consulting@apptec360.com

+41 61 511 3214

إخلاء المسؤولية